SECURITY
IN THE DIGITAL WORLD

Practical solutions for seniors with analysis of cybercrime case studies

CONTENTS:

Funded by the European Union

CYBER SAFE SENIOR

Modern technology is becoming more and more integrated into our lives, which emphasizes the crucial importance of security in the virtual world. This issue is particularly important for seniors, who are often not as proficient in modern technologies and are more exposed to cyber threats. E-book "Security in the digital world. “Practical solutions for seniors with an analysis of cybercrime case studies” offers the necessary knowledge and tools that support older people in protecting themselves against threats on the Internet.

This e-book was created as part of the "Cyber Safe Senior" project number 2023-1-PL01-KA220-ADU-000160325 funded by the European Union. This project aims to raise seniors' awareness of Internet safety rules and develop their digital skills. Responding to the growing demand for education in the safe use of the Internet, the project provides practical tips, case studies and analyzes to help seniors avoid dangers and react in emergency situations.

The e-book contains chapters on various aspects of cybersecurity such as cyber attacks, financial fraud, social manipulation, online transaction fraud and identity theft. Each chapter contains case studies that illustrate the activities of cybercriminals and show how to effectively defend against them. Thanks to its practical advice, this e-book is a valuable source of knowledge for seniors who want to safely use modern technologies.

SIMBIOZA MED GENERACIJAMI

Instytut Nowych Technologii

ILKSENOL DERNEĞİ

Institute of Entrepreneurship Development iED

As part of the project, we have prepared unique materials that not only provide valuable knowledge, but also engage and interest users. One of the key elements is professionally prepared video clips - five dynamic, visually appealing films that illustrate real situations, potential threats and appropriate responses to dangers in an accessible way. These films aim to educate through practical examples, which makes the information provided easier to understand and remember.

We have also prepared an interactive quiz package. These quizzes have been developed in a way that is not only educational, but also interesting and fun, so that participants can test their knowledge while having fun. This form of engaging recipients not only makes the message more attractive, but also increases its effectiveness, ensuring that the knowledge gained will stay with them for longer.

These elements, combining education and entertainment, make the project not only valuable, but also attractive and enjoyable for every recipient.

Funded by the European Union

CYBER SAFE SENIOR

VIDEOS:

Emotional manipulation - charity scam

Financial manipulation

Password cracking

Impersonation and deepfake

Online shopping pitfalls

QUIZZES:

SMS Scams: How Well Can You Protect Yourself?

Email attacks, phishing scams, the risks of using weak passwords, and malware and computer viruses.

Impersonation and deepfake technologies.

Buying and Selling Online: Can You Spot the Threats?

Financial manipulation and exploit the emotions of seniors.

SIMBIOZA MED GENERACIJAMI

Instytut Nowych Technologii

ILKSENOL DERNEĞİ

Institute of Entrepreneurship Development iED

CHAPTER 1.
CYBER ATTACKS AND INTERNET SECURITY

In today's digital world, seniors are increasingly vulnerable to cyberattacks that threaten their online safety. In this chapter, we'll discuss the methods of attack and the security measures that can help seniors protect themselves from threats.

Wi-Fi attacks include both private and public networks, which can be used by criminals to intercept data. It's important to understand the risks of using public hotspots and be able to recognize secure Wi-Fi networks.

Email attacks, such as phishing, send fake messages that appear to be from trusted institutions in order to obtain personal information. Weak passwords are another problem that can make it easier to access private accounts.

Malware and viruses pose a serious risk that can infiltrate devices and steal data. We'll discuss protection methods such as regular updates, antivirus software, and avoiding suspicious links.

We will focus on practical tips and strategies to help seniors understand and avoid these risks and protect their data and privacy online.

Attack via Wi-Fi networks (private and public)

HAZARD CHARACTERISTICS:

Public Wi-Fi networks allow access to the Internet for free and are considered a great convenience. They are available in many public places, including libraries, coffee shops, airports, restaurants and hotels. However, open Wi-Fi has long been considered a risky online environment for your information. While no Wi-Fi network is completely risk-free, the security of your private data largely depends on the type of Wi-Fi network. Attacks on Wi-Fi networks, both private and public, can take many forms.

Here are five types of such attacks:

Man in the middle attack (MitM)

In a MitM attack, the attacker intercepts communication between two devices on a Wi-Fi network by impersonating one of the parties. Thanks to this, it can capture data such as logins, passwords or banking information without users' knowledge.

Evil Twin type attack

In an Evil Twin attack, the attacker creates a fake Wi-Fi network that, at first glance, looks identical to a legitimate network. Users, thinking they are connecting to a real network, connect to a fake network, allowing the attacker to intercept any data being transmitted.

Attack via Wi-Fi networks (private and public)

HAZARD CHARACTERISTICS:

Brute Force Attack on Wi-Fi Password

The attacker tries to guess the Wi-Fi password using programs that systematically test different combinations of characters. When a password is weak or too simple, this attack can be effective, allowing unauthorized access to the network.

A Packet Sniffing type attack

In this attack, the attacker uses special software to capture and analyze data packets sent over a Wi-Fi network. Even on a secured network, if data is not properly encrypted, it can be read and used.

Denial of Service (DoS) attack

In a DoS attack, the attacker sends a large number of invalid requests or false deauthorization signals to a Wi-Fi access point, causing network congestion. This may temporarily disable or disrupt the network, preventing users from using the connection.

Attack via Wi-Fi networks (private and public)

CONSEQUENCES:

Using public and free Internet access, comes with a number of dangers that can jeopardize sensitive data and online security. It is important to know what the risks are when using public Wi-Fi networks.

Consequences resulting from different types of attacks on the Wi-Fi network:

01 Man-in-the-Middle (MitM)

Seniors can fall victim to identity theft or lose their savings if a criminal intercepts login details to bank accounts or social networking sites.

02 Evil Twin

Users may unknowingly provide their login credentials, credit card numbers, or other sensitive information, thinking they are using a secure network.

Attack via Wi-Fi networks (private and public)

CONSEQUENCES:

03 Brute Force

If seniors use simple or repetitive passwords, criminals can gain access to their networks, which can lead to privacy breaches as well as increased internet bills.

04 Packet Sniffing

Seniors may be at risk of leaking private information such as emails, passwords and personal information if attackers intercept unencrypted data.

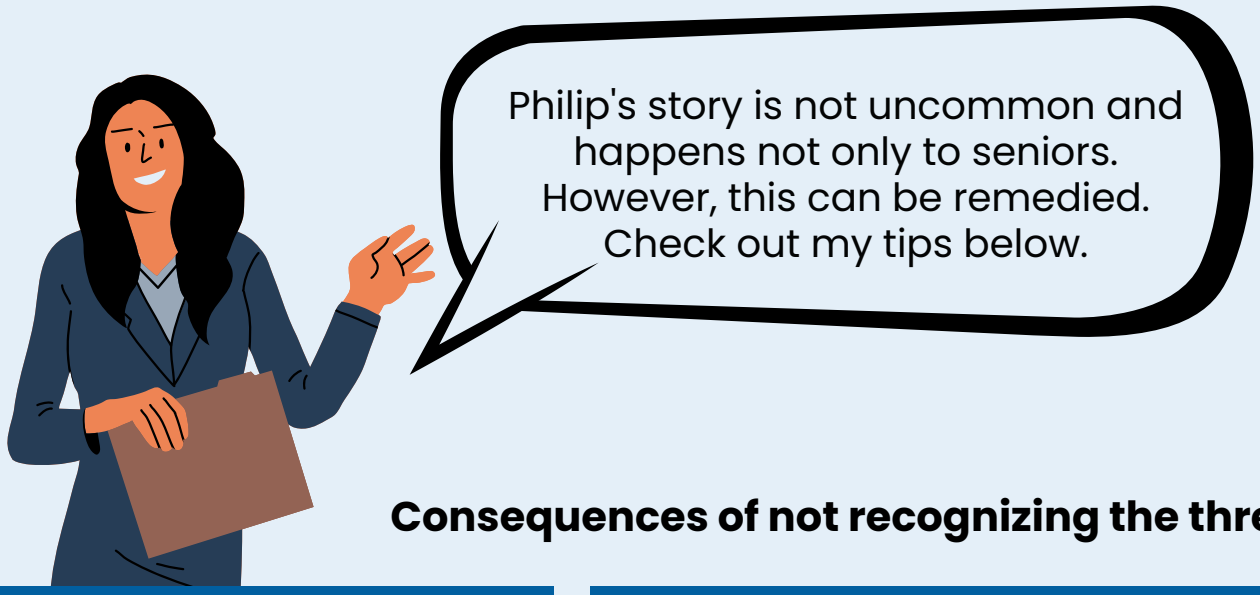
05 Denial of Service (DoS)

A DoS attack can prevent seniors from using the Internet, which is especially problematic for people who rely on technology to communicate with loved ones or handle everyday matters.

Attack via Wi-Fi networks (private and public)

— WAYS OF PROTECTION WITH HISTORY IN THE BACKGROUND

Philip decided to eat dinner at a nearby restaurant. Using the restaurant's public Wi-Fi, he opened his email to check the latest news. Unfortunately, unaware of the dangers associated with public Wi-Fi networks, he did not secure his connection. As a result of a Man-in-the-Middle attack, the criminal intercepted his email login details, resulting in unauthorized access to his account and potential leakage of confidential information.



Consequences of not recognizing the threat:

STEP 1: Attack on the Wi-Fi network in a restaurant in a public place

Philip uses the public Wi-Fi network in the restaurant to check his e-mail. The lack of appropriate security measures, such as the lack of two-factor authentication, allowed the criminal to intercept login details.

STEP 2: Unauthorized email access

As a result of the attack, the criminal gained unauthorized access to Philip e-mail account, gaining sensitive information such as private correspondence, contacts and other confidential data.

STEP 3: Leak of confidential information

Taking over an e-mail account may lead to a potential leak of Philip confidential information, which may threaten his privacy and security. A criminal could use this data for fraud, identity theft or other illegal activities.

STEP 4: Emotional consequences

Philip experienced stress, anxiety and loss of confidence in using public Wi-Fi networks. Additionally, the need to change passwords, monitor accounts, and take actions to prevent further attacks may require additional time and effort.

Attack via Wi-Fi networks (private and public)

WAYS OF PROTECTION WITH HISTORY IN THE BACKGROUND

You can avoid such consequences by following the methods below to protect yourself from attacks via Wi-Fi.

Use strong passwords:

Secure your Wi-Fi network with a strong, unique password. Remember not to use obvious passwords, such as name, surname, date of birth or other easy-to-guess character combinations.

Update software:

Update your router software regularly to protect against known security vulnerabilities.

Attack via Wi-Fi networks (private and public)

WAYS OF PROTECTION WITH HISTORY IN THE BACKGROUND

Enable encryption:

Make sure all data in transit is encrypted, even on secured Wi-Fi networks.

Avoid public Wi-Fi networks:

If possible, avoid using public Wi-Fi networks to transmit sensitive data. If you must use them, use a virtual private network (VPN).

Monitor your network:

Regularly check what devices are connected to your Wi-Fi network to quickly detect unauthorized devices.

Email attacks

HAZARD CHARACTERISTICS:

Email-based attacks are malicious attempts to gain unauthorized access to systems or information through email accounts. There are many types of attacks to which seniors are vulnerable. It's worth familiarizing yourself with some of the most common ones.

The main types of attacks on e-mail boxes:

Phishing attacks

Phishing is a common method in which fraudsters send fake emails that appear to come from trusted sources (e.g. banks, government offices).

Action of fraudsters:

- Fake links and attachments: Scammers send messages with links to fake websites or attachments designed to obtain sensitive information such as passwords and credit card numbers.
- Creating a sense of urgency: Emails often include information about problems with your account, the need to update your information immediately, or warnings about suspicious activity.

Spear Phishing attacks

Spear phishing is a more advanced form of phishing in which attacks are personalized and targeted at specific people.

Action of fraudsters:

- Personalized messages: Scammers collect information about the victim from public sources such as social media to create legitimate emails.
- Friend impersonation: These messages often appear to be sent by someone the victim knows (e.g. a colleague from work).

Email attacks

HAZARD CHARACTERISTICS:

Email Spoofing attacks

Email spoofing is a technique in which fraudsters change email headers to make them appear to be sent from a trusted source.

Action of fraudsters:

- Fake headers: Fraudsters change message headers to make it appear as if they were sent from a real address, such as from a friend, boss or trusted institution.
- Identity Concealment: Messages appear authentic, making them difficult to detect by recipients and anti-spam systems

Distribution of malware and ransomware

Cybercriminals often hijack email accounts to distribute malware.

Action of fraudsters:

- Infected attachments: Emails contain attachments that, when opened, install malware on the victim's computer.
- Malicious links: Emails may contain links to websites that automatically download and install malware on your computer.

Man-in-the-middle (MITM) attacks on email communications

An MITM attack occurs when an attacker intercepts and transmits data between two parties without either party's knowledge.

Action of fraudsters:

- Data interception: Hackers intercept communications to obtain sensitive information such as login credentials or company secrets.
- Spoofing: They can also send messages on behalf of one party, allowing for manipulation of communications.

Email attacks

HAZARD CHARACTERISTICS:

Email takeover or takeover attacks

Hackers try to gain access to your email account by guessing your password or using other methods.

Action of fraudsters:

- Password guessing: Hackers can use techniques such as brute force to guess your password.
- Phishing: They may also use phishing or other social engineering techniques to trick you into providing your login details.

Credential harvesting attacks

Hackers gain access to email accounts by tricking users into providing login details.

Action of fraudsters:

- Phishing: The user receives an email with a fake request for login details.
- Social influence: Hackers pretend to be someone else and ask for a username and password, often using social media information to make their request more credible.

Email attacks

CONSEQUENCES:

Email attacks have a number of serious consequences that can threaten confidential data and online security. To protect yourself, it is important to recognize them.

01 Phishing attacks

- Identity theft: Seniors can provide their login details, credit card numbers, which leads to identity theft.
- Financial Loss: Transmission of data may lead to unauthorized transactions and financial losses.

02 Spear Phishing attacks

- Breach of privacy: Seniors may share confidential information thinking they are communicating with someone they trust.
- Financial and Emotional Losses: Can be manipulated into taking actions that result in financial and emotional losses.

03 Email Spoofing attacks

- Security breach: Seniors may act on false information, leading to security breaches.
- Installation of malware: Clicking on links or attachments may lead to installation of malware.

Email attacks

CONSEQUENCES:

04 Distribution of malware and ransomware

- System Damage: Malware can damage your computer and make it unusable.
- Ransomware: Malware can encrypt files on your computer and demand a ransom to unlock them.

05 Man-in-the-middle (MITM) attacks on email communications

- Loss of confidentiality: Seniors may unknowingly reveal confidential information.
- Manipulation: Attackers can mislead both sides of the communication.

06 Email takeover or takeover attacks

- Identity theft: Hackers can access sensitive information and use it to steal your identity.
- Sending spam: Compromised accounts can be used to send spam and malware.

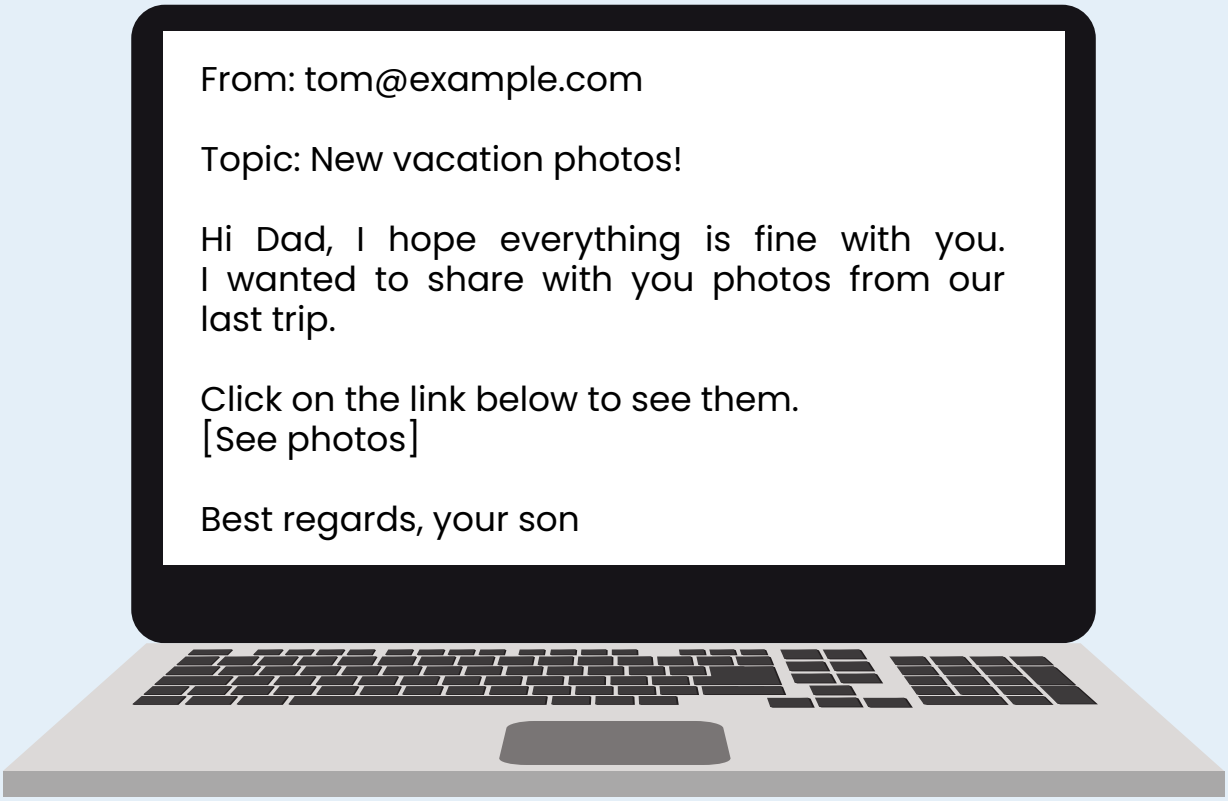
07 Credential harvesting attacks

- Loss of Access: Seniors may lose access to their email accounts.
- Privacy breach: Hackers can gain access to private information and correspondence.

Email attacks

WAYS OF PROTECTION WITH HISTORY IN THE BACKGROUND

Daniel regularly uses e-mail to keep in touch with his family. His son, who lived abroad, often emailed him updates. One day, Daniel received an e-mail that appeared to be sent by his son.



Consequences of not recognizing the threat:

STEP 1: Clicking on the link

Daniel, thinking he had received a message from his son, clicked on the link.

STEP 2: Infect your computer

Clicking on the link downloaded malware that was installed on Daniel's computer. Such software can track your online activity, steal passwords and other confidential information.

Email attacks

— WAYS OF PROTECTION WITH HISTORY IN THE BACKGROUND

Daniel's example shows how dangerous attacks on e-mail boxes can be.

The link in the message led to a website that automatically downloaded and installed malware on his computer.

STEP 3: Infect your computer

The malware was able to gain access to Daniel's personal data, including bank account numbers, passwords to various services and private documents.

STEP 4: Emotional stress

Daniel felt cheated and worried that someone was impersonating his son. The incident caused him great stress and anxiety.

Email attacks

WAYS OF PROTECTION WITH HISTORY IN THE BACKGROUND

You can avoid such consequences by following the methods below to protect yourself against email attacks.

Be careful when opening emails:

Daniel should be careful when opening e-mails:
Action:

- Always check the sender's email address, especially when the message contains links or attachments.
- Read messages carefully and pay attention to unusual requests and grammatical errors.

Antivirus software updates:

Daniel should make sure that his computer and phone have regularly updated antivirus software.
Action:

- Regularly updating antivirus software and scanning the system.
- Installing the latest operating system and web browser updates.

Email attacks

WAYS OF PROTECTION WITH HISTORY IN THE BACKGROUND

Two-Factor Authentication (2FA):

Daniel should consider activating an additional layer of security by using two-factor authentication (2FA) on all relevant accounts. This approach significantly increases the level of security even if the password is revealed.

