SILWERS

SENIORS ARTIFICIAL INTELLIGENCE LEARNING – WELL EDUCATED AND RISK SECURE

Co-funded by the European Union

Expert fora report

Erasmus+ KA220-ADU – Cooperation partnerships in adult education, Project No: ***2024-1-IS01-KA220-ADU-000256952***

Panel Objectives

1. Discussion of difficulties and concerns this group faces with new technologies along with identification of AI application areas and related risks.
2. Identification of current and future online threats for people 55+.
3. Presentation of real-life examples of incidents and benefits from AI use.
4. Definition of critical digital competencies for people 55+.

Results- Poland

Most Cited Online Threats for 55+

People aged 55 and over face unique challenges in the digital world, making them vulnerable to a variety of online threats.

Understanding the most common and impactful dangers is essential to improving their cybersecurity awareness and protection.

Online threats for 55+

- Phishing fraudulent emails, SMS, links, voice calls
- Deepfake attacks fake audio/video, impersonating family
- Fake online stores and scams counterfeit websites
- Emotional manipulation and social engineering scare tactics
- Identity theft using stolen personal data

Online threats for 55+

- Fraud on the grandchild imposters pretending to be family in distress
- Fake help requests via WhatsApp or Messenger
- Romance scams and fraud based on relationships built online
- Investment fraud fake advertisements with celebrities
- Malware and ransomware infected files, attachments

Online threats for 55+

- Unverified apps and unsafe software downloads
- Sharing sensitive data with strangers photos, information
- Using outdated devices or software
- Mass-personalized attacks using AI, targeting user profiles
- Health misinformation or dangerous medical advice from AI tools

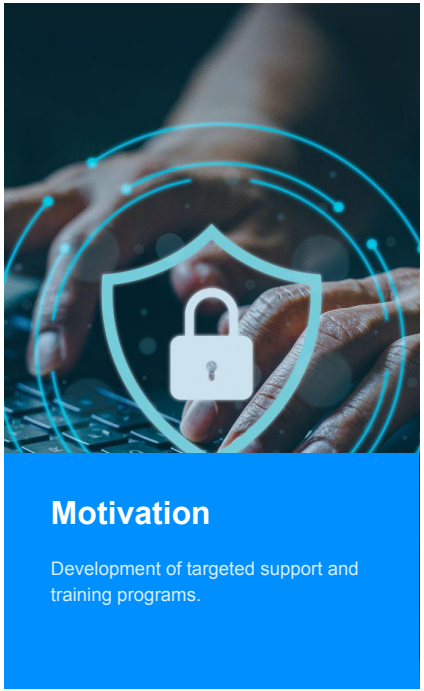
Online threats for 55+

- Scams exploiting digital exclusion in civic and banking services
- Lack of multi-factor authentication practices simplified passwords, re-uses
- Loss of access to critical services due to technological changes app-only access, limited alternatives
- Automated manipulation of social media feeds, producing misinformation and stress
- Password, identification, biometry, 2FA

Top 10 Concerns According to Experts

Experts highlighted key concerns that most affect people aged 55 and over when interacting with digital technologies.

Addressing these concerns is crucial for enhancing their confidence and safety in everyday online activities.



Top 10 Concerns According to Experts

- **Technological change** and complexity: Rapid pace of technology makes it hard for seniors to adapt, especially with updates and new devices.
- Fear and **emotional manipulation**: Scams frequently exploit emotions, such as fear or urgency, making seniors more vulnerable.
- **Social exclusion** and loneliness: Reduced contact with family and friends, often increased by digital communication replacing direct interactions.
- **Hesitation to ask for help:** Seniors often feel shame or embarrassment about asking younger people for assistance with technology.
- **Financial limitations**: Reluctance or inability to spend money on new devices or software, resulting in outdated, insecure technology.

