Online threats for 55+ - glossary

Phishing (fraudulent emails, SMS, links, voice calls)

Phishing is a type of cyberattack where criminals send fake emails, text messages, phone calls, or links pretending to be someone you trust, like a bank or a friend. Their goal is to trick you into giving out important personal information such as passwords, credit card numbers, or bank account details. These fake messages often look very real and try to make you act quickly by creating a sense of urgency or fear. The attackers want to steal your money or identity by fooling you into clicking on dangerous links or sharing sensitive data. To stay safe, always double-check who sent the message, avoid clicking on suspicious links, and never share personal information unless you are absolutely sure it is safe.

Deepfake attacks (fake audio/video, impersonating family)

Deepfake attacks involve creating fake audio or video recordings using artificial intelligence that look and sound very real. In these attacks, criminals imitate the voice or face of someone known, often a family member, to trick people into believing they are talking to a loved one. For example, a scammer might use deepfake technology to make a phone call that sounds exactly like a grandchild asking for money urgently. These fake recordings are very convincing and can fool even careful people. Deepfake attacks are dangerous because they exploit trust and emotions, making it hard to realize the deception until it’s too late. To protect yourself, always verify unusual requests by contacting the person directly through different communication channels before taking any action.

Fake online stores and scams (counterfeit websites)

Fake online stores and scams are fraudulent websites designed to look like legitimate shops but are actually created to trick people into buying products that don’t exist or are of poor quality. These fake stores often copy logos, product descriptions, and photos from real companies to appear convincing. Scammers use these sites to steal money and personal information from unsuspecting customers. They lure buyers with promises of very low prices or special offers that seem too good to be true. These websites might have strange web addresses, contain spelling mistakes, or lack proper contact details. After customers pay, they often never receive their order or get fake goods. To protect yourself, always buy from trusted stores, check website reviews, avoid deals that seem unrealistically cheap, and never share payment information on suspicious sites.

Emotional manipulation and social engineering (scare tactics)

Emotional manipulation and social engineering involve tricking people by playing on their feelings to make them act in ways they normally wouldn't. Cybercriminals use tactics like scare stories, urgency, fake authority, or kindness to create a sense of fear, trust, or obligation. For example, they might pretend to be a bank officer warning you about a problem with your account, urging you to act quickly, so you provide sensitive information without thinking. These tactics exploit natural human responses—fear, trust, curiosity, or helpfulness—making it difficult to resist. The best defense is awareness: recognizing these emotional tricks and pausing to verify who is really asking for information before responding.

Identity theft
(using stolen personal data)

Identity theft means when someone steals your personal information without your permission and uses it to pretend to be you. They might use your name, social security number, bank account details, or other data to open accounts, take out loans, or make purchases in your name. This can cause big money problems and damage your reputation.

Fraud “on the grandchild” (imposters pretending to be family in distress)

Fraud “on the grandchild,” also known as the “grandparent scam,” is a common method used by criminals who pretend to be a family member—usually a grandchild or child—in distress. This usually happens over the phone, where the scammer calls an older person and claims they are in serious trouble, such as having an accident, being arrested, or needing urgent financial help. The caller often asks for money to be sent quickly and insists that the victim keep it a secret, for example by saying, "Don’t tell mom, she’ll worry." This scam plays on emotions like love and concern for family members, making the person want to help immediately without stopping to think. Increasingly, scammers use technology like artificial intelligence to imitate the voice of the real grandchild, making the call sound very convincing.

Fake “help” requests via WhatsApp or Messenger

Fake “help” requests via WhatsApp or Messenger are scams where someone pretends to be a friend or family member in urgent trouble, asking for money or personal information. These messages often come unexpectedly from unknown or disguised contacts. The scammer may say they lost their phone, got locked out of their account, or need emergency financial help. They try to create a sense of urgency and trust to make victims act quickly without checking if it's true.

Romance scams and fraud based on relationships built online

Romance scams are a type of fraud where criminals create fake online profiles and pretend to be romantically interested in someone. They build trust and emotional connection over time, making the victim believe they are in a genuine relationship. Once they gain trust, scammers invent emergencies or urgent financial needs—such as medical bills or travel costs—and ask the victim for money or gifts.

These scammers are very skilled at appearing caring and trustworthy, often avoiding in-person meetings or video calls by giving excuses. They exploit loneliness and emotional vulnerability, which makes victims more likely to give them money.

Investment fraud (fake advertisements with celebrities)

Investment fraud involving fake advertisements with celebrities is a type of scam where criminals use images, videos, or names of famous people to make an investment opportunity seem legitimate and trustworthy. Sometimes these ads feature deepfake videos showing celebrities endorsing an investment, or they pose as news articles linking celebrities to financial success with certain platforms. The scammers trick people into believing they can make quick and large profits, often in cryptocurrencies or foreign exchange trading. They lure victims into creating accounts, depositing money, and then ask for more funds to pay fake fees or taxes. Early returns may be shown to gain trust, but when victims try to withdraw their money, they are blocked and asked for large additional payments.