Action:

- An additional layer of security: Using 2FA on all important accounts, which increases your level of security even if your password is exposed.

It is worth considering 2FA activation:

- when logging into your bank account online to secure access to your funds.
- when logging into your e-mail account, where important information and correspondence are stored.
- when accessing a social media platform, especially when used to communicate with family and friends and share personal photos and information.

By taking these precautions, Daniel can avoid many potential threats related to email attacks and other forms of cybercrime.

Remember my advice, because it will help you feel more confident when using the Internet and protect your personal and financial data against unauthorized access.

Weak password attacks

HAZARD CHARACTERISTICS:

Attacks using weak passwords are one of the most common methods used by cybercriminals.

The main types of attacks on e-mail boxes:

Dictionary attack

A dictionary attack involves testing a large number of potential passwords from a previously prepared list (dictionary). This list often includes common slogans and variations of words. This is an effective method if the user uses easy-to-predict passwords such as "password", "123456", or "qwerty".

Brute force attack

In a brute force attack, the attacker systematically tests all possible combinations of characters until the correct password is found. While this type of attack can take a long time, it can be effective for short and simple passwords.

A credential stuffing attack

This attack uses data collected from previous information leaks, such as logins and passwords. Attackers try to use the same login-password combinations on different websites, counting on the fact that users tend to reuse the same login details on multiple websites.

Phishing attack

While not a direct password attack, phishing is a technique that attempts to trick users into voluntarily revealing their login credentials. Attackers create fake websites that look identical to genuine websites (e.g. banking, email) and send emails encouraging people to log in.

Weak password attacks

CONSEQUENCES:

Attacks using weak passwords have a number of serious consequences for seniors, and can threaten sensitive data and online security. To protect yourself, it's important to know them.

01 Dictionary attack

Seniors who use easily predictable passwords such as "password" or "123456" may fall prey to this attack. As a result, their privacy may be violated and personal or financial data may be stolen.

02 Brute force attack

Elderly people who use short and simple passwords are vulnerable to brute force attacks. Criminals can access their accounts on Wi-Fi, leading to possible data leaks and identity theft.

03 A credential stuffing attack

Seniors who tend to use the same login details on multiple websites are vulnerable to this type of attack. This may lead to unauthorized access to their accounts on various online platforms.

04 Phishing attack

Older adults, who may be less aware of such threats, are susceptible to phishing attacks. Criminals can use fake websites or emails to trick people into obtaining their account login details, which could result in identity theft or financial fraud.

Weak password attacks

WAYS OF PROTECTION WITH HISTORY IN THE BACKGROUND

Anna uses her Facebook account to keep in touch with her colleagues from work. On a daily basis, she publishes photos there, shares important events and coordinates professional projects. Unfortunately, she fell victim to an attack in which her Facebook password was broken and her account taken over by cybercriminals.

Such cases are not uncommon and affect not only seniors, but also professionally active and technologically aware people. Anyone, regardless of age, can fall victim to cybercriminals if they do not take appropriate online security measures.

STEP 1: Using a simple password

Anna used a simple password like "12345678", which made the dictionary attack easier.

STEP 2: No unique passwords

Anna used the same password on many websites. Her password was used on other sites, resulting in a data leak.

Weak password attacks

WAYS OF PROTECTION WITH HISTORY IN THE BACKGROUND

You can avoid such consequences by following the methods below to protect against weak password attacks.

Change your password to a strong and unique one:

Anna should immediately change her Facebook password to a strong, long and unique password that is not used on any other website. The password should contain a mix of letters, numbers and special characters.

Activate two-factor authentication (2FA):

It's a good idea to enable two-factor authentication on your Facebook account, which will provide an additional layer of security. Thanks to this, even if someone knows the password, they will not be able to log in without a second authentication factor, e.g. an SMS code.

Check your security settings:

You should review your Facebook security settings to see if any unknown devices or apps have been added, and log out of all devices. You should also change your security questions if they are set.

Weak password attacks

WAYS OF PROTECTION WITH HISTORY IN THE BACKGROUND

Report an incident to Facebook:

The correct solution is to contact Facebook Support and report that your account has been compromised. Facebook can help you recover your account and protect it from further attacks.

Check out other accounts:

It is worth checking your other accounts on websites where she may have used the same password, and changing the passwords to unique and strong ones. This will prevent further account takeovers.

Phishing education:

It is also good practice to learn how to recognize phishing attempts in order to avoid this type of attacks in the future. Anna should pay attention to suspicious e-mails, links and carefully check the URL addresses of login pages.

Phishing

HAZARD CHARACTERISTICS:

Phishing is a form of cyberattack in which fraudsters try to obtain confidential information. The word "phishing" comes from the English word "fishing", which metaphorically refers to "fishing" for users' personal data.

The four main principles on which phishing is based:

Impersonating trusted sources

- Method: Fraudsters create fake websites, e-mails or messages that appear to come from trusted institutions (e.g. banks, technology companies, government offices).
- Technique: They use logos, colors and communication styles that mimic the original sources.
- Goal: Gain the victim's trust to provide their login credentials or other confidential information

Creating urgent and emotional messages

- Method: Using a sense of urgency or fear to compel the victim to act quickly.
- Technique: Sending a message about an alleged account breach, an outstanding payment, or a special opportunity that requires immediate response.
- Goal: To increase the chance that the victim will act impulsively, without careful consideration.

Phishing

HAZARD CHARACTERISTICS:

Using fake links and attachments

- Method: Sending messages with links to fake websites or attachments containing malware.
- Technique: The links may appear legitimate, but they lead to fake sites that collect login credentials or install malware on the victim's device.
- Purpose: Taking over login credentials, infecting the victim's device with malware or phishing for information.

Social engineering

- Method: Manipulating the victim through the use of psychological deception techniques.
- Technique: Using publicly available information, such as social media data, to create personalized messages. Scammers may also conduct phone calls pretending to be technical support workers.
- Purpose: To create a false sense of security and trick the victim into revealing confidential information.

Phishing

— CONSEQUENCES:

Why is phishing dangerous? The consequences of a successful phishing attack can be severe - from losing money to identity theft to infecting a device with malware. To protect yourself, it's important to know them.

01 Impersonating trusted sources

- Identity theft: Seniors may unknowingly provide personal information that will then be used to open false bank or credit accounts in their name.
- Financial loss: Sharing your bank account login details may lead to unauthorized transactions and loss of savings.

02 Creating urgent and emotional messages

- Unauthorized payments: Seniors can quickly respond to false alerts by providing their bank details and making unnecessary transfers.
- Loss of Savings: Being tempted to make quick decisions can lead to significant financial losses, especially if seniors provide their credit card information to fraudsters.
- Increased vulnerability: Repeated fraud attempts can make seniors more vulnerable to future attacks due to stress and uncertainty.

Phishing

— CONSEQUENCES:

03 Using fake links and attachments

- Device infection: Malware can infect a senior's computer or smartphone, leading to loss of control over the device and access to confidential information.
- Data theft: Malware can capture login credentials, allowing fraudsters to access bank accounts and other confidential resources.
- Repair costs: Removing malware and repairing an infected device may involve high technical costs that seniors may not be prepared for.

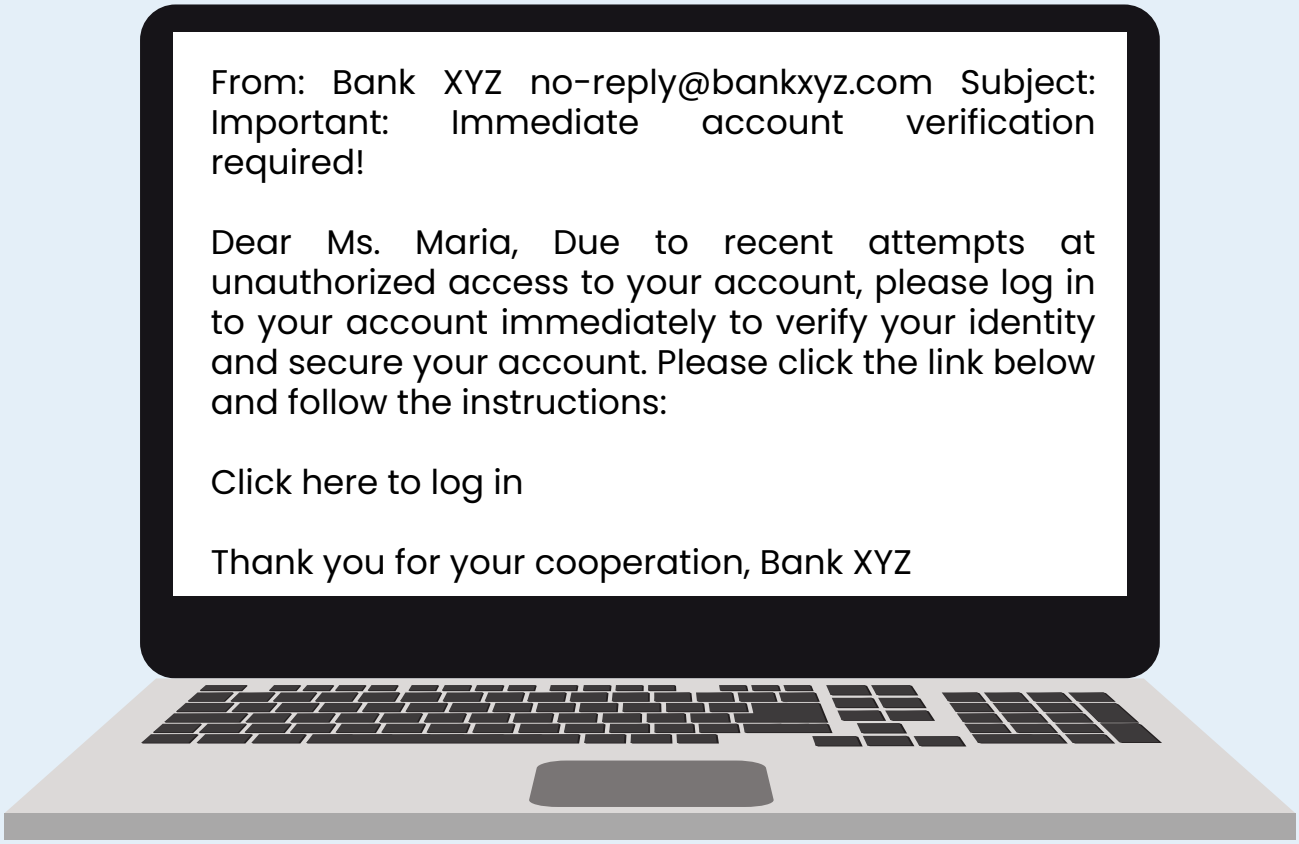
04 Social engineering

- Telephone scams: Seniors can be tricked into providing confidential information over the phone, leading to identity theft and financial loss.
- Loss of trust: Frequent social engineering attacks can lead to a lack of trust in legitimate institutions and people, making everyday life and financial management difficult.
- Emotional manipulation: Psychological effects such as fear, stress and anxiety can negatively impact seniors' mental health.

Phishing

WAYS OF PROTECTION WITH HISTORY IN THE BACKGROUND

Maria regularly uses the Internet to contact her family, check bank accounts and read news. One day she receives an email that appears to be from her bank.



Consequences of not recognizing the threat:

STEP 1: Clicking on the link

Maria, concerned about the content of the e-mail, clicks on the link without carefully checking its authenticity. The link takes her to a page that looks identical to her bank's login page.

STEP 2: Providing login details

Maria enters her login details into the fake website, thinking she is verifying her account.

Phishing

WAYS OF PROTECTION WITH HISTORY IN THE BACKGROUND

Maria's example illustrates a common phishing method of impersonating trusted sources. Let's look at the consequences that may result from Maria's failure to recognize this threat.

STEP 3: Additional attachment

The email also contains an attachment. Maria downloads an attachment that contains malware. Once she opens the file, the malware installs on her computer, allowing fraudsters to remotely access her device.

STEP 4: Data interception and money theft

When Maria clicked on the link, the fraudsters immediately intercepted her login details and gained access to Maria's real bank account.

STEP 5: Stress and anxiety

Maria is devastated by the loss of her savings and is afraid to use online banking and other online services in the future.

STEP 6: Infect your device

The malware on Maria's computer allows fraudsters to monitor her online activities, capture further login details and potentially infect other files.

Phishing

WAYS OF PROTECTION WITH HISTORY IN THE BACKGROUND

You can avoid such consequences by following the methods below to protect yourself against phishing scams.

Checking sender email address and links:

Maria should carefully check the sender's e-mail address and links in the message before clicking.

Action:

- Email address check: Make sure the email comes from the bank's real domain.

Setting up Two-factor authentication (2FA):

Maria should enable two-factor authentication (2FA) on her bank account, which adds an additional layer of security. Even if fraudsters get your password, they also need a second element of authentication, such as an SMS code.

Action:

- 2FA activation: Maria should contact her bank to enable 2FA.

Phishing

— WAYS OF PROTECTION WITH HISTORY IN THE BACKGROUND

Regularly updating antivirus software and operating system:

Maria should ensure regular updates of antivirus software and the operating system to ensure protection against the latest malware and phishing threats.

Action:

- Antivirus software: Maria should install antivirus software and make sure it is always up to date and remember to update it regularly.

By taking these precautions, Maria can reduce the risk of becoming a victim of phishing, protecting her data and finances. Always check the sender's email address carefully and avoid clicking on links or attachments in unexpected emails.

Malware and computer viruses

HAZARD CHARACTERISTICS:

The term malware is used to describe malicious programs designed to damage a computer or perform undesirable actions on it by the user. A computer virus is one of the most serious threats facing computer users. Malware is capable of inflicting tremendous damage - from stealing data to slowing down a system to completely destroying files.

Common types of malware:

Ransomware

A type of malware that blocks access to user data by encrypting it. The cybercriminal demands a ransom in exchange for the decryption key, promising to restore access to the data. However, criminals often renege on the agreement, selling confidential data even after the ransom is paid, and victims may be targeted again.

Trojan

A type of malware that disguises itself as legitimate software to infiltrate a user's device. Once installed, they open access to the device, allowing other types of malware to be installed, spy on users, and steal confidential information. Trojans often spread using social engineering techniques such as phishing and spoofed websites that encourage the user to download a malicious file.

Malware and computer viruses

HAZARD CHARACTERISTICS:

Worms

A type of malware similar to viruses but does not require user interaction to spread. Exploits vulnerabilities in installation and replication devices. Once it infects a device, it tries to connect to other devices on the same network and looks for further vulnerabilities to spread to them.

Spyware

Malware that installs on a victim's device to spy and collect sensitive information such as credentials and credit card numbers. Spyware may be bundled with other programs, or you can install it yourself by clicking on an ad or downloading free software from untrustworthy websites. Once installed, it tracks keystrokes, browsing history, and uses your device's camera and microphone.

Fileless malware

A type of malware that does not use executable files containing malicious code to infect a device. Instead, it makes changes to your device's legitimate system tools, allowing you to perform malicious activities without having to download files to your hard drive. Malicious fileless software code runs directly in the computer's memory, using existing system tools to achieve its goals.

Malware and computer viruses

HAZARD CHARACTERISTICS:

Mobile malware

A type of malware that attacks mobile devices such as smartphones and tablets to access sensitive data. Devices without adequate security measures are vulnerable to these types of attacks because they often lack the default defense mechanisms built into the original operating system.

Viruses

They are a type of malware that infects devices and reproduces to spread to other devices. They usually disguise themselves as malicious files or applications that victims install. Attackers often try to convince users to download these files using phishing attacks. When the victim downloads the infected file or application, the virus activates and starts replicating on the device. It frequently changes files to avoid detection and infects other devices. The virus can steal confidential data, slow down your device, freeze applications, and change and destroy files.

Malware and computer viruses

CONSEQUENCES:

The consequences of being infected with malware are very serious. Cyber criminals are driven by the desire for profit. They use infected devices to launch attacks, such as obtaining credentials for banking services, harvesting personal data for sale, selling access to computer resources or extorting fees from victims.

01 Ransomware

The software may result in loss of access to a senior's important data, such as financial documents or family photos. Moreover, paying the ransom does not guarantee data recovery, which may lead to additional financial losses.

02 Trojan

The software can result in the theft of sensitive information such as bank account passwords or credit card numbers, putting seniors at risk of identity theft and financial loss.

03 Spyware

The software can be used to eavesdrop on seniors' conversations or track their online activities, which violates their privacy and may lead to the use of collected data for blackmail or fraud purposes.

Malware and computer viruses

CONSEQUENCES:

04 Worms

The software can damage the operating system of a senior's device or take control of it by cybercriminals, which may make the device impossible to use or lead to the loss of important data.

05 Fileless malware

The software may run in the background, unnoticeably changing your device's settings or using its resources, which may lead to your device slowing down or causing problems with its performance.

06 Mobile malware

The software can lead to data loss or a violation of a senior's privacy by accessing their personal information or tracking their location.

07 Viruses

Viruses can steal confidential data such as passwords, financial information or personal data, violating users' privacy. They can replicate and spread to other devices on the network, causing further infections and increasing the scale of the problem.

Malware and computer viruses

— WAYS OF PROTECTION WITH HISTORY IN THE BACKGROUND

Alexander was looking through his e-mail. He noticed some news he didn't expect and it made him curious. He clicked on the attachment in this email. He noticed something strange. Something began to change files on his computer, causing significant disruptions to his work. What could have happened?

Cases similar to Aleksander's are unfortunately quite common. Clicking on a suspicious email attachment may lead to your computer being infected with malware. As a result, serious disruptions to operations and data security may occur.

STEP 1: Clicking on the email attachment

Aleksander was browsing his e-mail and, unsuspectingly, clicked on the attachment in the e-mail.

STEP 2: Device infection

Clicking on the fake attachment infected his device with a virus.

STEP 3: Virus replication/multiply

The malicious code (attached) began to quickly replicate on Aleksander's computer, causing changes to files and disruptions in his work.

STEP 4: Possibility of data theft

Additionally, the virus may have had the ability to steal confidential data from Alexander's device, which could lead to further security and privacy issues.

Malware and computer viruses

WAYS OF PROTECTION WITH HISTORY IN THE BACKGROUND

You can avoid such consequences by following the malware protection methods below.

Update your software regularly whenever new suspected threat messages become available, which reduces the risk of infection with malware that exploits these vulnerabilities.

Be careful when opening email attachments and downloading files, especially if they are from unknown senders or seem suspicious.

Avoid clicking on suspicious links or pop-ups as they may lead to infections or data capture.

Malware and computer viruses

WAYS OF PROTECTION WITH HISTORY IN THE BACKGROUND

Use public Wi-Fi networks with caution as they are vulnerable to attacks; consider using a VPN service to secure your internet connection. By using a VPN, your data is encrypted as it travels over public networks, which means that even if someone

Use antivirus and anti-malware programs that help prevent infections and remove malware, including spyware and adware. Antiviruses mainly focus on detecting and eliminating viruses, while antimalware deals with a broad spectrum of malware, including malicious applications that are not classified as viruses.

By following these recommendations, Alexander and other Internet users can avoid threats from malware. Remember not to make decisions too quickly and always act cautiously in the virtual world.