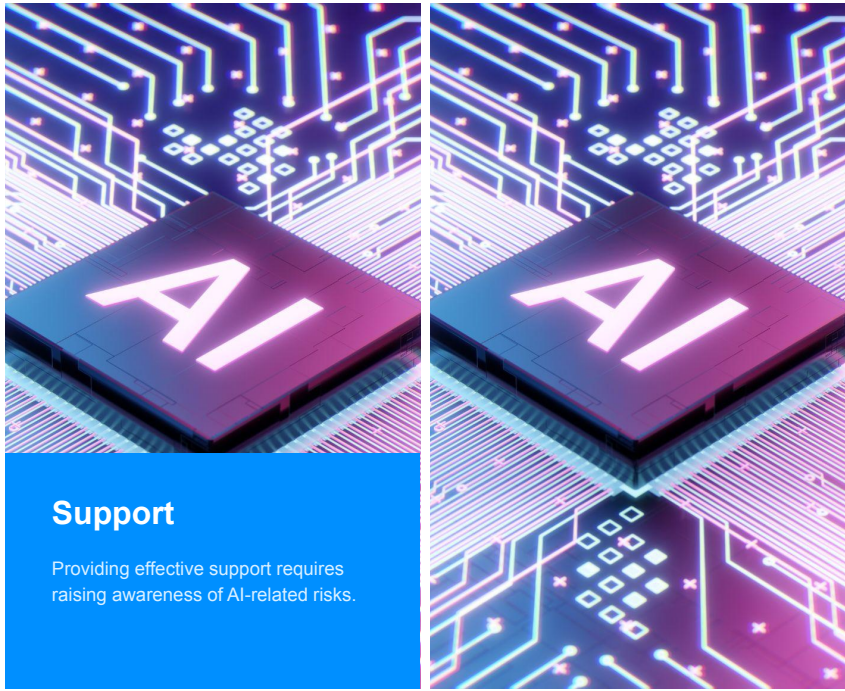
Top 10 Concerns According to Experts

- **Digital exclusion** in services: Everyday tasks (like buying tickets, banking, medical appointments) are increasingly moved online, leaving seniors without alternatives.
- Low **digital competence**: Lack of basic skills and experience, sometimes exacerbated by not having computer education earlier in life.
- Impulsiveness and **risky decisions**: A tendency to act quickly when confronted with technology problems—sometimes leading to mistakes or falling for scams.
- **Vulnerability** to misinformation: Trouble distinguishing true information from digital manipulation, especially online.
- Device and **software maintenance issues**: Problems with updating devices, managing passwords, and understanding digital security best practices, increasing risk.

Key AI Usage Areas and Cyber Risks

Artificial intelligence is increasingly integrated into many aspects of daily life, offering significant benefits but also introducing new cybersecurity risks.

Understanding the main AI application areas and their associated threats is essential for protecting vulnerable groups such as people aged 55 and over.



Support

Providing effective support requires raising awareness of AI-related risks.

Key AI Usage Areas and Cyber Risks

- **Personal assistants** in phones and devices (e.g., voice assistants like Alexa) that support seniors in daily tasks but require understanding privacy and security.
- AI in **healthcare monitoring** (wearables, anomaly detection in heart rate) that provides early warnings but needs trust and basic digital skills to operate.
- AI-powered fraud and **scam detection** (phishing identification, deepfake recognition) to protect seniors from targeted attacks but requiring knowledge of recognizing suspicious content.

Key AI Usage Areas and Cyber Risks

- AI-generated **personalized attacks** that adapt to individual seniors' behavior and emotions, making online threats harder to detect.
- **Content generation** and misinformation via AI (deepfakes, false ads, fake news) influencing decisions and causing confusion among seniors lacking critical evaluation skills.
- AI in **smart home** and IoT devices assisting daily life but posing risks if devices are unsecured or poorly managed.
- AI-assisted travel and **leisure planning** helping organize trips and activities, enhancing comfort but requiring some digital literacy for safe use.