Malware and ransomware (infected files, attachments)

Malware is malicious software that can infect your computer or phone and cause harm, such as stealing your personal information, damaging files, or taking control of your device. Ransomware is a special type of malware that locks or encrypts your files, making them inaccessible until you pay a ransom—usually in cryptocurrency—to the attacker. The ransomware may enter your device through infected email attachments, malicious websites, or unsafe downloads. Once infected, ransomware prevents you from using your important files and sometimes demands money to restore access. Paying the ransom does not guarantee that your data will be released, and it encourages criminals to continue these attacks.

Unverified apps and unsafe software downloads

Unverified apps and unsafe software downloads are cyber threats where people download and install applications or files from unknown or unreliable sources. These apps or downloads may contain hidden malware, viruses, or spyware that can harm your device, steal personal information, or give hackers unauthorized access.

Because these apps are not checked or approved by trusted platforms, they can interfere with your device’s security, cause crashes, or expose you to scams. Fake apps might look like real ones, but when installed, they can collect your data or spread harmful software.

Sharing sensitive data with strangers (photos, information)

Sharing sensitive data with strangers, such as photos or personal information, is a cyber threat where people give away private details to unknown or untrusted people online. This can seem harmless, like sharing a photo, but these details can be misused to steal your identity, commit fraud, or harm your reputation.

Photos might reveal your home, location, or personal habits without you realizing it. Strangers can use this information to trick you or target you in scams. To stay safe, only share personal information and photos with people you trust, think carefully before posting online, and adjust privacy settings to limit who can see your information.

Data leaks from using outdated devices or software

Using outdated devices or software is a cyber threat because old versions often lack the latest security updates. These missing updates create weaknesses, called vulnerabilities, that hackers can easily exploit to access your personal information or control your device. This can lead to data leaks, theft, or infection by malware.

Outdated software also slows down your device and may stop working with newer programs, making your everyday activities harder. To protect yourself, it’s important to regularly update your device and software with the latest patches and security fixes. This closes security gaps, keeps your data safer, and ensures your device runs smoothly.

Mass-personalized attacks using AI, targeting user profiles

Mass-personalized attacks using AI are cyber threats where attackers use artificial intelligence to create highly customized and convincing messages targeted at individuals based on their personal data. AI analyzes information from social media, emails, and public sources to craft messages that look very familiar and trustworthy to the target.

These attacks can include personalized phishing emails or messages that mention the victim's name, job, recent activities, or interests. The goal is to trick people into clicking malicious links, revealing passwords, or transferring money. Because AI constantly learns and adapts, these attacks become more effective and harder to detect.

Health misinformation or dangerous medical advice from AI tools

Health misinformation or dangerous medical advice from AI tools is a cyber threat where artificial intelligence generates incorrect, misleading, or harmful health information. People may trust AI chatbots or online tools for medical advice, but sometimes these systems produce wrong diagnoses, suggest unsafe treatments, or spread false claims about diseases.

This misinformation can lead to people delaying proper medical care, using ineffective remedies, or taking harmful actions. AI-generated content may sound very professional and convincing, making it difficult to tell if the advice is reliable.

Scams exploiting digital exclusion in civic and banking services

Scams exploiting digital exclusion in civic and banking services are threats targeting people who have limited access to or knowledge of digital technologies. These scams take advantage of people who struggle to use online government or bank services, sometimes because they lack devices, internet access, digital skills, or confidence.

Criminals trick these individuals by offering fake help with online processes or by sending fraudulent messages mimicking official institutions, hoping victims will share sensitive data or send money. Because these people have fewer resources or support to recognize scams, they are more vulnerable.

Lack of multi-factor authentication practices (simplified passwords, re-use)

Lack of multi-factor authentication (MFA) means using only a password—often simple or repeated on many sites—to protect online accounts. This is risky because if someone steals or guesses your password, they can easily get into your accounts.

Multi-factor authentication adds an extra layer of security by requiring two or more forms of verification. For example, after typing your password, you might enter a code sent to your phone or use a fingerprint scan. This makes it much harder for hackers to access your account, even if they have your password.

Automated manipulation of social media feeds, producing misinformation and stress

Automated manipulation of social media feeds is a cyber threat where computer programs, called bots, and artificial intelligence control what content you see on your social media pages. These systems analyze what you like, share, or comment on, and then show you more similar posts to keep you engaged.

Unfortunately, this can be used to spread misinformation, fake news, or extreme content that causes stress, fear, or anger. Bots can artificially boost the popularity of such posts by liking, sharing, or commenting, making it seem like many people agree with them.