Further Readings

ATTACK VIA WI-FI NETWORKS (PRIVATE AND PUBLIC)

- www.keepersecurity.com/pl_PL/threats/man-in-the-middle-attacks-mitm.html
- www.cdv.pl/blog/blog-ekspercki/najpopularniejsze-rodzaje-atakow-hakerskich/
- www.socialwifi.com/pl/baza-wiedzy/bezpieczenstwo-sieci/najpopularniejsze-rodzaje-atakow-na-wifi/

EMAIL ATTACKS

- www.powerdmarc.com/pl/what-are-email-based-attacks/
- https://www.gov.pl/web/baza-wiedzy/czym-jest-phishing-i-jak-nie-dac-sie-nabrac-na-podejrzane-widomosci-e-mail-oraz-sms-y
- www.keepersecurity.com/blog/pl/2023/08/30/the-most-common-types-of-cyberattacks/

WEAK PASSWORD ATTACKS

- www.keepersecurity.com/blog/pl/2024/01/12/types-of-password-attacks/
- www.securivy.com/blog/brute-force/
- www.keepersecurity.com/pl_PL/threats/dictionary-attack.html

PHISHING

- www.gov.pl/web/baza-wiedzy/czym-jest-phishing-i-jak-nie-dac-sie-nabrac-na-podejrzane-widomosci-e-mail-oraz-sms-y
- www.orange.pl/poradnik/twoj-internet/co-to-jest-phishing-i-jak-sie-przed-nim-bronic/
- www.kwestiabezpieczenstwa.pl/phishing/

MALWARE AND COMPUTER VIRUSES

- www.keepersecurity.com/blog/pl/2024/01/24/twelve-common-types-of-malware/
- www.hackeru.pl/wirus-komputerowy/
- www.powerdmarc.com/pl/types-of-malware/

CHAPTER 2.
FINANCIAL AND INVESTMENT FRAUD

In today's world, seniors are increasingly falling victim to financial scams, which take various forms and are continually being refined by criminals. This chapter aims to highlight the most common types of scams to help seniors recognize threats and protect their savings.

Among the most prevalent methods are financial and investment manipulation, based on false promises of quick profits, and charitable scams that exploit seniors' empathy. Another danger is the promise of large winnings through fake prizes and lotteries, which require payment to claim.

Scams involving digital currencies, like Bitcoin, are also becoming more common, offering a new avenue for criminal activity. It's also important to mention Nigerian scams—international fraud schemes based on fictitious transactions.

Understanding these threats is crucial for seniors to consciously protect their finances.

Financial and investment manipulations

HAZARD CHARACTERISTICS:

Financial and investment manipulation refers to deceptive practices aimed at convincing individuals to invest their money in fraudulent or unsuitable schemes. These schemes often promise high returns but ultimately result in financial loss for the investors.

Types of manipulation in financial investments:

False Promises of High Returns

Scammers use persuasive tactics to promise investors unusually high returns on their investments. These promises may seem too good to be true and often target seniors who are seeking ways to supplement their retirement income.

Pressure to Invest Quickly

Scammers often employ high-pressure sales tactics to pressure individuals into making quick investment decisions without thoroughly researching or understanding the investment products. They may create a sense of urgency by claiming limited-time offers or emphasizing the fear of missing out on lucrative opportunities.

Complex and Confusing Investment Products

Scammers may recommend complex or obscure investment products that are difficult for investors, especially seniors, to understand. These products may involve high fees, hidden risks, or lack transparency about how the invested funds will be used.

Financial and investment manipulations

CONSEQUENCES:

Financial and investment manipulation can have serious negative effects such as:

01 Financial Consequences

Falling victim to financial manipulation can result in the loss of hard-earned savings and investments. You may find yourself with significantly less money than expected, impacting your ability to cover daily expenses and enjoy your retirement.

02 Emotional Impact

Being deceived by financial fraudsters can lead to feelings of betrayal and disappointment. You may feel embarrassed or ashamed that you fell for a scam, impacting your self-esteem and confidence.

03 Personal Consequences

Falling victim to financial manipulation can erode trust in others, making you more cautious and skeptical of future investment opportunities. This loss of trust can strain relationships and make it difficult for you to seek financial advice or support

Financial and investment manipulations

WAYS OF PROTECTION WITH HISTORY IN THE BACKGROUND

Sofia receives an email from an unknown sender claiming to offer a lucrative investment opportunity in a new technology company. The email promises high returns and urges Mrs. Jenkins to act quickly to secure her spot in the investment.
However, Sofia remembers the advice she read about being cautious with unsolicited emails promising big profits.

Sofia's story is unfortunately not the only case, but it shows the importance of protecting seniors from financial manipulation. Seniors should be aware of the various forms of manipulation they may encounter and know methods to avoid them.

STEP 1: Verification

Sofia decides to verify the legitimacy of the investment opportunity before taking any action.

STEP 2: Consultation

Sofia seeks advice from her trusted family member who has experience in finance.

STEP 3: Confirmation

Still skeptical, Sofia decides to contact the company directly to verify the investment opportunity

STEP 4: Report

Sofia decides to report the suspicious email to the relevant authorities.

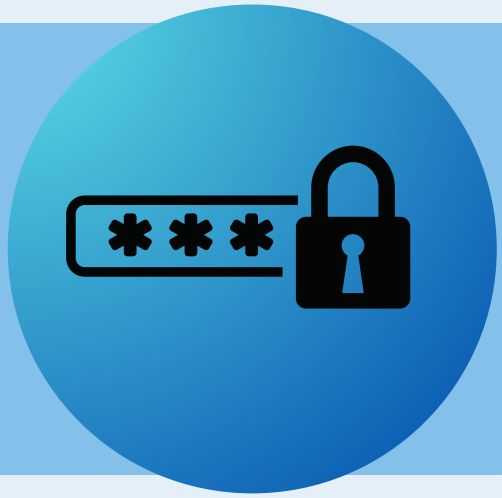
Financial and investment manipulations

WAYS OF PROTECTION:

Protecting yourself from financial and investment manipulation is crucial for safeguarding your hard-earned money. Here are some straightforward steps you can take.

Be careful with email:

If you receive an unexpected email promising big profits or urgent financial deals, it's wise to be cautious. Take a moment to check the sender's email address for any strange signs. And if something feels off, don't click on any links or download any attachments.



Strengthen your passwords:

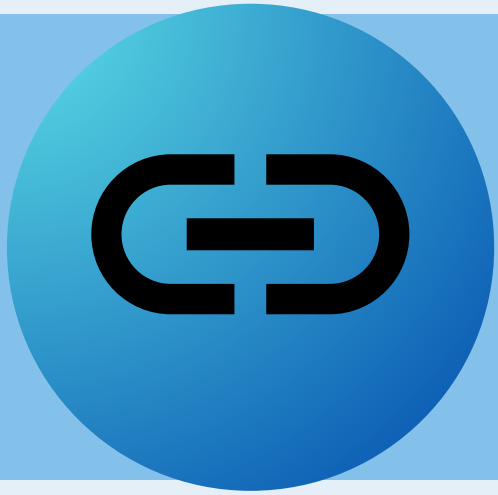
When setting up passwords for your online accounts, make sure they're strong and unique. Use a mix of letters, numbers, and symbols, and avoid using easy-to-guess information like your birthday or pet's name.

Financial and investment manipulations

WAYS OF PROTECTION:

Watch out for suspicious links and websites:

If you come across a website that seems fishy or unfamiliar, don't share any personal or financial information. Look for "https://" and a padlock symbol in the address bar for secure websites.



Stay informed about online safety:

There are plenty of resources and educational materials available to help you learn about common scams targeting seniors.

Lastly, **don't be afraid to ask for help:**

If you're unsure about a financial decision or suspect you've been targeted by a scam, reach out to family members, friends, or trusted professionals for advice and support. And if you believe you've fallen victim to financial manipulation, report it to the proper authorities right away, like the Federal Trade Commission or your state's consumer protection agency.

Apparent altruism: charity fraud

HAZARD CHARACTERISTICS:

Charity scams on the internet often prey on the generosity and goodwill of individuals, particularly targeting seniors aged 65 and above. These scams may involve fake charities posing as legitimate organizations, soliciting donations for supposed causes such as disaster relief, medical research, or helping the less fortunate.

Types of manipulation in Charity Scams:

High-pressure tactics

Scammers may use persuasive language or emotional appeals to pressure victims into making donations quickly.

Impersonation of legitimate charities

Fraudsters may create fake websites or send emails that mimic the branding of well-known charities to deceive victims.

Fake stories and testimonials

Scammers may fabricate heart-wrenching stories or provide fake testimonials to elicit sympathy and encourage donations

Lack of transparency

Fake charities often provide vague or misleading information about their mission, goals, and how donated funds will be used.

Apparent altruism: charity fraud

CONSEQUENCES:

Falling victim to charity scams can be very hard for seniors, both financially and emotionally.

01 Financial loss

Falling victim to charity scam can result in the loss of hard-earned savings and investments. You may find yourself with significantly less money than expected, impacting your ability to cover daily expenses and enjoy your retirement.

02 Emotional distress

Being manipulated into charity fraud can make you feel betrayed, guilty, and embarrassed of falling a victim to this fraud

03 Trust issues

It can also make it difficult to trust real charities in the future, because it becomes harder to tell the difference between genuine and fake appeals.

Apparent altruism: charity fraud

WAYS OF PROTECTION WITH HISTORY IN THE BACKGROUND

Alice receives an email claiming to be from a charity organization seeking donations to help children in need. The email includes emotional stories and photos of children purportedly benefiting from the charity's work.
However, Alice remembers the advice she read about being suspicious with emails promising to donate money to charities.

Alice's story is unfortunately not the only case, but it shows the importance of protecting seniors from charity scams. Seniors should be aware of the various forms of scams they may encounter and know methods to avoid them

Step 1: Research the charity

Before donating Alice checks the charity's registration status and reviews on reputable websites

Step 2: Be cautious of unsolicited requests

Alice questioned this unexpected email asking for donations.

Step 3: Never share personal information

Alice avoided to provide sensitive information like Social Security numbers or banking details to unknown or unverified charities.

Step 4 : Donate directly

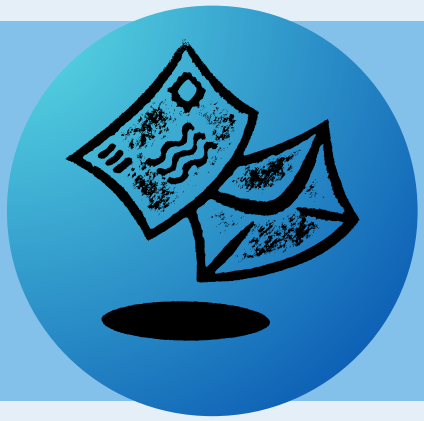
If Alice wants to donate, Instead of clicking on links in emails or responding to phone calls, she donated directly through the charity's official website

Apparent altruism: charity fraud

WAYS OF PROTECTION:

Protecting yourselves charity scams and it's consequences is very crucial. Here are some simple steps you can adopt to prevent yourself from falling victim to the charity fraud

Research charities by checking their status and reviews on legitimate charity websites.



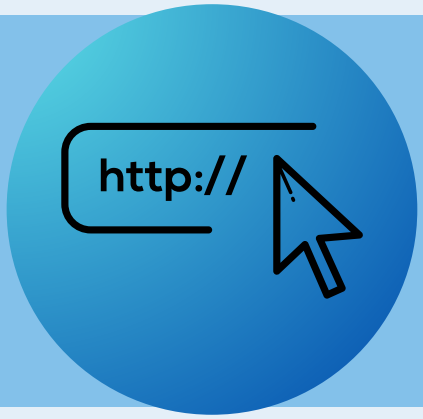
Be cautious of unexpected requests for donations through emails, phone calls, or social media, as real charities don't usually use high-pressure tactics.

Never share personal information like Social Security numbers or banking details with unknown charities.

Apparent altruism: charity fraud

WAYS OF PROTECTION:

Donate directly through the charity's official website or by mailing a check to their verified address.



Stay informed about common charity scams and learn to recognize warning signs.

Don't hesitate to ask family, friends, or financial advisors for help when evaluating charity requests or if you suspect a scam.

Tempting illusions: fictitious prizes and sweepstakes

HAZARD CHARACTERISTICS:

Scams based on fake prizes, lotteries, and sweepstakes are deceptive and deliberately exploit people's desire to win by convincing them that they have won big prizes. Scammers solicit victims to pay them fake winnings but end up stealing money from the victim's wallet.

Types of manipulation in fictitius prizes and sweepstakes:

Impersonation

Scammers often impersonate representatives of renowned companies or lotteries managed by governments (especially foreign ones) and use manipulative tactics to exploit their victim's trust hoping to take advantage of their desire for financial security.

Exclusivity

Scammers try to convince victims that they have been chosen as the only or rare lucky winners in order to create a sense of uniqueness and exclusive opportunity for the victim.

Unrealistic promisses

Scammers promise unrealistic amounts of prize money, luxury products, etc. that are too good to be true, using pressure tactics to get victims to react immediately and in confidence.

Tempting illusions: fictitious prizes and sweepstakes

CONSEQUENCES:

The consequences of “tempting illusion” scams are varied and often long-lasting.

01 Financial Consequences

One of the worst consequences of such scams is financial devastation for the victims, and most victims often suffer significant financial losses. Victims may lose their life savings, become over-indebted, or even go bankrupt. Recovery from such financial situations can take years.

02 Emotional Concequences

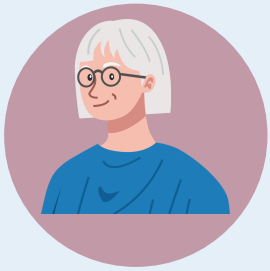
Victims of scams often experience deep emotional distress and struggle with feelings of betrayal, violation, shame, and guilt. The emotional turmoil caused by deception and fraud can lead to anxiety, depression, and even post-traumatic stress disorder (PTSD) and can also affect physical health.

03 Legal Consequences

In cases of scams where victims are persuaded to cash phony "prize cheques”, they can even face legal consequences, including money laundering and forgery charges, in addition to financial loss.

Tempting illusions: fictitious prizes and sweepstakes

WAYS OF PROTECTION WITH HISTORY IN THE BACKGROUND



Greta, received an unexpected text message informing her that she had won a jackpot in a foreign lottery and should immediately pay an upfront *'administration fee'* to claim her prize money.
The message also made it clear that she was not to share information about her lottery win and the procedures for receiving her prize with anyone.

Unfortunately for the scammer ...

Greta recently attended a cyber security, course, which included sessions on online scams.

STEP 1: Recognizing warning signs

Greta immediately spotted the signs of the scam: an *unexpected message, a lottery win* (for which she had not bought a ticket) and *a request for advance payment.*

STEP 3: Avoiding involvement

Greta did not respond to the text message, thus protecting her personal data and avoiding financial loss.

STEP 2: Identifying other scam strategies

Greta recognized the instruction *not to share details of her lottery winnings with others* as a tactic to isolate her and make it easier for her to fall for a scam.

STEP 4: Reporting

Greta immediately informed her family, friends and the relevant authorities about the attempted scam and shared the information on social media.

Tempting illusions: fictitious prizes and sweepstakes

WAYS OF PROTECTION:

If you come across an attempted *"Tempting Illusion"* type of scam, the first thing to remember is that there is no free money, and keep in mind the well-known saying: *"If something looks too good to be true, it probably is."* Here are some additional tips in case you might find yourself in such a situation.

Use common sense:

Resist the urge to act quickly on unexpected prize notifications that you have received either via email, social media, or text message!

Before taking any action, consider whether you have even participated in any sweepstakes or lottery.

Check legitimacy:

Check the website or the sender of the notification through other channels.

Do an internet search or consult with family or friends to check credibility!

Don't click or tap on links in notifications, especially if they are suspicious!

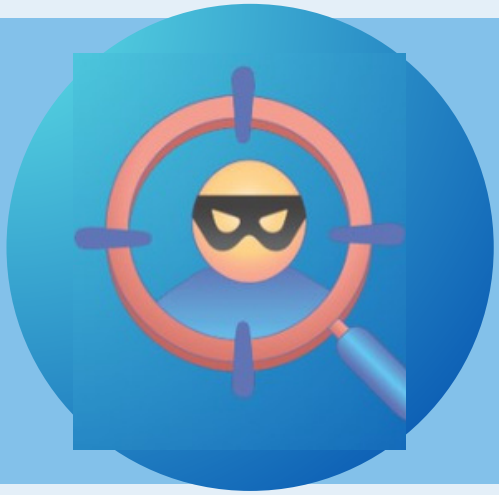
Tempting illusions: fictitious prizes and sweepstakes

WAYS OF PROTECTION:

Examine the details:

Carefully check all the information you have received in the notification.

Be aware of any unclear or unusual requests, such as requests for personal details, financial information, or payment in advance!



Remember:

Do not ever send money or pay a fee to collect a prize/money on an unexpected prize-winning notification!

Legitimate sweepstakes don't require any payment to enter or claim a prize, and participation in lotteries necessitates purchasing a ticket.

Tempting illusions: fictitious prizes and sweepstakes

WAYS OF PROTECTION:

If you have disclosed your personal or financial details to a scammer, you should immediately **change the passwords of your email account and all other accounts.** Also, **change the PINs** on your bank accounts, and if you use online banking, **don't forget to change your online banking password.**

Use strong passwords with a combination of upper and lower case letters, numbers, and special character!

If you have opened a suspicious link and shared your financial or personal information or had a loss, report it immediately to the appropriate authority in your country!

Digital currency scams

HAZARD CHARACTERISTICS:

Cryptocurrency fraud refers to any fraudulent activity associated with digital currencies, such as Bitcoin. It can take many forms, including scam initial coin offerings (ICOs), Ponzi schemes, and fraudulent investment opportunities. These scams typically promise high returns to lure in victims, who then lose their investment when the fraudsters disappear with the funds. Seniors are particularly vulnerable to these types of fraud due to their unfamiliarity with digital technologies and the internet. Fraudsters often exploit seniors' trust and financial security, making it essential to raise awareness and provide education to protect them from such scams.

Types of cryptocurrency fraud:

Scam Initial Coin Offerings (ICOs)

This type of fraud takes place during the fundraising stage of new cryptocurrencies. Developers present a promising new digital currency, often with a detailed whitepaper and high return promises. Unfortunately, once they collect enough funds from investors, these developers vanish without a trace, leaving investors with worthless tokens.

Ponzi Schemes

These schemes promise high, low-risk returns. However, returns are paid using funds from new investors, not from profits. The scheme collapses when there are not enough new investors, causing significant losses for the last investors.

Fake Wallet Scams

This type of fraud involves apps or software that claim to safely store cryptocurrencies. These wallets often have professional-looking interfaces and may even mimic legitimate wallets. However, they are actually designed to siphon away digital currencies. Once a user deposits their cryptocurrencies into these fake wallets, the scammers gain access to them, often resulting in the complete loss of the user's digital assets.

Digital currency scams

CONSEQUENCES:

Financial and investment manipulation can have serious negative effects such as:

01 Financial Loss

The most immediate and apparent consequence of cryptocurrency fraud is financial loss. Victims often lose their entire investment, which can be devastating, especially if they've invested a large portion of their savings.

02 Loss of Trust

Victims of cryptocurrency fraud often lose trust in digital currencies and may be hesitant to invest or participate in the digital economy in the future. This can hinder the growth and acceptance of cryptocurrencies.

03 Legal Consequences

In some cases, participants in fraudulent schemes, even unknowingly, may face legal consequences. This can include investigation by regulatory authorities and potential charges if they have unknowingly helped facilitate the fraud.

Digital currency scams

WAYS OF PROTECTION WITH HISTORY IN THE BACKGROUND

One day, Helen received an email. It was an invitation to invest in a new cryptocurrency that promised significant returns. Intrigued and eager to grow her digital portfolio, decided to investigate.

The email was from a company called "CryptoGold," and their website was impressive, replete with testimonials from satisfied investors and promises of high returns. The opportunity seemed too good to pass up, so she decided to invest a small portion of her savings.

Days turned into weeks, and Helen eagerly checked her online wallet every day, hoping to see her investment grow. But, instead, she noticed that her investment was dwindling. Confused and worried, she tried reaching out to "CryptoGold." However, all her emails bounced back, and the once impressive website was now inaccessible.

Hellen's story underscores the need to protect seniors from cryptocurrency scams by raising awareness and education. Seniors can be vulnerable due to digital unfamiliarity and thus need to understand the risks, signs of scams, and importance of skepticism towards high-return promises. Supportive networks are also crucial for safe digital navigation.

STEP 1: Research the company

Hellen should have thoroughly researched "CryptoGold" before investing. Instead of being impressed by the website and testimonials, she should have checked if the company was registered and looked for reviews or warnings from other users.