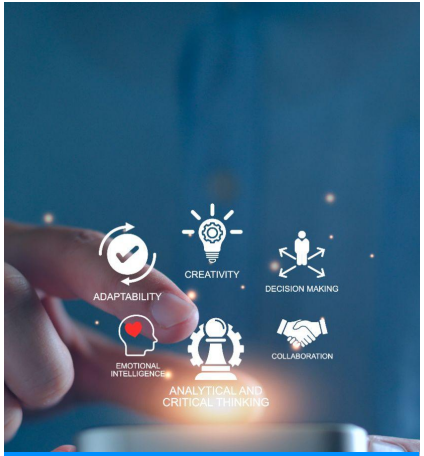
Key AI Usage Areas and Cyber Risks

- Automated **social interaction** bots simulating human conversation, often used in scams or isolation reduction, needing awareness to avoid deception.
- AI in digital **financial services** automating transactions and banking that can improve accessibility but demand knowledge of security practices and fraud prevention.
- AI tools in **communication** with family and caregivers (real-time monitoring, emergency alert systems) enhancing safety but requiring competence in setup and interpretation.

Critical Competencies for Seniors

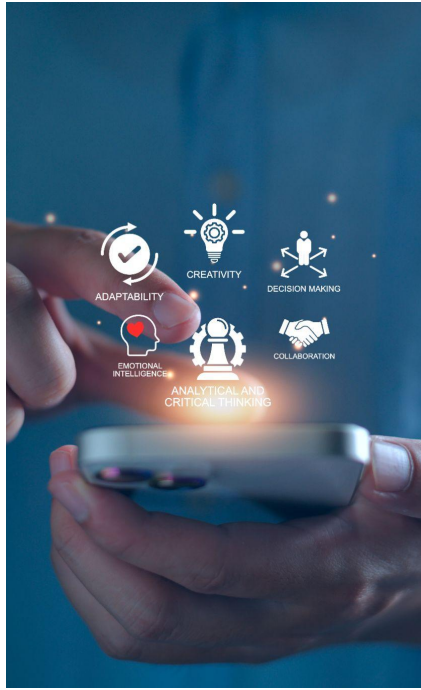
Developing essential digital competencies is vital to empower seniors to navigate the online world safely and confidently.

These skills help them effectively utilize technology to enhance their everyday life and resilience against cyber threats.



Competencies

Enable seniors to better protect themselves and confidently engage with modern technologies.



Critical Competencies for Seniors

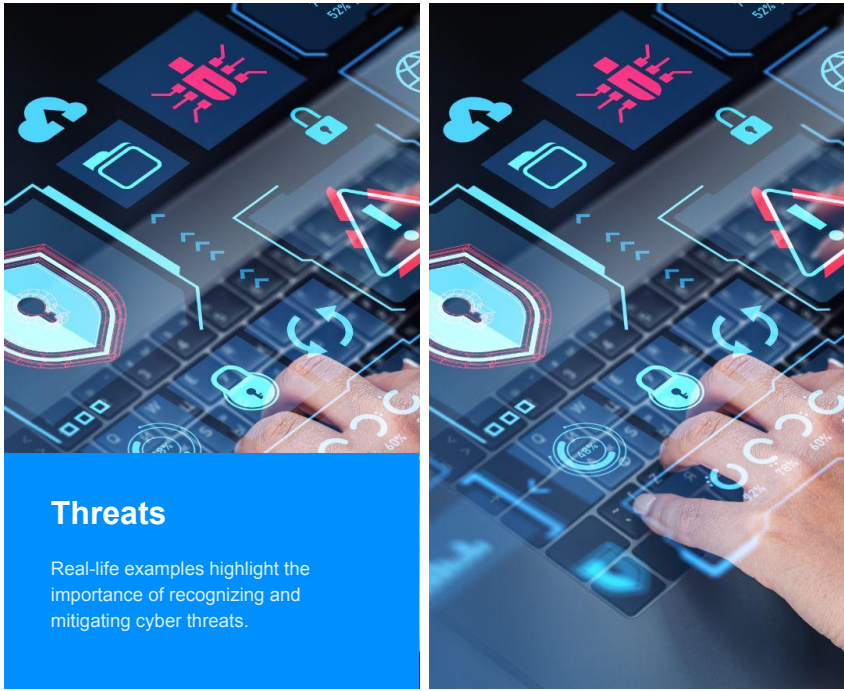
- **Understanding** basic digital device operation and security settings.
- **Recognition** of AI-driven manipulation and fraudulent content.
- **Digital literacy** to safely interact with AI assistants and smart devices.
- **Awareness** of data privacy and protection measures in AI applications.
- **Ability** to seek trustworthy information and validate AI-generated content.