STEP 2: Verify communication

Hellen received an unsolicited email and trusted it without verification. She should have been cautious and validated the sender's identity by cross-checking with trusted sources, such as official company contact information or known cryptocurrency forums.

STEP 3: Avoid immediate decisions

Hellen quickly decided to invest without taking the time to fully understand the terms and risks involved. She should have avoided making hasty investment decisions and sought advice from knowledgeable individuals or financial advisors.

STEP 4: Monitor investments regularly

Hellen did not notice any immediate signs of fraud and kept hoping for positive returns. She should have regularly monitored her investments and immediately flagged any unusual activity or lack of transparency for further investigation.

Digital currency scams

WAYS OF PROTECTION:

Protecting yourself from cryptocurrency fraud is crucial, especially for seniors, because they can be particularly vulnerable due to unfamiliarity with digital technologies. Fraudsters often target seniors with promises of high returns, exploiting their trust and financial security. Falling victim to these scams can result in significant financial loss, loss of trust in digital innovations, and potential legal consequences. Educating oneself, conducting thorough research, and maintaining a healthy skepticism towards too-good-to-be-true offers are essential steps in safeguarding one's assets and ensuring financial well-being.

Education:

Understanding how cryptocurrencies work is the first step to avoiding fraud. This includes understanding the technology behind it, how transactions work, and how to securely store and protect your digital assets.

Research:

Before investing in any cryptocurrency, thoroughly research the digital currency, the team behind it, and read any available whitepapers. Be wary of new cryptocurrencies that promise high returns with little risk.

Digital currency scams

WAYS OF PROTECTION:

Secure your wallet:

Protect your digital assets by using a secure wallet. This could be a hardware wallet that stores the currency offline or a reputable online wallet with strong security measures. Always enable two-factor authentication if available.

Be skeptical:

Be skeptical of any investment that promises high returns with little to no risk. These are often too good to be true. Remember that legitimate investments typically do not guarantee returns and always involve some level of risk.

Report suspicious activity:

If you come across a potential cryptocurrency scam, report it to your local authorities and any relevant online platforms. This not only helps protect you, but also helps to alert and protect others.

International financial fraud

HAZARD CHARACTERISTICS:

The 419 scam, also known as the Nigerian scam, is a notorious advanced fee fraud that originated in Nigeria, running from the earliest days of the Internet, and has become one of the most widespread scams globally.

Types of manipulation in 419 scam:

Impersonation *(variation 1)*

With the word "Greetings" in the subject line, you will be greeted by a wealthy Nigerian prince, (even a Nigerian astronaut), wealthy lawyer or businessman and offered a large sum of money to help him transfer his money out of Nigeria (or enable him to access the account) in exchange for a small upfront payment to cover the alleged transaction costs.

Impersonation *(variation 2)*

With the word "Greetings " in the subject line, you will be greeted by a person who is facing a difficult life situation, such as the kidnapping of that person's children; or a person who, because of the political situation, has become a fugitive or an innocent prisoner, etc. However, they all share a long and sad story about why they cannot collect their money, so they are asking for your help.

International financial fraud

Behind Nigerian scams are professional scammers who use a systematic approach and tried-and-tested techniques to manipulate human emotions and vulnerabilities. They employ a pre-prepared playbook, known in Nigerian fraud as a "script" or "format." This often includes elaborate stories, false identities, and forged documents that appear legitimate and are simply copied and used by scammers in their communication with victims.

Playing on human emotions

In the Nigerian scam, communication takes place exclusively via email, text messages or social networks. In this type of scam, scammers do not communicate with victims via video or telephone. The received messages contain grammatical errors and poor text formatting.

Exclusive use of written digital communication

Once the victim no longer provides money or personal information or realizes it has been scammed, the scammers immediately stop responding to correspondence and simply disappear.

Disapperance

International financial fraud

— CONSEQUENCES:

This scam can endanger people of all ages, especially those who believe in get-rich-quick schemes or are financially naive. However, seniors are even more vulnerable, as they typically trust others more and know less about online security.

01 Financial Consequences

Victims can lose large sums of money, leading to serious financial problems. When victims respond positively, they fall into the trap of being asked for more and more money by the scammers, who make up all sorts of false excuses or proposals for extra payments. In this case, the *Sunk Cost Fallacy* can also appear, where victims continue to pursue something they have already invested heavily in (whether it's money, time, effort, emotional energy, etc.), even though giving up would be a much better idea.

02 Emotional Concequences

When shame or embarrassment encourages secretive behavior, it can often lead to victims being scammed repeatedly.

03 Social Consequences

After being scammed, a person's trust in other people can be greatly diminished, leading to isolation and difficulties in maintaining and forming relationships.

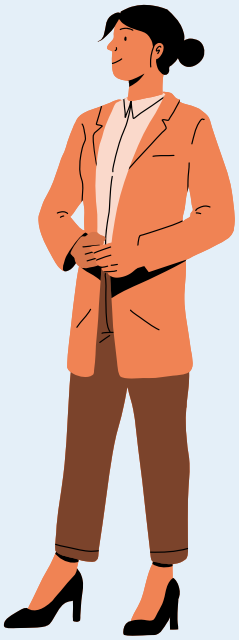
International financial scam

WAYS OF PROTECTION WITH HISTORY IN THE BACKGROUND

Emma was surfing the web when she received an email titled *"Greetings".* The email's sender was a *Nigerian "prince"* who needed her help transferring a large sum of money from Nigeria. In return, she would have received a percentage of the funds for her assistance, in exchange for a small fee to facilitate the transaction.
Despite the tempting offer, Emma became suspicious!

Unfortunately for the scammer ...

Emma recently read an online article about 419 scams and learned about all variations of the scam.



STEP 1: Recognizing warning signs in communication
Emma noticed that the content of the email was written in very poor English and made no sense at all.

STEP 2: Using knowledge
Emma also learned while reading an online article about 419 scams that there are no royal families in Nigeria.

STEP 3: Taking decisive action
Emma immediately flagged the email as spam and deleted it. She did the same with other follow-up emails, that came from the "alleged" Nigerian prince.

STEP 4: Fostering a community of informed and vigilant individuals
Emma shared her experience with her husband, family, and friends. and shared the information on social media.

International financial fraud

WAYS OF PROTECTION:

If you come across an attempted 419 type of scam, the first thing to remember is that nobody has gotten a large sum of money because of an unexpected message in their inbox!

Here are some additional tips in case you might find yourself in such a situation.

If you receive a 419 scam offer and you are tempted to accept it, **stop** and ask yourself these **two simple common-sense questions:**

Why would you share your personal and financial information with a complete stranger (coming from a country you have no connection with), and **why would this stranger choose you to share a fortune with?**

Even if you are moved to the depths of your heart, by the story *"of child abduction"*, **never send money** (or other financial information) before checking the authenticity of the person asking you for financial help!

Keep also in mind that 419 scams lure you to pay via wire transfer services! (usually Western Union)

International financial fraud

WAYS OF PROTECTION:

Examine the authenticity of the content:

As 419 scammers repeatedly use scripts, you can check the authenticity of an email by simply **inserting a short part of the content into a search engine** (Google, Bing, etc.). If the content is part of known or uncovered scam messages, you will find websites that warn about this scam that have already been reported by other victims.

Do not reply to scam e-mails (not even as a joke)!

Delete them immediately!

Remember if you reply - you'll be most probably caught in a financial trap!

International financial fraud

WAYS OF PROTECTION:

If you have disclosed your financial details to a scammer, **change your PINs and login password** (if you use online banking).

Take additional security measures for financial transactions, such as **two-factor authentication** (2FA) and the **transaction alert function** and **monitor your account balance regularly.**

If you have suffered a financial loss, report it immediately to your bank and other appropriate authorities in your country!

Further readings

FINANCIAL AND INVESTMENT MANIPULATIONS

- https://faircanada.ca/investing-basics/protecting-vulnerable-investors-from-financial-abuse/
- https://economictimes.indiatimes.com/wealth/legal/will/how-can-senior-citizens-protect-themselves-from-financial-exploitations-by-their-own-families/articleshow/103877992.cms?from=mdr
- https://www.morganstanley.com/articles/elder-financial-abuse-protecting-loved-ones
- https://www.ncbi.nlm.nih.gov/pmc/articles/PMC6044329/
- https://www.psychiatrist.com/pcc/financial-abuse-older-adults-screening-prevention-interventions-primary-care-providers/
- https://www.youtube.com/watch?v=7G8lil8Yupg
- https://www.c-span.org/video/?324176-1/financial-exploitation-senior-citizens

APPARENT ALTRUISM: CHARITY FRAUD

- https://www.bbc.com/news/uk-34530586
- https://www.youtube.com/watch?app=desktop&v=MTm-fq0OUQQ
- https://www.americanseniorallliance.com/episode_5
- https://www.youtube.com/watch?v=vR53sRLVgpc
- https://www.theguardian.com/society/2015/sep/01/charities-face-scrutiny-over-trading-of-elderly-mans-data

Further readings

TEMPTING ILLUSIONS: FICTITIOUS PRIZES AND SWEEPSTAKES

- https://www.identityguard.com/news/lottery-scams
- https://www.pcrisk.com/ https://www.naperville.il.us/services/naperville-police-department/community-education-and-crime-prevention/frauds-and-scams /
- https://www.scamwatch.gov.au/system/files/Little%20Black%20Book%20of%20Scams%20-%20Final.pdf
- https://www.gamblingcommission.gov.uk/public-and-players/guide/lottery-scams-and-fraud
- https://www.identityguard.com/news/online-safety-tips-for-seniors
- https://www.liveabout.com/warning-signs-of-sweepstakes-scams-886996
- https://surfshark.com/research/data-breach-impact/crime-lottery-inheritance-scam https://www.aura.com/learn/sweepstakes-scams

DIGITAL CURRENCY SCAMS

- https://www.consumer.ftc.gov/articles/what-know-about-cryptocurrency-and-scams https://www.coindesk.com/learn/crypto-scams-types-of-crypto-schemes-and-how-to-avoid-getting-scammed
- https://www.fastex.com/en/learn/crypto-scams-explained
- https://cointelegraph.com/explained/impersonation-scams-in-crypto-explained https://www.ftc.gov/news-events/news/press-releases/2022/06/new-analysis-finds-consumers-reported-losing-more-1-billion-cryptocurrency-scams-2021
- https://www.mdpi.com/2227-9091/11/3/51
- https://www.cybertrace.com.au/cryptocurrency-fraud-explained
- https://www.arkoselabs.com/guide-to-cryptocurrency-security
- https://www.ftc.gov/news-events/news/press-releases/2023/03/ftc-new-analysis-reveals-consumers-lost-nearly-500-million-cryptocurrency-scams
- https://www.kaspersky.com/resource-center/threats/top-seven-tips-for-preventing-cryptocurrency-scams

Further readings

INTERNATIONAL FINANCIAL FRAUD

- https://www.altospam.com/en/glossary/scam-nigerian419/
- https://www.comparitech.com/identity-theft-protection/nigerian-scam/
- https://www.comparitech.com/identity-theft-protection/nigerian-scam/
- https://www.britannica.com/topic/cybercrime/Identity-theft-and-invasion-of-privacy#ref829190
- https://www.wallstreetmojo.com/nigerian-scam/#nigerian-letter-scam-explained
- https://whatismyipaddress.com/nigerian-fraud-combines-scams
- https://hackernoon.com/the-nigerian-prince-email-and-the-history-of-social-engineering-techniques
- https://www.cnbc.com/2019/04/18/nigerian-prince-scams-still-rake-in-over-700000-dollars-a-year.html

CHAPTER 3.
SOCIAL MANIPULATION AND EMOTIONAL DECEPTION

Modern scams increasingly take the form of social and emotional manipulation, making seniors particularly vulnerable to these threats. Criminals exploit emotions, trust, and naivety to achieve their goals, often ruining the financial and emotional well-being of their victims. This chapter aims to discuss the most common scams based on emotional and social manipulation, helping seniors recognize and protect themselves from these dangers.

Among the most dangerous are romantic scams, where criminals build relationships to extort money. Smishing and phone scams also pose serious threats, as scammers impersonate trusted individuals or institutions to obtain personal information or funds.

Grandparent scams, where fraudsters pose as family members, and scams involving medical products are additional methods of manipulation.
Understanding these threats is crucial for protecting the financial and emotional well-being of seniors.

Fraud in male-female relationships

HAZARD CHARACTERISTICS:

An online dating scam, also known as a romance scam, occurs when a victim is deceived into believing they are in a romantic relationship with someone they met online. However, their supposed partner is a scammer.

Types of manipulation in an online romance:

Fake identity

Scammers create fake online profiles and present themselves as being far away from the victim, most often abroad, on a mission (doctor, soldier, philanthropist), working on an oil rig, etc.

Perfection

Scammer's interests and hobbies are almost exactly the same as victims ... and the photos are just ... WOW! Although apart from a few "perfect photos", there are not many (or any) other photos of him/her in various situations in life.

Fast progress

Once everything is looking rosy (declaration of love, proposal, etc.), the scammer invites victims to communicate privately (thus obtaining their phone number, email address, and other information) and promises to see them in person soon.

Request for... MONEY

And just when everything is looking even rosier along comes the request for money, accompanied by a story that evokes empathy and a request for specific payment methods (wire transfer, a newly established bank account in the victim's name, etc.).

Fraud in male-female relationships

— CONSEQUENCES:

Romantic scams can lead to severe financial losses and significant emotional distress for victims.

01 Financial Consequences

Because victims often believe they are helping a loved one in need, they are willing to use their money and invest it in the relationship. For the sake of "love" some victims even sacrifice their entire savings, take out additional loans, or even sell their assets. The data that scammers obtain from victims (bank account, credit card information) can be used to make unauthorized transactions or withdrawals, leading to significant financial losses.

02 Emotional Concequences

Online dating fraud is especially cruel since it plays on people's emotions. The revelation that an online relationship is a scam causes similar emotional damage to the victim as the sudden end of a relationship based on physical interaction. This often makes it difficult for victims to break the affection they feel for the scammer, even when they realise that they have been scammed.

03 Legal Consequences

Victims of romantic scams are prone to psychological pain such as shame, embarrassment, stress, anxiety, depression and fear. Victims may experience symptoms resembling major depressive disorder, grief or post-traumatic stress disorder (PTSD).

Fraud in male-female relationships

— WAYS OF PROTECTION WITH HISTORY IN THE BACKGROUND

Two years after her husband's death, Margot's grandchildren convinced her to sign up for an online dating site. Soon, she began chatting with a man named Tom, a doctor on a humanitarian mission in Africa.

After a few weeks of heartfelt conversations, Tom claimed he had *'Cash flow problems'* and needed money to cover the expenses. Margot became suspicious and discussed the unusual request with her grandchildren. Together, they investigated his profile and discovered that Tom was a scammer.

Unfortunately for the scammer ...

Margot made the right decision when she spoke openly to her loved ones about her suspicions of a scam.

STEP 1: Following intuition
Margot sensed something was wrong. She trusted her instincts and didn't rush to help him, but first thought about the strangeness of his request.

STEP 2: Looking for advice from trusted people
Instead of making the decision herself Margot consulted her grandchildren. She shared the details of Tom's request with them and sought their advice.

STEP 3: Investigating
Together they investigated Tom's profile and found out that he was a scammer. This realization prevented Margot from sending him money and falling victim to his scam.

STEP 4: Reporting
Margot informed the dating site, contacted the site administrator, and reported Tom for suspected scamming.

Fraud in male-female relationships

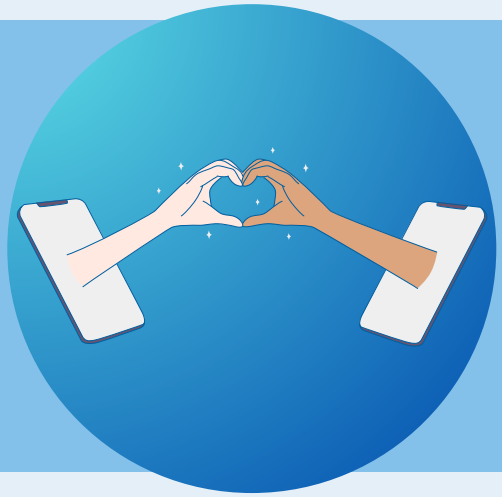
WAYS OF PROTECTION:

Romantic scammers exploit the loneliness of seniors, especially recently widowed or divorced, taking advantage of their vulnerability and financial resources to develop fake online romantic relationships on social media platforms, dating websites, etc.

Here are some additional tips in case you might find yourself in such a situation.

Be careful what you share online:

The information you share publicly (your interests, hobbies, lifestyle, etc.) can be used by scammers to create a fake persona to attract your romantic interest.



In any online relationship, keep your personal/financial information to yourself:

Don't share too much personal information with a potential online romantic partner, and certainly don't disclose your financial information.

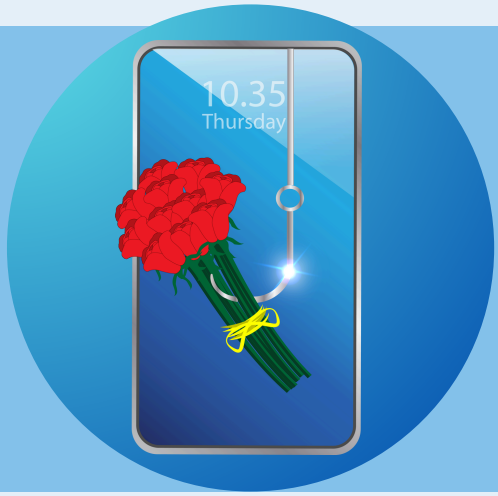
But most of all - **Don’t send money or buy valuables to anyone you’ve never met!**

Fraud in male-female relationship

WAYS OF PROTECTION:

Verify:

While you can't verify everything a romantic online partner tells you, you can check certain concrete details by **using the Internet to verify** their name, surname, place of residence, profiles on social media, **authenticity of posted and sent photographs, and check if they use recycled backstories or expressions** in communication, as scammers often reuse the same backstories and lines repeatedly.



Remember!

If your romantic online partner **refuses to meet you face-to-face, makes up excuses why he/she can't meet, or never takes part in a video call or other forms of live "interaction",** it might be that you have become involved with a scammer.

Fraud in male-female relationship

WAYS OF PROTECTION:

If you have shared passwords to your accounts and have detected suspicious activity, **check immediately if any settings have been changed**, and **check the last logins and activity on your accounts**. If you notice any unknown or suspicious logins, **inform your service provider** and **your contacts** and warn them to be alert for suspicious messages that may appear to be coming from you.

The best advice is to change all passwords you have given access to!

If you suspect your online relationship is a scam**, stop communicating immediately** and **block the scammer** on social media, email, messaging apps, dating websites, **etc.**

If your bank or credit accounts were used contact the bank or the police!

Spread the word!

Smishing SMS-scams

HAZARD CHARACTERISTICS:

Smishing is a portmanteau of "SMS" (short message service) and "phishing." In these attacks, cybercriminals send fraudulent text messages and attempt to trick or manipulate victims into divulging personal or financial information, taping on malicious links, or downloading harmful software or apps.

Types of manipulation in smishing:

Impersonation

Scammers deceive victims by impersonating legal institutions, businesses, or other organizations through text messages. These messages prompt victims to take immediate action, such as tapping on a link in the message, replying with personal information, or dialing a specified number.

Possible and plausible context

Using a situation that could be relevant to victims (message from the bank, credit card services, customer support, etc.) allows scammers to build an effective disguise and helps them override any suspicion that it might be spam.

Playing on emotions

By intensifying a victim's emotions the message feels personalized and triggers a specific emotion response, such as urgency, fear, or curiosity. Employing these tactics, scammers craft messages designed to prompt victims into taking immediate action.

Smishing-SMS scams

CONSEQUENCES:

Due to their limited experience with modern technologies and cybersecurity knowledge, seniors often find it difficult to recognize signs of danger in smishing messages, such as false calls to action or suspicious links. They tend to be less suspicious and more likely to believe deceptive smishing messages.

01 Financial Consequences

If victims disclose their personal or financial information, such as credit card numbers or bank account numbers, they can suffer more financially as scammers use this information to carry out unauthorised transactions or withdraw money from the victim's account. These consequences can cause serious financial problems and long-term damage.

02 Identity Theft

In the event of identity theft, your personal data is misused, which affects your personal security and privacy. If it becomes associated with illegal activities, you may also face legal consequences. Getting your identity back can be very time-consuming as it involves many administrative (as well as legal) procedures.

03 Psychological Consequences

Smishing messages often exploit emotions such as fear, panic or confusion, which can affect the psychological well-being of victims.

Smishing SMS-scams

— WAYS OF PROTECTION WITH HISTORY IN THE BACKGROUND

Peter received a text message on his smartphone from his bank notifying him that his account had been temporarily blocked. The message contained an unusual request that he should IMMEDIATELY tap on a link to activate his account.
Although Peter panicked for a moment, he decided not to click on the link because he found the message very suspicious.

Unfortunately for the scammer ...

Peter recently watched an online educational video about smishing and learned to recognize the features of this type of scam.

STEP 1: Recognizing warning signs
Peter also noticed spelling mistakes or awkwardly phrased sentences in the message, which indicated that the message was not authenticated.

STEP 2: Noticing lack of personal contact
Peter also noticed that the message was anonymous and did not contain the bank's details or a contact person the client could contact for further information.

STEP 3: Verifying information
Instead of tapping the link, Peter called the bank, using the phone number from his phonebook, and checked with the bank whether the message was real.

STEP 4: Informing/reporting
After Peter informed the bank, which confirmed the attempted scam, the bank informed all its clients and reported the attempt of scam to the relevant authority.

Smishing SMS-scams

WAYS OF PROTECTION:

It's easy to protect yourself from the potential consequences of these attacks - just ignore them. Of course, you should not ignore all messages, as text messages are a legitimate tool for many retailers and other institutions to reach you.

Here are some additional tips in case you might find yourself in such a situation.

Do not respond:

If you receive an unexpected or suspicious text, even requests to respond, like texting "STOP" to unsubscribe, it can be a tactic used to identify active phone numbers and lead to scam.

- Example 3

Do not panic:

Take your time and slow down if a message seems urgent.

Treat URGENT account updates or URGENT limited-time offers as potential indicators of smishing.

Stay cautious!

Smishing SMS-scams

WAYS OF PROTECTION:

Do not use links or contact information provided in the message!
Verify, check, and reach out directly through official communication channels, not through the details or information provided in the text.

Keep in mind!
Legitimate institutions (e.g. banks, government departments, etc.) never request sensitive data via SMS or uncertified connections.

If you suspect an attempted smishing attack, **change all your account passwords and PINs immediately.**

Additionally, **monitor your finances and online accounts** for unusual login locations or any suspicious activities.

If you are a fall victim of smishing, contact the relevant institutions that can help you immediately. In the event of a financial attack, contact your bank to freeze your account or cancel your credit cards.

Telephone scams involving the elderly

HAZARD CHARACTERISTICS:

Telephone scams, also known as vishing, are particularly effective against the elderly. Typical tactics include unexpected calls from unknown or foreign numbers, fake numbers, or platforms like Viber and WhatsApp. Vishing calls may come from a real person or a pre-recorded robocall. Scammers use voice tactics to steal confidental personal data such as identifying information, bank account numbers, login details, and passwords.

Types of manipulation in vishing:

Impersonation

Scammers often impersonate employees of banks, government agencies, insurance or other well-known companies to appear legitimate and obtain financial and personal information. They use psychological tactics to create a sense of urgency, convincing victims that they are in trouble. They may threaten and try to scare them.

Persuasiveness

Scammers may also use persuasive language and tone to convince the victim that they are on their side. This is why they often lead the conversation in a friendly, approachable, compassionate manner and appears to be helpful and often use ambiguous language or change the subject during a conversation to distract the victim.

Persistence

Scammers are characterised by persistence including repeat calls from the same number (they might even contact victim several times a day etc.). In his way, slowly and steadily, gaining the victim's trust. This tactic is used to gain the victim's trust and to lure them into revealing sensitive information.

Telephone scams involving the elderly

— CONSEQUENCES:

Seniors often consider phone calls to be an important way of communicating and value the personal interaction that a phone call provides. It is this high level of trust in personal communication over the phone that makes them more vulnerable to different types of telephone scams and more easily believe misleading requests for information or action made by fraudsters.

01 Financial Consequences

Victims of phone scams often suffer direct financial losses. Scammers can deceive victims into making payments or providing banking information, leading to unauthorized transactions or draining of bank accounts. This can significantly impact their savings and financial security.

02 Identity Theft

Telephone scams often involve the theft of personal information such as social security numbers, dates of birth and addresses. Victims may face significant challenges in solving these problems and recovering their identities.

03 Reputational Damage

In cases where the scam is the result of unauthorised financial activities or transactions, the victim may also suffer damage to his or her financial reputation. Rebuilding reputations can be difficult and requires extensive documentation and communication with financial institutions.

Telephone scams involving the elderly

— WAYS OF PROTECTION WITH HISTORY IN THE BACKGROUND

Andrew received a phone call from a person claiming to be from a health insurance company and needing further information to update his medical records. The caller was very friendly but he didn't introduce himself by his first and last name. He just said that he was calling on behalf of the insurance company and explained that it was a routine check.
When he started asking for personal details such as insurance number and date of birth, Andrew became suspicious.

Unfortunately for the scammer ...

Andrew actively participates in online forums and communities where security issues are discussed and experiences of scams are shared.

STEP 1: Verifying the identity of the caller
Andrew was unable to verify the caller's identity on the insurance company's official website because the alleged employee of the insurance company did not give his full name - so Adrew became suspicious.

STEP 2: Being attentive to suspicious requests
When the caller started asking for personal information such as insurance number and date of birth, Andrew questioned the authenticity of the call and immediatelly dissconnected the call.

STEP 3: Using previous knowledge
Andrew recognised the signs of deception due to his active participation in online forums discussing security issues, which helped him to quickly spot the suspicious elements of the call.

STEP 4: Informing/reporting
Andrew called his health insurer directly to check whether the call was a scam attempt and spread the word about on forums and communities where he is active.

Telephone scams involving the elderly

WAYS OF PROTECTION:

Due to the accelerated progress of telecommunications technology, scammers have taken advantage of the anonymity and easy access to phone calls to conduct fraudulent activities. It is therefore crucial that seniors maintain a high level of vigilance and are aware of the risks associated with communicating over the phone.

Here are some additional tips in case you might find yourself in such a situation.

Ignore unexpected calls from unknown numbers or simply let them go to voicemail and decide whether to return the call based on the information provided.

Avoid using any call-back number they provide, as it could be part of a scam. Instead **look up the official phone number and call them directly** to confirm the legitimacy of the request.

Never share financial or personal information over the phone!

Hang up the phone immediatelly if they try to get this kind of information!

Telephone scams involving the elderly

WAYS OF PROTECTION:

Check the line:

Be aware that scammers can keep your phone line open even after you've hung up.

Use a different phone to check if the line is free, or **wait at least 10 to 15 minutes** to make sure that any scammers have hung up.

Try call blocking:

Activate your phone's call blocking functions to filter out possible vishing scams. Most smartphones offer this functions.

If you don't have a smartphone, contact your phone service provider to find out what services they offer to block unwanted calls.

If you are a victim of vishing, immediately contact the relevant institutions that can help you

Scams that exploit emotional family ties

HAZARD CHARACTERISTICS:

The grandparent scam is a type of fraud where scammers prey on the emotional bonds between grandparents and their grandchildren. The scammer typically pretends to be a grandchild in distress, needing immediate financial help.

Types of manipulation in the grandparent scam:

Urgency

The scammer creates a sense of urgency to prevent the grandparent from thinking too much or contacting other family members.

Secrecy

Scammers may ask the grandparents to keep the situation a secret, claiming embarrassment or fear of getting in more trouble.

Emotionally manipulative

Scammers exploit the grandparent's love and concern for their grandchild to elicit a quick response.

Scams that exploit emotional family ties

CONSEQUENCES:

Falling victim to a grandparent scam can have severe consequences.

01 Financial loss

Financially, you might lose your hard-earned money, as scammers often ask for large sums that can deplete your savings. If you provide your bank details, they can steal even more

02 Emotional distress

Emotionally, the fake emergencies create significant stress and anxiety, and discovering it was a scam can leave you feeling deeply betrayed and hurt.

03 Loss of trust

This experience can lead to a loss of trust, making you doubt real emergencies and feel suspicious of any unexpected contact, even from legitimate sources.

04 Isolation

Additionally, you might feel embarrassed or ashamed, leading to reluctance to communicate about financial matters with family or friends, and scammers may target you again, seeing you as an easy mark.

Scams that exploit emotional family ties

— WAYS OF PROTECTION WITH HISTORY IN THE BACKGROUND

Mary lives alone and enjoys a close relationship with her family, especially her grandchildren. One evening, Mary received a phone call from someone claiming to be her grandson, Jack, who urgently requested a big amount of money. This call led to a distressing and costly experience for Mary.
However, Mary remembers the advice her grandson gave her about being cautious with phone calls with people asking for money.

Mary's experience highlights the importance of staying informed about common scams and verifying any urgent and emotional requests for money. By understanding the tactics scammers use, such as creating urgency, demanding secrecy, and manipulating emotions, seniors can better protect themselves from becoming victims. If in doubt, always verify the information with other family members and never rush to send money.

Step 1: Verification

Mary asked the caller questions only Jack would know, and she took a moment to call Jack directly to avoid the scam.

Step 2: Awareness

Knowing about such scams in advance helped Mary recognize the warning signs.

Step 3: Communication

Mary has already discussed with family about potential scams and setting up a family code word for emergencies can provide additional protection.

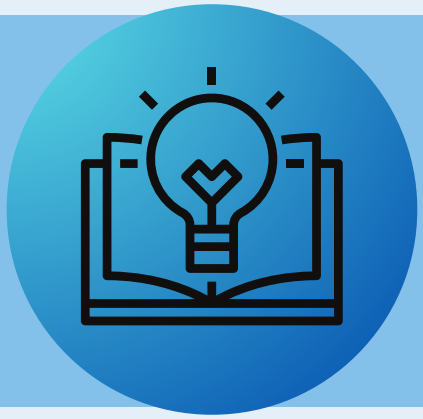
Scams that exploit emotional family ties

WAYS OF PROTECTION:

Protecting yourself from scams that exploit emotional family ties is crucial for safeguarding your hard-earned money. Here are some straightforward steps you can take.

Stay informed:

Educate yourself and your loved ones about common scams targeting seniors, including the grandparent scam.
Stay updated on new tactics scammers may use by following reputable sources of information.



Verify identities:

Always ask questions only the real family member would know, such as the name of a pet or a specific family event.
If in doubt, call back using a known number to verify the caller's identity.

Set up a family code word:

Establish a secret code word with your family that only trusted individuals would know.
Use this code word in emergencies to verify the identity of callers claiming to be family members.

Scams that exploit emotional family ties

WAYS OF PROTECTION:

Avoid rushed decisions:

Take your time when receiving unexpected or urgent requests for money.
Scammers use urgency to prevent you from questioning their story or seeking advice from others.

Use caller ID and call blocking:

Utilize caller ID to screen incoming calls and block unknown or suspicious numbers.
Report scam calls to your phone service provider or relevant authorities.

Guard personal information

Be cautious about sharing personal and financial information over the phone or online.
Avoid providing sensitive details unless you are certain of the recipient's identity.

Scams involving medical products

HAZARD CHARACTERISTICS:

In recent years, scammers have increasingly targeted vulnerable individuals, including seniors, with fraudulent schemes involving medical products. These scams often exploit emotions and fears related to health issues, promising miracle cures, treatments, or remedies that are too good to be true

Types of manipulation in medical product fraud:

False Promises

Scammers make bold claims about their products, promising miraculous results with little to no scientific evidence.

High Pressure Tactics

They often use high-pressure sales tactics, urging you to buy quickly before the "limited-time offer" expires.

Emotional Manipulation

These scams play on your emotions, preying on your fears about health issues and offering false hope for a quick and easy solution.

Scams involving medical products

CONSEQUENCES:

Medical product manipulation can have serious negative effects such as:

01 Financial loss

Falling victim to medical product scam can result in spending large sums of money on ineffective or even dangerous products, depleting your savings.

02 Health risks

In some cases, the scammers use unregulated or counterfeit medical products which can lead to serious health complications or interactions with existing medications.

03 Emotional Distress

Being scammed can lead to feelings of shame, guilt, and embarrassment. You may feel betrayed and anxious, which can negatively impact your overall mental health and well-being.

04 Deterioration of Quality of Life

The combined effects of financial loss, health risks, and emotional distress can lead to a significant decline in the quality of life for victims. They may struggle with managing their daily activities and maintaining their independence.

Scams involving medical products

WAYS OF PROTECTION WITH HISTORY IN THE BACKGROUND

Thomas receives an email advertising a new "miracle supplement" that claims to cure arthritis, diabetes, and high blood pressure overnight. The email offers a limited-time discount and urges him to buy now to avoid missing out on the opportunity for better health.
However, Thomas remembers the advice he read about being cautious with miracle treatments.

Thomas's story is unfortunately not the only case. Medical product scams prey on the vulnerabilities and emotions of seniors, promising quick fixes for complex health issues. By staying informed, skeptical, and consulting with healthcare professionals, you can protect yourself from falling victim to these fraudulent schemes. Remember, your health is priceless, and there are no shortcuts to genuine wellness.

Step 1: Stay skeptical

Thomas remembered that legitimate medical breakthroughs are rigorously tested and verified by experts.

Step 2: Consult professionals

Thomas called his personal doctor and discussed any new treatments or supplements.

Step 3: Research

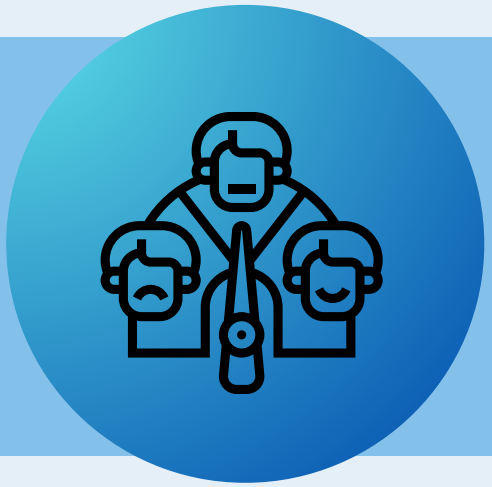
Thomas looked for unbiased reviews and scientific evidence supporting the product's claims before considering a purchase.

Scams involving medical products

WAYS OF PROTECTION:

Remember, protecting yourselves from medical product fraud is crucial for safeguarding your hard-earned money and your health. One of the most crucial step is to seek for emotional support. Here are some straightforward steps you can take.

Seek for emotional support:
Social support from family, friends, and community members can provide seniors with the emotional strength and reassurance they need to resist manipulation. When seniors feel supported and valued, they are less likely to fall prey to scammers who exploit emotional vulnerabilities.



Stay informed:
Social networks can be a vital source of information. Family members and friends can share warnings about ongoing scams, provide tips on how to recognize fraud, and suggest trusted sources for medical products and treatments. Staying informed through social support can significantly reduce the risk of falling for scams.

Scams involving medical products

WAYS OF PROTECTION:

Consult healthcare professionals:
Before trying any new medical product or treatment, consult with your healthcare provider to ensure it is safe and effective.

Be skeptical of miracle claims:
If a product claims to cure multiple unrelated health conditions or offers quick and effortless results, it's likely too good to be true.

Research Thoroughly:
Take the time to research the product and the company behind it. Look for reviews from reputable sources and check if the product is approved by regulatory agencies.

Further readings

FRAUD IN MALE-FEMALE RELATIONS

- https://www.sciencedirect.com/science/article/pii/S2949791423000441
- https://hu.usembassy.gov/be-wary-of-online-romance-scams/
- https://consumer.ftc.gov/articles/what-know-about-romance-scams#whatis https://us.norton.com/blog/online-scams/romance-scams
- https://www.unit21.ai/fraud-aml-dictionary/romance-fraud
- https://www.hsbc.co.uk/help/security-centre/romance-scams-case-study/
- https://www.equifax.co.uk/resources/identity-protection/how-to-spot-and-avoid-romance-scams.html
- https://dfpi.ca.gov/2024/03/05/romance-scams-what-consumers-need-to-know/
- https://complyadvantage.com/insights/what-is-a-romance-scam/

SMISHING SMS-SCAMS

- https://www.kaspersky.com/resource-center/threats/what-is-smishing-and-how-to-defend-against-it
- https://www.proofpoint.com/us/threat-reference/smishing
- https://www.sinch.com/blog/what-is-smishing/
- https://business.bofa.com/en-us/content/what-is-smishing-how-to-prevent-it.html
- https://www.forbes.com/advisor/business/what-is smishing/#how_to_protect_against_smishing_section
- https://www.techtarget.com/searchmobilecomputing/definition/SMiShing
- https://cybeready.com/category/the-complete-guide-to-smishing
- https://www.rd.com/article/what-is-smishing/

Further readings

TELEPHONE SCAMS INVOLVING THE ELDERLY

- https://www.ageuk.org.uk/information-advice/money-legal/scams-fraud/phone-scams/
- https://www.ageuk.org.uk/globalassets/age-uk/documents/information-guides/ageukig05_avoiding_scams_inf.pdf
- https://www.helpguide.org/articles/abuse/elder-scams-and-senior-fraud-abuse.htm
- https://www.seniorliving.org/research/common-elderly-scams/
- https://www.ooma.com/blog/home-phone/protect-seniors-from-elderly-phone-scams
- https://taking.care/blogs/resources-advice/scams-targeting-the-elderly#How_to_avoid
- https://www.terranovasecurity.com/solutions/security-awareness-training/what-is-vishing
- https://www.kaspersky.com/resource-center/definitions/vishing
- https://www.proofpoint.com/us/threat-reference/vishing

SCAMS THAT EXPLOIT EMOTIONAL FAMILY TIES

- https://www.homeinstead.com/location/347/news-and-media/the-grandparent-scam/
- https://www.europol.europa.eu/media-press/newsroom/news/crime-against-elderly-four-arrests-in-germany-and-poland
- https://www.identityguard.com/news/grandparent-scam#:~:text=The%20most%20common%20grandparent%20scam,often%20claim%20to%20be%20overseas.
- https://www.cbsnews.com/news/what-being-targeted-by-grandparent-scam-sounds-like-60-minutes/
- https://www.youtube.com/watch?v=v2VFy2igHPE
- https://globalnews.ca/video/9901367/calgary-senior-falls-victim-to-grandparents-scam-costing-her-thousands

Further readings

SCAMS INVOLVING MEDICAL PRODUCTS

- https://www.forres-gazette.co.uk/news/older-people-targeted-by-medical-scam-116453/
- https://www.who.int/news-room/fact-sheets/detail/substandard-and-falsified-medical-products
- https://www.ema.europa.eu/en/human-regulatory-overview/public-health-threats/falsified-medicines-overview
- https://www.bbc.com/news/business-58029113
- https://www.europol.europa.eu/media-press/newsroom/news/544-arrests-and-%E2%82%AC63-million-of-fake-pharmaceuticals-and-illegal-doping-substances-seized

CHAPTER 4.
ONLINE TRANSACTION FRAUD

In the era of online payments and transactions, there are more and more reports of online frauds. Criminals have access to many seniors in the use of new technologies, which makes them more sophisticated in fraudulent practices. In this section, we will discuss the most common scams with online proceedings to help seniors solve and avoid them.

Travel and ticket scams involve offering fictitious offers that never materialize. In subscription scams, seniors are tricked into accepting services that automatically charge fees. Fake online stores extort payments for undelivered products. Buy-sell scams include fraudulent purchases where products are not listed or are not available, and where seniors sell their belongings for free on classifieds sites.

Understanding these threats is crucial so that seniors can safely take advantage of the opportunities offered by the Internet, and protect their finances from fraud.

Travel and ticketing scams

HAZARD CHARACTERISTICS:

Travel and ticketing fraud refers to fraudulent schemes that involve the selling of fake travel, tour, and ticket packages. This type of fraud often occurs online, where scammers set up professional-looking websites or send out emails offering heavily discounted deals. Seniors, who may be less familiar with modern online fraud tactics, are particularly vulnerable to these scams. Unwitting customers, especially seniors attracted by these offers, make payments for these non-existent services and are left with no recourse when they realize they've been scammed. It is crucial to educate seniors about these fraudulent schemes to help them avoid significant financial loss and emotional distress.

Types of travel and ticketing fraud:

Fake Airline Tickets

This involves scammers selling non-existent airline tickets. They may set up fake websites that look like genuine airline sites, lure customers with discounted ticket prices, and then disappear after collecting payment.

Fraudulent Holiday Packages

This occurs when scammers offer comprehensive holiday packages at heavily discounted rates. After the customer makes the payment, they discover that the package doesn't exist, or it doesn't include what was promised.

Timeshare Scams

Scammers may pose as timeshare sellers or resellers, promising great deals on timeshare properties. They may ask for upfront fees and then disappear once the payment is made.

Travel and ticketing scams

— CONSEQUENCES:

Travel and Ticketing Fraud can have serious negative effects such as:

01 Financial Loss

The most direct consequence of travel and ticketing fraud is financial loss. Scammers take payments for non-existing services, leaving victims with no recourse to recover their money.

02 Identity Theft

Often, these frauds involve the victim providing sensitive personal and financial information under the guise of booking a trip. This information can then be used for identity theft.

03 Emotional Distress

Falling victim to such fraud can lead to significant emotional distress. The excitement of a planned trip turns into disappointment and frustration, not to mention the feelings of violation and vulnerability after being scammed.

Travel and ticketing scams

— WAYS OF PROTECTION WITH HISTORY IN THE BACKGROUND

One day, George received an email from an online travel agency offering a fantastic deal on a European holiday package. The deal included flights, accommodations, and sightseeing tours in Rome, Paris, and London. The package was deeply discounted, and George, excited by the prospect of his dream trip, decided to investigate further.

He clicked through to the travel agency's website, which looked professional with high-quality images of the destinations and glowing testimonials from happy customers. Convinced, George decided to book the holiday package. He entered his credit card details and received an email confirming his booking.

Days turned into weeks, and George did not receive any further communication about his trip. He started to worry and tried to contact the travel agency, but found that their phone number was disconnected, and his emails were left unanswered.

George's story highlights the need to educate seniors about online scams. As they become more tech-savvy, they are at higher risk. Informing them about scam signs, like overly attractive deals, and the importance of verifying a company's authenticity before purchasing can help them stay safe. Sharing such experiences can effectively warn seniors about online fraud.

STEP 1: Verify authenticity vs. immediate trust
George trusted the travel agency based on their professional-looking website and testimonials without further verification. George should have verified the authenticity of the travel agency by checking customer reviews, confirming its registration and physical address, and assessing their response rate by contacting them directly.

STEP 2: Use secure payment methods vs. entering credit card details
George entered his credit card details directly on the travel agency's website without ensuring the security of the payment process. George should have used secure payment methods that offer buyer protection, such as credit cards through a trusted payment platform, and avoided sharing credit card details directly on unfamiliar websites.

STEP 3: Follow-up communication vs. waiting without action
George waited weeks without receiving any further communication about his trip and only tried to contact the agency when he started worrying. George should have followed up with the travel agency shortly after making the booking to confirm the details and ensure continuous communication.

STEP 4: Report suspicious activity vs. delayed response
George delayed contacting his credit card company until he realized something was wrong. George should have reported any suspicious activity or lack of communication to his credit card company immediately to potentially halt the transaction and investigate the issue.

Travel and ticketing scams

WAYS OF PROTECTION:

It is crucial for seniors to protect themselves from Travel and Ticketing Fraud to avoid significant financial loss, emotional distress, and potential identity theft. Scammers often target seniors, who may be less familiar with online fraud tactics, taking advantage of their trust and excitement about travel deals. By protecting themselves, seniors can ensure their hard-earned money is not stolen, their personal information remains secure, and their travel plans are not ruined by fraudulent schemes.

Research the Company Thoroughly:

Before making any purchases, always ensure to conduct a comprehensive research of the company. Make sure to look for customer reviews and ratings to determine the company's credibility and ensure its legitimacy. This will give you a better understanding of the company's reputation among its previous customers.

Use Only Secure Payment Methods:

When purchasing online, it's crucial to use only secure payment methods. Avoid making direct bank transfers and refrain from sharing credit card details over platforms that aren't secured. It's always safer to use payment options that offer buyer protection.

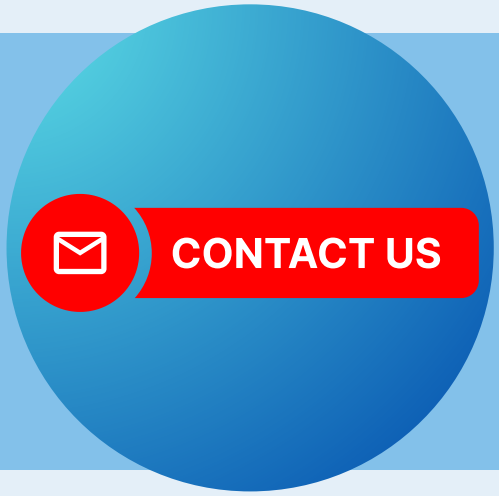
Travel and ticketing scams

WAYS OF PROTECTION:

Be Cautious of Deals That Seem Too Good to Be True:

If a deal or discount appears too good to be true, it probably is. Be particularly cautious of heavily discounted prices for items like airline tickets or holiday packages. It's always better to do a bit of market research before jumping on such deals.

- Example 3



Contact the Airline or Hotel Directly:

If you receive an email offering a discounted flight or hotel stay, it's a good idea to contact the airline or hotel directly to verify the offer. This will ensure that the offer is legitimate and not a scam.

Ensure Personal Information is Safe:

Exercise caution when sharing personal information. Always check that the platform is secure before entering any sensitive information. Never share important personal details on platforms that lack adequate security measures.

Subscription fraud

HAZARD CHARACTERISTICS:

Subscription fraud is a type of scam where individuals are tricked into signing up for expensive memberships or services without their knowledge. These scams often result in recurring charges that are difficult to cancel, impacting vulnerable individuals, including seniors.

Types of manipulation in subscription scams:

Deceptive Ads and Links

Scammers use misleading advertisements or pop-up links to lure you into signing up for what seems to be a free trial or a low-cost service

Hidden Terms

The terms and conditions of the subscription, including the cost and duration, are often hidden in fine print or not clearly explained.

Automatic Renewals

Once signed up, the subscription automatically renews, leading to unexpected charges on your credit card or bank account.

Difficulty Cancelling

Cancelling the subscription is intentionally made difficult, with complicated procedures, unresponsive customer service, or unclear cancellation policies.

Subscription fraud

CONSEQUENCES:

Subscription fraud can have serious negative effects such as:

01 Financial loss

Falling victim to subscription scam can result in the loss of hard-earned savings. You can lose significant amounts of money due to recurring charges they did not anticipate or agree to.

02 Identity Theft

Providing personal and payment information to fraudulent websites can lead to identity theft and further financial harm.

03 Emotional Stress

The frustration and stress of dealing with unauthorized charges and trying to cancel the subscription can impact your emotional well-being.

Subscription fraud

— WAYS OF PROTECTION WITH HISTORY IN THE BACKGROUND

David saw an online advertisement for a free trial of a new vitamin supplement. The ad claimed he only need to pay a small shipping fee to subscribe an then he would get unlimited vitamins for the rest of the year. Excited about trying the supplement, he decided to enter his credit card information to cover the shipping cost.
While doing that, David remembered what he read about some websites taking money away from innocent people.
So what did David do?

Step 1. Read the fine print

Before signing up, he looked for any mention of ongoing subscriptions or additional charges.

Step 2. Research

He looked up the company and read reviews to see if others have experienced similar issues

Step 3. Monitor statements

Regularly checked his statements to catch unauthorized charges early.

Subscription fraud

WAYS OF PROTECTION:

Protecting yourself from subscription scams is crucial for safeguarding your hard-earned money. Here are some straightforward steps you can take.

Read the Fine Print:

Always read the terms and conditions before signing up for any service, especially if it involves a free trial or discounted offer

Be Wary of Free Trials:

Be cautious of free trials that require your credit card information. Check if the trial converts into a paid subscription and what the costs will be.

Research the Company:

Look up reviews and ratings of the company offering the subscription. Ensure they have a good reputation and reliable customer service.

Subscription fraud

WAYS OF PROTECTION:

Monitor Bank Statements:

Regularly check your bank and credit card statements for any unauthorized or suspicious charges.

Set Up Alerts:

Use account alerts to notify you of any new charges or transactions. This way, you can quickly identify and dispute unauthorized charges.

Seek Help:

If you find yourself a victim of subscription fraud, contact your bank or credit card company immediately to report the unauthorized charges. They can help you stop further charges and recover your money

Fraud in creating fake online stores

HAZARD CHARACTERISTICS:

Fake online stores are fraudulent websites created to look like legitimate shopping sites. These scammers use deceptive sales tactics to trick people into making purchases. Instead of receiving the items they ordered, victims often receive counterfeit goods, low-quality items, or nothing at all. This type of fraud can significantly impact vulnerable individuals, including seniors.

Types of manipulation in fake online stores:

Too-Good-to-Be-True Prices

Scammers attract buyers with unbelievably low prices or massive discounts on popular items.

Poor Website Design

While some fake sites are very sophisticated, many have poor design, broken links, or low-quality images.

Limited Contact Information

Legitimate businesses provide clear contact information, including physical addresses and customer service phone numbers.

No Reviews or Fake Reviews

A lack of genuine customer reviews or only having overly positive, generic reviews can be a red flag.

No Secure Connection

Legitimate shopping sites use secure connections to protect your data. Look for "https" and a padlock icon in the browser address bar.

Fraud in creating fake online stores

CONSEQUENCES:

Fraud concerning fake online stores can cause serious negative effects such as:

01 Financial loss

Falling victim fraud regarding fake online stores can result in the loss of savings. You may find yourself with significantly less money than expected, impacting your ability to cover daily expenses and enjoy your retirement.

02 Emotional stress

Realizing they have been scammed can cause significant emotional distress. Seniors may feel embarrassed, ashamed, or guilty for falling for the scam. This emotional impact can lead to anxiety, depression, and a decreased sense of trust in online shopping and financial institutions.

03 Persolan information theft

Fake online stores often collect personal and financial information during the checkout process. This information can be used for identity theft, leading to unauthorized transactions, new credit accounts opened in the victim's name, and other forms of fraud.

Fraud in creating fake online stores

— WAYS OF PROTECTION WITH HISTORY IN THE BACKGROUND

Eva saw an ad on social media for a high-end blender at a 75% discount. Excited by the great deal, she clicked the link and she was directed to a website that looked professional but offered limited contact information. The site insisted on payment through a wire transfer to secure the low price.
After making the payment, she never received the blender, and attempts to contact customer service went unanswered.

What Eva should have done to avoid being scammed?

Fake online stores can be deceiving and cause significant financial and emotional harm, especially to seniors. By staying informed and following the protective measures outlined below, you can reduce the risk of falling victim to these scams. Always take the time to research and verify online stores before making any purchases to ensure a safe and secure shopping experience.

Step 1. Research the Website

She should have checked for reviews and look up the store's contact information.

Step 2. Verify Secure Connections

Ensure the website has "https" and a padlock icon.

Step 3. Be Skeptical of Deals

Question the too-good-to-be-true discount.

Step 4. Use Safe Payment Methods

Avoid wire transfers; use a credit card instead.

Fraud in creating fake online stores

WAYS OF PROTECTION:

Remember, dear seniors, protecting yourself from fake online stores is crucial for safeguarding your money and your emotions. Here are some straightforward steps you can take.

Research the Website:

Check for reviews and ratings from other customers. Use trusted review sites to verify the store's legitimacy. Look up the store's contact information and try reaching out before making a purchase.

Verify Secure Connections:

Ensure the website uses a secure connection ("https" and a padlock icon). Avoid entering personal or payment information on sites without a secure connection

Be Skeptical of Too-Good-to-Be-True Deals:

If the prices seem unbelievably low or the deals are too good to be true, they probably are. Compare prices with other reputable retailers.

Fraud in creating fake online stores

WAYS OF PROTECTION:

Use Safe Payment Methods:

Use credit cards for online purchases as they offer better fraud protection. Avoid using wire transfers, prepaid cards, or cryptocurrency for payments.

Check the Website's Details:

Look for clear, detailed product descriptions and professional images. Verify the site's contact information, including phone numbers and physical addresses

Know the Return Policy:

Legitimate stores have clear return policies. Be wary if this information is missing or unclear.

Fraudulent purchases via online advertisements (buying)

HAZARD CHARACTERISTICS:

Online fraudulent advertising is a significant threat, with scammers leveraging social media platforms, popular websites, and even search engines such as Google. Fake ads can take many forms, including pop-ups, banners, social media ads, and sponsored content. These deceptive online ads are designed to trick unsuspecting users into clicking on them, potentially leading to fraudulent purchases.

Types of manipulation in purchases via online advertisements

Imitation

Scammers typically use promotional material (logos, captions, slogans, etc.) from real well-known brands. Then, they start running targeted ads to scam victims. Scammers may also use social engineering tactics, such as enticing offers, to lure users into clicking on these fake advertisements.

No *"real"* goods

As fake ads can appear very professional and convincing, it is difficult to distinguish them from legitimate ads. When a victim clicks on an ad, they usually end up in a fake shop - where phishing may occour - or in a shop that sells counterfeits. In these cases (in addition to the phishing), there is also a risk that the victim will not receive the product or will receive a product of a lower quality than paid for.

Malvertising

Scammers often use fake ads with embedded malicious code that can infect users' devices when clicked. This method, known as malvertising, has become a widespread tactic used by cybercriminals to spread malware via fake ads.

Fraudulent purchases via online advertisements (buying)

— CONSEQUENCES:

Regardless of the method chosen, scammers behind fake ads are always driven by financial gain.

01 Financial consequences - Direct Financial Theft

Fake ads offering heavily discounted products from well-known brands often conceal shops that aim to capture payment details and sensitive information during the checkout stage of a transaction. This information can be used to steal money from accounts, initiate additional cyberattacks, or sell to other cybercriminals. In many cases, victims receive counterfeit goods or nothing at all.

02 Financial consequences - Ransomware Costs

Due to system compromise and data breaches through the method of malvertising can also have financial consequences. Upon clicking on the ad, malware starts to download and install ransomware - a type of malware that encrypts your files - scammers than demand payment for their release. The costs associated with paying the ransom, repairing your system, and removing malware can be significant.

03 Identity theft

Through the phishing method, scammers impersonate legitimate brands in an attempt to trick victims into sharing personal informatio or by installing spyware (through the method of malvertsig) which secretly collects sensitive information from the device, such as login credentials and financial data can lead to severe identity theft, where victims' sensitive data is misused.

Fraudulent purchases via online advertisements (buying)

WAYS OF PROTECTION WITH HISTORY IN THE BACKGROUND

Liza, a regular user of various social media platforms, was browsing Facebook when she came across an online ad offering a very nice blender. The ad showed a picture of a top-of-the-line blender at an extremely low price with a promise of fast delivery.
The ad seemed too good to be true, but she clicked on it by mistake and was redirected to what initially seemed to be a legitimate online store ... However, Liza recognized the warning signs!

Unfortunately for the scammer ...

Liza attended an advanced workshop on social media scams.

STEP 1: Quality checking

After the redirect, Liza immediately noticed that the website was poorly designed, had many grammatical errors and that the photos were of poor quality in contrast to the advertisement.

STEP 2: Technical checking

Liza noticed that the URL of the website did not match the brand name. Instead, the title was made up of random letters and numbers.

STEP 3: Legitimacy checking

When Liza checked the website, she found that key contact details such as the company address, telephone number and customer service email were missing.

STEP 4: Feedback checking

Liza also noticed that there were no customer reviews or feedback on the website. A legitimate online trader usually provides reviews and opinions from previous customers.

Fraudulent purchases via online advertisements (buying)

WAYS OF PROTECTION:

Scams with fake adverts, where criminals market fake or non-existent products at attractive prices and take advantage of seniors' interest in discounts. Scammers may prolong the scam by making up excuses for delivery delays, which further increases the financial damage to victims.

Here are some additional tips in case you might find yourself in such a situation.

To protect yourself against possible scams, it is **safest to ignore adverts**, especially those you find suspicious!

Also **be careful where you click or tap!** Paying attention to where your mouse or fingers are on the screen and being mindful of what part of the page you scroll through can help you avoid accidental clicks or taps!

Be cautious when clicking or taping on any link, even those at the top of search engine results.

Pay close attention to distinguish between ads and genuine search results. Ads typically appear first and are marked with "Ad" or "Advertisement."

Be aware that scammers intentionally pay for ad placements in search engines!

Fraudulent purchases via online advertisements (buying)

WAYS OF PROTECTION:

Always type the website URL directly into your browser:

Look for a lock icon and "https" in your browser to confirm it's secure, verify the URL (float a cursor over the URL).

Protect your computer:

It is important to install and regularly update anti-virus, security software on your computer. This will ensure that your computer is protected from different types of threats such as viruses, hacker attacks and malware.

Enable the pop-up blocking function in your web browsers!

Fraudulent purchases via online advertisements (buying)

WAYS OF PROTECTION:

Fake online sellers/scammers usually request payment via unreliable methods such as bank transfers (as they offer less protection in the event of a scam, compared to other payment methods such as credit cards) or unknown payment platforms.

Never ever make a payment in this way! Also, never disclose your financial or other sensitive information!

If you fall for a scam, **try to gather as much evidence as possible and report it to the relevant authority immediately!**

Report! Most platforms have reporting mechanisms in place to address such issues.

Use the reporting feature on the platform, typically accessible via the ***'Report'*** **button on the ad or user profile.**

Await instructions from the platform's support team and cease all interactions with the suspected individual after reporting.

Fraudulent purchases via classifieds sites (selling)

HAZARD CHARACTERISTICS:

Online marketplaces can be a great way for seniors to make some extra money, as they can sell their items such as handmade crafts, antiques, or unnecessary household items etc. This enables them to earn additional money, which can be used to improve their standard of living or for special occasions. Seniors need to be particularly vigilant when selling, as these markets are also prone to scammers posing as potential buyers.

Types of manipulation in classified buyer scams:

No personal contact

Scammers are willing to "buy" an item without seeing it and often use various excuses such as illness, honeymoon, or traveling abroad etc. They only contact victims via text messages or emails and avoid phone calls or video calls. They often ask for the item to be sent to their "shipping agent" or arrange for a courier to pick it up. All these methods of communication allow scammers to conceal their identity.

No cash

Scammers exclusively request payment by cheque, money order, bank transfer, international funds transfer, mobile payment apps, etc., sending fake payment confirmations and hoping that victims will send the item before realising it is a scam. They may use »excuses«, such as there was a problem with the payment they sent, they may ask victims to pay in advance for transport or shipping costs and promise to reimburse the costs, etc.

Overpayment

Scammers typically offer victims more money than the asking price. The reasons vary - they may claim to compensate for the victim's "troubles," cover supposed shipping costs, or feign making a mistake in the payment amount. However, once the victims receive an overpayment, the scammers will request the excess funds back.

Fraudulent purchases via classifieds sites (selling)

CONSEQUENCES:

Victims of classified buyer scams may experience the following adverse effects:

01 Financial Consequences

Victims may face financial consequences, such as the monetary loss of the value of the items if they have sent items without receiving payment. If there has been an overpayment and the victims have returned the money, they are likely to find that the initial payment was fraudulent - the cheque will be deducted or the customer's online payment will be rejected - in this case, the victims have lost the money they 'returned' and the monetary value of the items.

02 Emotional consequences

The victim may develop a range of symptoms, including negative thoughts about themselves. Victims may think they are not smart or that there is something wrong with their ability to judge others. They often blame themselves for the crime, feeling that they have been too trusting, and feel angry, sad, betrayed, helpless and embarrassed.

03 Legal consequences

If the victim has agreed to and accepted payment by cheque, but the cheque was forged, the unsuspecting victim will be held legally liable for attempting to cash the illegal cheque when the bank detects the forgery. Furthermore, the victim may face difficulties in future financial transactions.

Fraudulent purchases via classifieds sites (selling)

WAYS OF PROTECTION WITH HISTORY IN THE BACKGROUND

Leon posted an ad on the Facebook Marketplace for a second-hand bicycle for 200 euros and immediately received a message from "Tim," who wanted to buy it without negotiating the price and even offered 30 euros more for postage costs.
Leon found it strange that Tim did not want to see the product in person, despite living in the same town. Tim also wanted to pay for the product via PayPal and asked for Leon's social security number and home address. That's when Leon backed off in a hurry!

Unfortunately for the scammer ...

Leon has monitored the awareness campaign within the user community and educated himself on the common attempts of this type of scam and the preventive measures.

STEP 1: Recognizing suspicious behavior

Leon found it strange that Tim did not want to see the product in person, despite living in the same town. This was the first warning sign as legitimate buyers usually prefer to inspect items before making a purchase.

STEP 2: Researching

Leon researched Tim's profile and found suspicious contact information and inconsistent communication. Leon blocked Tim and immediately cut off all communication, thus preventing further risks.

STEP 3: Protecting

Tim wanted to pay via PayPal, which is not suspicious by itself, but he also requested Leon's social security number and home address, which is highly unusual and unnecessary. Leon consciously decided not to share this information.

STEP 4: Informing/reporting

Leon shared his experience with the community and reported Tim's profile to the platform. By doing this, he helped raise awareness and protect other users as well.

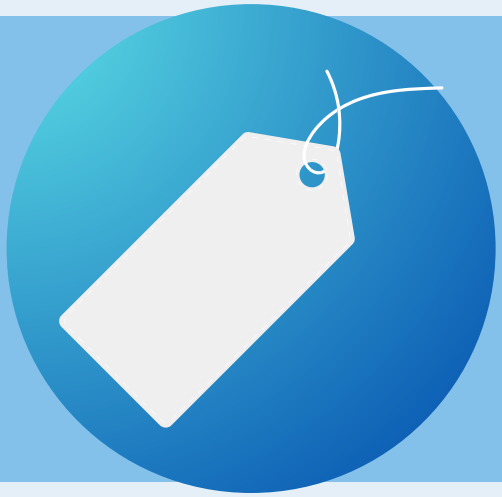
Fraudulent purchases via classifieds sites (selling)

WAYS OF PROTECTION:

If you are advertising your items for sale through online classifieds portals, here are some simple steps you can take to empower and protect yourself from scammers pretending to be potential buyers.

Be wary when someone offers you more than your asking price is (unless you are selling an item with multiple competitive bids). Do not engage with anyone who offers to send you payment in a higher amount, expecting you to send back the excess.

Immediately reject such payment and insist on receiving the correct amount in a new transaction.



Ask for payment in cash:

If that is not possible, **do not send an item before you receive payment, and make sure the payment is legitimate.**

If you send before they pay, you will have no way to get your item back!

Fraudulent purchases via classifieds sites (selling)

WAYS OF PROTECTION:

Do not trust payment confirmations by email – they could be fake! Check your bank account directly to see whether payment has been received

It is best to **deal with local buyers** you can meet in person and only accept cash to avoid possible scams. **Do not pay any apparent shipping costs or transfer fees.** Particular caution is advised when selling to buyers abroad.

Ignore any requests to provide any unecessary information. Provide only the information strictly necessary to complete the transaction.

If you are selling an item, **do not click on any link sent to you by the buyer and do not to send the buyer any information that could give them access to any of your bank accounts.**

Report! Most platforms have reporting mechanisms in place to address such issues.
Use the reporting feature on the platform, typically accessible via the ***'Report'*** **button on the ad or user profile.**
Await instructions from the platform's support team and cease all interactions with the suspected individual after reporting.

Further readings

TRAVEL AND TICKETING FRAUD

- https://www.comparitech.com/blog/information-security/avoid-common-ticket-and-travel-scams-online/ https://www.aura.com/learn/airline-scams
- https://www.interpol.int/en/Crimes/Financial-crime/Airline-ticket-fraud
- https://www.nyccriminallawyer.com/ticket-scams/
- https://www.chargebackgurus.com/blog/travel-agency-chargebacks
- https://chargebacks911.com/otas-lose-billions-every-year-to-travel-fraud/
- https://www.traveldailynews.com/post/how-fraudsters-exploit-travel-agencies
- https://www.consumerreports.org/travel/avoiding-travel-scams/
- https://www.bbb.org/all/travel-scams
- https://www.consumer.ftc.gov/articles/travel-scams

SUBSCRIPTION FRAUD

- https://balkaninsight.com/2023/08/22/subscription-scams-the-mobile-users-paying-for-unwanted-services/
- https://commission.europa.eu/live-work-travel-eu/consumer-rights-and-complaints/enforcement-consumer-protection/coordinated-actions/consumer-frequent-traps-and-scams_en
- https://www.evz.de/en/shopping-internet/internet-fraud/subscription-traps.html
- https://www.europe-consommateurs.eu/en/shopping-internet/internet-fraud-and-scams/subscription-traps.html
- https://www.flagright.com/post/understanding-subscription-fraud
- https://www.which.co.uk/news/article/5-subscription-scams-and-traps-to-watch-out-for-aYwJA0u8EFZ9

Further readings

FRAUD IN CREATING FAKE ONLINE STORES

- https://www.statista.com/statistics/1182221/online-shopping-fraud-incidents-uk/
- https://www.northyorkshire.police.uk/news/north-yorkshire/news/news/2024/04-april/online-shopping-fraud/
- https://us.norton.com/blog/online-scams/fake-e-shops
- https://www.youtube.com/watch?v=ltI7DXrNQCA
- https://www.youtube.com/watch?v=CQYmfcLW_oc

FRAUDULENT PURCHASES VIA ONLINE ADVERTISEMENTS (BUYING)

- https://www.rd.com/list/fake-ads-on-social-media/
- https://www.seniorlifestyle.com/resources/blog/protect-your-parents-from-common-digital-traps/
- https://www.takefive-stopfraud.org.uk/advice/general-advice/purchase-fraud/ primeri https://bolster.ai/glossary/fake-ads
- https://www.investigatetv.com/2023/11/14/how-determine-if-social-media-ads-are-real-or-fake/
- https://thegratifiedblog.com/social-media-marketing/how-to-spot-fake-ads-on-facebook/#What_Are_Fake_Ads
- https://trafficwatchdog.pl/en/articles/85/ad-frauds-in-social-media
- https://www.tracit.org/uploads/1/0/2/2/102238034/tracit_fradulentadvertisingonline_execsummary_july2020_final.pdf
- https://commission.europa.eu/system/files/2020-01/survey_on_scams_and_fraud_experienced_by_consumers_-_final_report.pdf

Further readings

FRAUDULENT PURCHASES VIA CLASSIFIEDS SITES (SELLING)

- https://www.westpac.com.au/security/types-of-scams/online-shopping-scams/
- https://www.ccpc.ie/consumers/money/scams/social-media-scams/
- https://www.desjardins.com/qc/en/tips/spot-avoid-scams-online-classifieds.html https://www.obvy-app.com/en/magazine/individuals/avoid-scams/scam-sites-small-ads/2341
- https://www.interbank.com/fraud-protection/beware-of-online-scams-how-to-spot-fake-listings-on-social-media-sale-groups/
- https://www.dropzone.com/help/classifieds/classifieds-buyer-scams-r23/
- https://www.nab.com.au/about-us/security/online-safety-tips/buying-selling-scams
- https://fastercapital.com/content/Classified-ads-site--Safety-Measures-When-Using-Classified-Ad-Websites.html
- https://consumer.ftc.gov/consumer-alerts/2022/07/selling-stuff-online-heres-how-avoid-scam

CHAPTER 5.
IDENTITY MANIPULATION AND EXPLOITATION OF PUBLIC TRUST

Modern frauds increasingly rely on identity manipulation and exploiting trust in public institutions, which puts seniors in a particularly vulnerable position. Criminals not only impersonate trustworthy institutions, but also use advanced technologies to achieve their goals. In this chapter, we will discuss the most common identity and trust frauds to help seniors recognize and avoid these threats.

Serious threats to seniors include false accusations of a crime, where scammers falsely accuse seniors in order to extort money or information. Government impersonation is another dangerous method, where criminals pretend to be the government to obtain personal information or money. Deepfake technology allows for the creation of fake but convincing recordings, which can lead to serious consequences. Service scams impersonating government institutions often involve fake offers that are intended to extort money. Fake accounts are used to blackmail seniors by threatening to reveal false information.

Understanding these threats and their mechanisms is crucial for seniors to effectively protect their identity, finances, and trust in public institutions. In this chapter, we will discuss these issues in detail to help you recognize and avoid such scams.

Allegations of involvement in crime

HAZARD CHARACTERISTICS:

Scamming a user out of money by claiming to be a judge, police officer or prosecutor and claiming that his name is linked to terrorism. "Allegations of involvement in crime" refer to claims or accusations that a person, organization, or even seniors have participated in illegal activities. These allegations are not yet proven and require investigation to determine their validity. The nature of the crime can vary widely, including fraud, theft, or other unlawful actions, and such allegations can have serious legal and social implications for the accused, including seniors. Seniors may be particularly vulnerable to such allegations due to their potential lack of familiarity with digital technology and common scam tactics.

Types of allegations of involvement in crime:

Involvement in a Terrorist Financing Network

Alleging that the victim's bank account has been linked to transactions funding terrorist activities is a type of scam that aims to intimidate the victim and induce panic. In this scenario, the scammer emphasizes the seriousness of the allegation. The scammer will usually demand immediate action from the victim, which could be paying a "fine" or "fee". Throughout the interaction, the scammer uses psychological manipulation tactics to get the victim panicked and manipulate them into sharing their personal information and/or money. They might even warn the victim not to contact anyone and keep this a secret.

Association with known terrorist organisations

In this scenario, the scammer might contact the victim and introduce themselves as an authoritative person, claiming to be a part of a law enforcement agency or judicial system. They warn the victim about their name being found in a list of individuals associated with a known terrorist organization. They might give fabricated details to get the victim scared and panicked. Demanding the victim to take immediate action, they might use threats or intimidating speech to maintain control.

Suspicious Travel History or Activities

In this scenario, the scammer contacts the victim posing as a police officer, judge or a prosecutor. They inform the victim that their travel history or certain activities raised suspicion. They might mention spesific places that the victim actually visited. To make it more believable, they might add details like dates of the travel, or names of suspected terrorists they believe you contacted with. Like the other scenarios, the scammer pressures the victim into making quick decisions and use manipulation tactics to get the victim provide personal information

Allegations of involvement in crime

CONSEQUENCES:

Fallegations of involvement in crime can have serious negative effects such as:

01 Damage to Reputation

Being associated with a crime, even if the allegations are not proven, can have serious impacts on a person's reputation. This could affect personal relationships, as well as professional opportunities.

02 Legal Consequences

If the allegations lead to a criminal investigation and the person is found guilty, they could face legal consequences. These can include fines, probation, or even imprisonment.

03 Emotional Distress

Being accused of a crime can cause significant emotional distress. The individual may experience feelings of fear, shame, or embarrassment, and these emotions can have long-term effects on their psychological wellbeing.

Allegations of Involvement in crime

CONSEQUENCES:

04 Identity Theft and Using It to Commit Further Crimes

Allegations involving identity theft can lead to further criminal activities being conducted in the victim's name, exacerbating the legal and personal repercussions.

05 Loss of Funds

Victims of crime allegations, especially those involving financial fraud, may suffer significant financial losses, either directly through theft or indirectly through legal fees and other costs associated with defending themselves.

06 Infecting Devices with Viruses

In cases involving cybercrime allegations, there is a risk that the accused person's devices may be targeted and infected with viruses or malware, leading to data breaches and further complications.

Allegations of Involvement in crime

— WAYS OF PROTECTION WITH HISTORY IN THE BACKGROUND

One day, Rita received an email, informing her that her name was involved in a high-profile crime investigation related to a fraudulent online transaction. The email appeared to be from the local police department and was quite detailed, creating a sense of urgency and fear.

The email instructed Rita to click on a link and input her personal information, including her social security number and bank account details, supposedly to verify her identity and clear her name from the investigation. Frightened by the allegations and desperate to resolve the issue immediately, Rita followed the instructions.

A few days later, she received a call from her bank, informing her about suspicious activities on her account. It was at this point that Rita realized she had been tricked by a scammer who used allegations of involvement in crime as a ruse.

This story underscores the importance of educating seniors about the risks and tactics of online scams. As demonstrated in Rita's case, scammers can prey on their lack of familiarity with the digital world and use scare tactics to trick them into divulging sensitive personal information. By educating seniors about these threats and teaching them how to verify the legitimacy of such requests, we can protect them from becoming victims of such scams.

STEP 1: Verification
If Rita gets an unexpected email, especially from a supposed government body or law enforcement, she should not respond directly. She should find the official contact details independently and verify.

STEP 2: Protect personal info
Rita should not share sensitive information like her social security number or bank details via email. Legitimate organizations don't ask for this via email.

STEP 3: Monitor accounts
Rita should regularly check her financial and online accounts for suspicious activity to catch fraud early and secure her accounts.

STEP 4: Use security software
Installing and updating security software can protect Rita from online threats like viruses, malware, and phishing. The software can scan for threats and block suspicious sites.

Allegations of Involvement in crime

WAYS OF PROTECTION:

Seniors must protect themselves from crime allegations, which can damage their reputation, lead to legal trouble, and cause emotional distress. They are often targeted due to unfamiliarity with digital technology, making them vulnerable to scams. Preventive measures can safeguard their finances, personal information, and well-being.

Verification of Unexpected Requests:
Always be vigilant when you receive unexpected emails or communication, especially from a source claiming to be a government body, a law enforcement agency, or a service you use. Instead of responding directly to the email or clicking on any links, independently find the official contact details for the organization and reach out to them for verification. This way, you can confirm whether the request is legitimate or a potential scam.

Being Cautious About Sharing Personal Information:
Your personal information is precious and should be protected at all costs. Never provide sensitive personal information like your social security number, bank account details, or other personally identifiable information in response to an email request or an unverified source. Legitimate organizations typically do not ask for this kind of information via email or unsolicited communication.

Allegations of Involvement in crime

WAYS OF PROTECTION:

Regular Monitoring of Accounts:
Regularly monitoring your financial and online accounts can help you spot any suspicious activity early on. This is crucial for preventing further damage, as you can immediately report the activity to the relevant authorities or the service provider and take steps to secure your account.

Use of Secure and Unique Passwords:
Using strong and unique passwords for all your online accounts is a fundamental security measure. A strong password includes a mix of letters, numbers, and symbols and is not easily guessable. Do not use the same password across multiple accounts. If one account gets compromised, others remain safe.

Installation of Security Software:
Installing and regularly updating security software on your computer provides a first line of defense against many online threats. This includes viruses, malware, ransomware, and phishing attempts. It can scan your system for threats, block suspicious websites, and provide real-time protection against malware attacks.

Manipulations in impersonation of state institutions

HAZARD CHARACTERISTICS:

Impersonating government officials is a type of scam where scammers pretend to be from various government agencies like tax authorities, police, or pension funds. These scams pose a significant threat to individuals' personal information and financial security. Scammers use different tactics to deceive their victims, but there are some common signs to watch out for.

Types of manipulation in impersonanation of state institutions:

Unsolicited communication

Scammers usually contact victims unexpectedly via phone, email, text, or even advertising online. The initial aim is to trick victims into initiating communication with the scammers. They usually have the intended victim's basic personal details to make them appear legitimate. Once contact is established, scammers will demand that the victim provide sensitive information, pay "fines" (through unusual payment methods), or perform other actions.

Pretending to be trustworthy

In the conversations with the victims, they provide a lot of false information about themselves, and their duties and use official-sounding terms, falsely implying government affiliation. In communication via mail or online they use official-looking government seals, logos, names of actual officials in the positions, fake websites, and email domains to fool victims into trusting them. The emails often also contain an attachment usually a PDF file) and a warning to read the attached documents.

Threats and urgency

Scammers use intimidation, and deadlines and threaten legal action or fines to force immediate responses. For instance, an email purporting to be from the police may threaten to initiate criminal proceedings if the victim does not respond within a specified timeframe. These tactics can induce panic and impair judgment, causing even typically rational individuals to react out of fear.

Manipulations in impersonation of state institutions

CONSEQUENCES:

Government imposter scams quite literally bank on the fact that seniors make great potential victims as older generations are often more trusting in governmental establishments and they are used to more respect authority and institutions. In addition, they have savings and are likely receiving some form of government benefits.

01 Financial Consequences

Victims lose money they transfer to scammers as payment to resolve fictitious tax, legal, or other obligations. In addition to the lost money, victims may incur additional costs to resolve the situation. If scammers gain access to their bank account, it can lead to further financial losses due to unauthorized purchases. In the worst-case scenario, the account can be emptied, causing irreparable damage, especially to seniors who may have lost their hard-earned savings.

Manipulations in impersonation of state institutions

02 Identity theft

If a victim experiences a loss of sensitive personal data, it can lead to further financial loss, as scammers can use information from a passport or ID card to open new bank accounts and take out loans in the victim's name without their knowledge. In the case of healthcare identity theft, the victim may lose healthcare benefits, while in tax identity theft, they may be left without a tax refund. Identity theft is a traumatic experience and has many other consequences, such as criminals using the victim's identity to commit crimes (including cybercrimes), potentially leading the victim to face legal consequences for actions they did not commit.

03 Loss of trust in public institutions

These types of scams can have a significant impact on individuals' trust in public institutions, as victims can feel a deep sense of betrayal and loss of trust in these institutions. This can cause them to become skeptical of genuine communications and less willing to cooperate, as they may begin to question legitimate requests and information, which leads to a lack of willingness to engage with government institutions. Increased concern about the potential for scams can also affect public opinion and reduce confidence in the ability of government bodies to effectively protect and serve citizens.

Manipulations in impersonation of state institutions

— WAYS OF PROTECTION WITH HISTORY IN THE BACKGROUND

Simon received a call from a person who, in an official tone, identified herself as an employee of the tax authority. She told him he owed back taxes and would be arrested and taken to jail if he did not immediately settle the debt by paying in one of the cryptocurrencies. Despite the caller being persistent and intimidating, Simon hung up the phone.
Shortly after ending the call, he received a message with the same content as the conversation, which also included a suspicious link to the tax authority's website.

Unfortunately for the scammer ...

Simon attended an educational lecture on government impersonation scams organized by the Tax Administration.

STEP 1: Recognizing the warning signs
Simon was initially scared, but he recognized signs of fraud when the caller mentioned paying outstanding tax obligations with cryptocurrency, which is not a standard method of tax payment.

STEP 2: Identifying an unusual behavior
Because the caller threatened arrest and imprisonment, Simon doubted the legality of such threats and promptly ended the call.

STEP 3: Verifying
Simon immediately checked if the phone number was associated with the relevant tax authority and found that it was not. The suspicious domain contained in the text message only confirmed his suspicions, so he blocked the number.

STEP 4: Reporting
Simon contacted the official tax authority using their official phone number and informed them of the attempted scam.

Manipulations in impersonation of state institutions

WAYS OF PROTECTION:

Here are some additional tips in case you might find yourself in such a situation.

Hang up, Delete, Don't reply:

Ignore calls, emails, texts, and messages on social media that claim to come from governmental institutions and ask you to pay, confirm sensitive information, or give other information.

The real governmental institution will never call, email, text, or message you on social media to demand money or information.

Do not maintain contact with scammers and do not provide your personal information or make any payments!

Legitimate institutions adhere to specific procedures and rules regarding payments, financial obligations, and other administrative matters, and they will never ask you to pay using payment methods such as cryptocurrencies, money transfer services, payment platforms, etc.

Manipulations in impersonation of state institutions

WAYS OF PROTECTION:

Do not rely on the contact information provided in emails and SMS!
Make sure you independently confirm the sender's identity before responding to correspondence purporting to be from a governmental institution.

To ensure the legitimacy of the communication look for the official contact information for the relevant agency and get in touch with them directly!

Immediately cut contact with anyone who tries to threaten or intimidate you!
Threats and intimidation can lead to emotional distress and psychological harm.

Remember!

Legitimate government institutions do not use threats of arrest or imprisonment to obtain payment of tax obligations or other debts.

If you have become a victim of scam and have transferred money only to later realize it was a scam, immediately contact your bank and file a complaint. Report the damage to the police.

If any other personal information has been disclosed during the scam, promptly notify the relevant institution that the scammers used for their scamming purposes.

Manipulation using deepfake technology

HAZARD CHARACTERISTICS:

Deepfake Fraud refers to a type of scam where artificial intelligence is used to create or alter video, audio, or images with the intention to deceive. This often involves creating synthetic content of an individual, mimicking their voice, facial expressions, and mannerisms to make it appear as if they are doing or saying something they did not. These fraudulent videos, audio clips, or images are often used to trick victims into parting with money, revealing sensitive information, or damaging reputations. Seniors, in particular, are frequently targeted due to their perceived vulnerability and lack of familiarity with such sophisticated technological threats. Deepfake fraud can also be employed for blackmail, extortion, spreading false information, or breaching security systems. Given the significant emotional and financial impact on seniors, it is crucial to raise awareness and educate them on how to recognize and protect themselves from these deceptive scams.

Types of deepfake fraud

Identitying Theft

This type of deepfake fraud involves creating a synthetic video of an individual to impersonate them. The fraudster can use this video to trick victims into believing they are interacting with the real person, leading to potential financial loss or theft of personal information.

False Information Dissemination

In this type of fraud, deepfakes are used to spread misinformation or propaganda. This could involve creating videos of public figures saying or doing things they never did, thereby misleading the public and influencing opinions or actions.

Security Breach

Deepfakes can also be used for breaching security systems that rely on facial recognition technology. By creating a synthetic video of an authorized individual, fraudsters can trick these systems and gain unauthorized access to sensitive areas or classified information.

Manipulation using deepfake technology

— CONSEQUENCES:

Deepfake fraud can have serious negative effects such as:

01 Financial Loss

Victims of deepfake fraud can suffer significant financial loss. This can occur when they are tricked into transferring funds or disclosing financial information based on deceptive deepfake content.

02 Emotional Distress

Being a victim of deepfake fraud can lead to severe emotional distress. The violation of personal identity and the potential exposure of personal information can leave victims feeling vulnerable and violated.

03 Damage to Reputation

Deepfake fraud can cause severe reputational damage to individuals and organizations. False information spread through deepfakes can undermine public trust and lead to loss of business, legal issues, and other negative consequences.

Manipulation using deepfake technology

CONSEQUENCES:

04 Disinformation

Deepfakes can be used to spread false information or propaganda, misleading the public and influencing opinions or actions. This can have serious social and political ramifications, such as undermining trust in institutions or manipulating election outcomes.

05 Identity Theft

Deepfake technology can be used to create synthetic videos or audio clips of individuals, leading to identity theft. Fraudsters can impersonate someone to gain access to personal information, financial resources, or secure systems.

06 Legal Consequences

The use of deepfake technology to commit fraud or disseminate false information can lead to legal consequences for both the perpetrators and the victims. Victims may face legal challenges in proving their innocence or reclaiming their reputation, while perpetrators can face criminal charges.

07 Social Trust Erosion

The prevalence of deepfakes can erode social trust, making people skeptical of the authenticity of digital content. This can lead to a general mistrust of media and information shared online, complicating communication and the spread of genuine information.

Manipulation using deepfake technology

— WAYS OF PROTECTION WITH HISTORY IN THE BACKGROUND

One day, Bill received an email from his grandson, Jack. The email contained a video where Jack was seemingly asking for help. He said he had lost his wallet while traveling and needed some funds to get back home. The video looked incredibly genuine, as it had Jack's voice and mannerisms down to the tee.

Bill, worried about his grandson, immediately transferred the funds. It was only later when he spoke to his daughter that he found out Jack had never made the trip in the first place.

Confused and shocked, Bill realized he had been a victim of a deepfake fraud. The video of Jack was not real but was a deepfake - a synthetic video produced using artificial intelligence.

This story emphasizes the vulnerability of seniors to deepfake fraud, highlighting the need for awareness and education among this demographic. Seniors, like Bill, may not be aware of such sophisticated scams, making them easy targets. The narrative underscores the importance of informing seniors about deepfake technology, teaching them how to verify requests for financial aid, and encouraging open communication within families to confirm the authenticity of such requests.

STEP 1: Verification
Always verify any requests for financial aid or sensitive information. For Bill, this means contacting his grandson directly through a known and trusted method, such as a phone call, to confirm the authenticity of the request before taking any action.

STEP 2: Education and Awareness
Bill should stay informed about the latest technological threats like deepfakes. Understanding how they work and how they can be used in scams will help him recognize potential fraud attempts and take protective measures.

STEP 3: Advanced Security Measures
Bill should use advanced security measures such as two-factor authentication for his email and social media accounts. This adds an extra layer of protection against unauthorized access and potential scams.

STEP 4: Open Communication
Bill should maintain open communication with his family about any unusual requests or messages he receives. By discussing these with trusted family members, he can quickly identify and avoid potential scams.

Manipulation using deepfake technology

WAYS OF PROTECTION:

Deepfake fraud can lead to significant financial loss, emotional distress, and damage to one's reputation. Additionally, seniors may face challenges in recovering from such scams, both financially and emotionally. By being aware of these threats and taking protective measures, seniors can safeguard their personal information, maintain their financial security, and uphold their dignity and peace of mind.

Education and Awareness:
Stay informed about deepfakes, their potential uses, and the latest tools available to detect them. Regularly update your knowledge about these threats and the protective measures against them.

Verification:
Always verify the source of videos, especially those prompting for financial aid or sensitive information. Contact the person appearing in the video through a trusted method to confirm its authenticity.

Manipulation using deepfake technology

WAYS OF PROTECTION:

Use of Advanced Security Measures: Employ advanced security measures such as two-factor authentication and biometric verification to secure your personal and financial information.

Rely on Trusted Sources: Only share sensitive information with trusted sources and via secure platforms. Be wary of unsolicited communications asking for personal details or financial information.

Report Suspicious Activity: If you encounter a potential deepfake, report it to the appropriate authorities. This could help prevent others from becoming victims and aid in the apprehension of the fraudsters.

Service fraud impersonating state institutions

HAZARD CHARACTERISTICS:

Service fraud that impersonates state institutions involves scammers pretending to be official government agencies or services. These fraudsters offer help with processing official documents, such as passports, visas, or social security benefits, but their real aim is to steal your personal information or money.

Types of manipulation in service fraud:

Impersonation of Official Services

Scammers create fake websites or send emails that look like they come from government agencies. They may use official logos and language to appear legitimate.

Urgent and Authoritative Language

These scams often use urgent language, warning you of consequences if you don't act quickly. This can include threats of fines, legal action, or missed deadlines.

Requests for Personal Information

They ask for sensitive information such as your Social Security number, bank account details, or passport information

Upfront Payments

The scammers request payment for their "services" upfront, often through untraceable methods like wire transfers, prepaid cards, or cryptocurrency

Lack of Direct Contact Information

Genuine government websites provide clear contact information and customer service options. Fake sites often have limited or fake contact details.

Service fraud impersonating state institutions

CONSEQUENCES:

Service fraud can have serious negative effects such as:

01 Legal and Administrative Problems

Using fake services can result in legal issues if the victim unknowingly submits fraudulent documents or fails to comply with legal requirements. This can lead to fines, penalties, or additional legal costs.

02 Identity Theft

Scammers often collect personal information under the guise of needing it for state-related services. This information can be used to steal the victim's identity, leading to unauthorized financial transactions, new accounts opened in their name, and other fraudulent activities.

03 Loss of Trust in Legitimate Institutions

After being scammed by someone posing as a state institution, seniors may become distrustful of real government agencies and officials. This can hinder their willingness to seek help or services they genuinely need

04 Financial Loss

Seniors may pay for fake services, such as processing fees for nonexistent benefits or assistance with official documents. This results in direct financial loss, which can be especially damaging for those on fixed incomes.

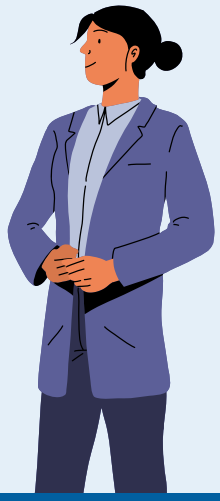
Service fraud impersonating state institutions

— WAYS OF PROTECTION WITH HISTORY IN THE BACKGROUND

Grace receives an email claiming to be from the Government, stating that her passport needs urgent renewal to avoid penalties. The email provided a link to a website that looked official, with the department's logo and formal language. The website asked for personal information and a euro 150 fee to expedite the renewal process. What should Grace do?

Service fraud impersonating state institutions can lead to severe financial and emotional harm, especially for seniors. By verifying the source of information, being skeptical of urgent requests, protecting personal information, and using safe payment methods, you can safeguard yourself from these scams.

Always ensure you are interacting with genuine government websites and services to avoid falling victim to fraudulent schemes.



Step 1. Verify the source

Check the Department of State's official website directly or call their customer service to confirm the renewal process.

Step 2. Be skeptical of urgent requests

Recognize that genuine government agencies will not send urgent renewal requests via email.

Step 3. Do not share personali information

Avoid entering your personal information on the provided website until you verify its authenticity.

Step 4. Use safe payment methods

Be cautious about payment requests and verify if the government provides such fees and services.

Service fraud impersonating state institutions

WAYS OF PROTECTION:

Protecting yourself from service fraud impersonating state institution is crucial for safeguarding your personal information, your money and your emotions. Here are some straightforward steps you can take.

Do Not Share Personal Information:

Avoid providing sensitive information such as your Social Security number, bank details, or passport information online unless you are certain the website is legitimate.

Verify the Source:

Ensure you are on an official government website. Look for ".gov" in the web address, which is used by government institutions. Contact the government agency directly using information from an official source, not the contact details provided in the suspicious email or website

Be Skeptical of Urgent Requests:

Be cautious if you receive urgent or threatening messages demanding immediate action or payment. Genuine government agencies do not operate this way.

Fraud through fake accounts

HAZARD CHARACTERISTICS:

Blackmailing using fake accounts refers to a deceptive practice where fraudsters create counterfeit social media profiles, often impersonating someone the victim knows or trusts. This scam particularly targets seniors, who may be less familiar with digital platforms. Fraudsters typically initiate contact by sending friend requests, then proceed to share explicit or harmful content. The fraudster then demands money or other forms of payment, threatening to damage the senior's reputation by linking them to the inappropriate content.

Types of blackmailing using fake accounts:

Impersonation of a Friend or Acquaintance

The scammer creates a fake account pretending to be someone the victim knows, gains their trust, and then uses this trust to initiate the blackmail.

Catfishing

The scammer creates a fake identity, often a person who is romantically interested in the victim. Once the victim is emotionally invested, the scammer starts the blackmail.

Impersonation of a Celebrity or Public Figure

The scammer creates a fake account of a celebrity or public figure. They then contact fans or followers, sharing explicit content and demanding money with the threat of tarnishing the fan's reputation.

Fraud through fake accounts

CONSEQUENCES:

Blackmailing using fake accounts can have serious negative effects such as:

01 Emotional and Psychological Distress

One of the primary impacts a victim may face is significant emotional and psychological distress. This is often a direct result of the relentless threats and constant harassment perpetrated by the fraudster. Such distress can manifest in numerous ways, including fear, anxiety, depression, and sleep disturbance, significantly affecting the victim's everyday life.

02 Financial Loss

A further risk that victims are exposed to is the potential for considerable financial loss. This typically occurs when the victim, feeling cornered and overwhelmed by the fraudster's unyielding demands, ultimately gives in. As a result, they may experience not only the loss of their hard-earned money but also the stress and anxiety that accompanies such loss.

03 Damage to Reputation

Lastly, there's the risk of severe damage to the victim's reputation. This can occur if the fraudster decides to follow through with their threats, potentially releasing damaging or sensitive information about the victim. This could lead to a significant decline in the victim's social standing and could affect their personal and professional relationships, as well as future opportunities.

Fraud through fake accounts

WAYS OF PROTECTION WITH HISTORY IN THE BACKGROUND

One day, Susan received a friend request from an account bearing the name of a long-lost friend. Delighted by the prospect of reconnecting, she accepted the request. Soon after, they started exchanging messages, reminiscing about old times. However, things turned sinister when the friend started sharing explicit content and demanded money, threatening to tarnish her reputation by associating her name with the content.

Shaken by the abrupt change, Susan decided to reach out to her actual friend through a different medium. When she learned that her friend had no knowledge of this account, she realized that she had been interacting with a fake account.

This story underscores the importance of educating seniors on the potential risks of interacting with unknown entities online. It highlights how seniors can be targeted by scams such as blackmailing through fake accounts, due to their potential lack of familiarity with digital platforms. The story serves as a reminder to seniors to verify the identities of individuals before engaging with them online and to report any suspicious activities to the platform or local authorities. It emphasizes the need for awareness and vigilance in the digital world to protect their well-being and financial security.

STEP 1: Verify friend requests
Susan accepted a friend request from an account she believed to be a long-lost friend without verifying its authenticity. Susan should have contacted her actual friend through another medium to verify the authenticity of the friend request before accepting it.

STEP 2: Be cautious with personal information
Susan engaged in conversations and shared personal memories without suspecting any foul play. Susan should have been cautious and avoided sharing personal information or engaging in sensitive conversations until she was certain of the other party's identity.

STEP 3: Recognize suspicious behavior
Susan continued to interact with the account even after they started sharing explicit content and making demands. Upon noticing the suspicious behavior, Susan should have immediately stopped engaging with the account and flagged it as suspicious.

STEP 4: Report and educate
After realizing the account was fake, Susan reported the incident and shared her experience with friends and family. Susan's actions in reporting the account and educating others were appropriate. She should continue to advocate for awareness and vigilance against online scams.

Fraud through fake accounts

WAYS OF PROTECTION:

Protecting yourself from blackmailing using fake accounts is crucial, especially for seniors, because it helps prevent emotional and psychological distress, financial loss, and damage to reputation. Seniors may be more vulnerable to these scams due to a potential lack of familiarity with digital platforms. By being vigilant and cautious online, seniors can safeguard their well-being and financial security, ensuring a safer and more enjoyable online experience.

Verification of Friend Requests:
Always authenticate the identity of the individual sending a friend request, particularly if you haven't been in contact with them for some time. This can be done by reaching out to them through another medium that you have previously used to communicate.

Privacy Settings:
Ensure that your social media accounts are set to the highest privacy settings. This will limit the amount of information that can be seen by individuals who are not on your friends list.

Fraud through fake accounts

WAYS OF PROTECTION:

Do Not Share Sensitive Information:
Avoid sharing personal or sensitive information online. If the person you are communicating with starts behaving suspiciously or demanding money, stop the conversation immediately.

Report Suspicious Activity:
If you encounter a suspicious account, or if someone starts sharing inappropriate content or making threats, report the account to the social media platform and your local authorities.

Educate Yourself and Others:
Learn about the common signs of online scams and teach others about these signs as well. This can help you and your loved ones avoid falling victim to such scams.

Further readings

ALLEGATIONS OF INVOLVEMENT IN CRIME

- https://www.legalmatch.com/law-library/article/allegations-of-criminal-involvement.html
- https://www.findlaw.com/criminal/criminal-charges/defending-against-criminal-charges.html
- https://www.nolo.com/legal-encyclopedia/criminal-defense-strategies
- https://www.lawinfo.com/resources/criminal-defense/
- https://www.justia.com/criminal/
- https://www.avvo.com/topics/criminal-charges
- https://www.legalzoom.com/articles/what-to-do-if-youre-accused-of-a-crime
- https://www.hg.org/criminal.html https://www.lawyers.com/legal-info/criminal/
- https://www.americanbar.org/groups/criminal_justice/

MANIPULATIONS IN IMPERSONATION OF STATE INSTITUTIONS

- https://www.ncoa.org/article/government-imposter-scams-what-they-are-and-how-to-spot-them
- https://www.nia.nih.gov/news/high-vulnerability-government-impersonation-scams-among-older-adults
- https://www.idnow.io/glossary/impostor-fraud/
- https://www.thomsonreuters.com/en-us/posts/investigation-fraud-and-risk/senior-citizens-financial-scams/
- https://consumer.ftc.gov/articles/how-avoid-government-impersonation-scam#whattoknow
- https://regtechtimes.com/government-impersonation-scams-your-shield/
- https://www.europol.europa.eu/media-press/newsroom/news/beware-of-scams-involving-fake-correspondence-europol

Further readings

MANIPULATION USING DEEPFAKE TECHNOLOGY

- https://www.bitdefender.com/blog/labs/deepfakes-what-they-are-how-they-work-and-how-to-protect-against-malicious-usage-in-the-digital-age
- https://mitsloan.mit.edu/ideas-made-to-matter/deepfakes-explained
- https://www.media.mit.edu/posts/deepfakes-explained/
- https://www.sentinelone.com/blog/what-are-deepfakes-how-can-you-spot-them/
- https://www.datavisor.com/blog/how-deepfakes-are-made-and-how-fraudsters-use-them/
- https://www.iproov.com/blog/deepfake-fraud-identity-theft-explained
- https://techmonitor.ai/technology/ai-and-automation/audio-deepfake-scams-the-growing-threat-explored
- https://readwrite.com/are-deepfakes-illegal-ais-dark-side-explained/

SERVICE FRAUD IMPERSONATING STATE INSTITUTIONS

- https://www.c-span.org/video/?468676-1/social-security-scams
- https://www.nia.nih.gov/news/high-vulnerability-government-impersonation-scams-among-older-adults
- https://www.bressler.com/news-1882
- https://consumer.ftc.gov/articles/how-avoid-government-impersonation-scam
- https://www.facebook.com/europol/videos/%EF%B8%8F-beware-scammers-impersonating-europol-officers-europol-never-contacts-members-/1097501060976901/?_rdr

Further readings

FRAUD THROUGH FAKE ACCOUNTS

- https://www.malwaretips.com/i-have-your-secrets-fake-blackmail-sextortion-scam-email
- https://www.microsoft.com/en-us/microsoft-365-life-hacks/privacy-and-safety/sextortion-scams
- https://www.scamnet.wa.gov.au/scamnet/Fight_back.htm
- https://www.antivirus.com/blackmail-and-sextortion-emails
- https://www.malwaretips.com/hello-perv-blackmail-emails-are-fake
- https://www.womenslaw.org/about-abuse/abuse-using-technology/impersonation
- https://www.minclaw.com/how-to-deal-with-google-chat-blackmail
- https://www.digitalinvestigation.com/blog/blackmail-on-tiktok
- https://www.justice.gov/opa/pr/us-law-enforcement-joins-international-partners-disrupt-international-sextortion-ring
- https://www.cyber.gov.au/acsc/view-all-content/publications/sextortion-scams

www.cybersafesenior.eu

Cyber-Safe-Senior

Funded by
the European Union

CYBER SAFE
SENIOR

Instytut
Nowych Technologii

Institute of Entrepreneurship Development
iED

İLKSENOL
DERNEĞİ

SIMBIOZA
MED GENERACIJAMI

"Funded by the EU. The views and opinions expressed are those of the author(s) and do not necessarily reflect the views of the European Union or the Erasmus+ National Agency.
The European Union nor the grantor is not responsible for them."