Critical Competencies for Seniors

- Emotional **resilience** to avoid being manipulated by AI-driven scams.
- **Comfort** with basic troubleshooting and maintenance of digital tools.
- **Knowledge** of secure password management and authentication practices.
- Competence to **use** AI tools for health, safety, and communication.
- **Openness** to continuous learning due to the rapid development in AI technologies.

Real-life Threats Identified by Experts

Experts shared real-life examples illustrating both the risks and benefits of digital technologies for people aged 55 and over. These cases provide valuable insights into common cyber threats of artificial intelligence on seniors' daily lives.



Real-life Threats Identified by Experts

- Use of **deepfake** technology to impersonate a family member: A senior receives a phone call where the caller, using a convincingly simulated voice of a grandchild or child, claims to need immediate money (e.g., for an accident). The senior, convinced by the emotional manipulation and the familiarity of the voice, transfers money, often using BLIK or bank transfer.
- Romance **scams** involving AI: Seniors are targeted online by individuals (sometimes chatbots or automated profiles) who develop emotional “relationships” and then request money under false pretenses, exploiting loneliness and trust.

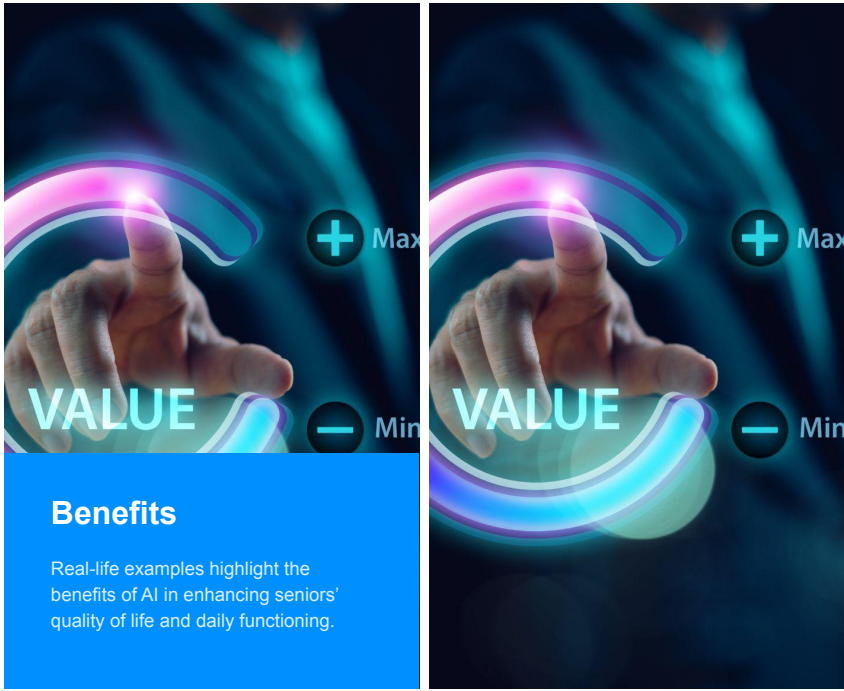
Real-life Threats Identified by Experts

- Fake **lottery** or prize win: A senior is informed, often through a call or email using AI-generated content, that they have won a large sum of money. To claim it, they are asked for a deposit or personal information, resulting in financial loss and sometimes identity theft.
- **Manipulation** through fake online stores: Seniors unknowingly purchase goods from websites that are almost identical to legitimate stores (with a minor spelling change in the address or name). They pay for goods that never arrive, falling victim to sophisticated AI-based phishing sites.
- AI-facilitated medical **misinformation**: Seniors consult AI chatbots or online tools for health advice. Sometimes, the advice is misleading, causing them to skip consulting their doctor or even take incorrect medications, which can be dangerous to their health.

Real-life Benefits Identified by Experts

Experts shared real-life examples illustrating both the risks and benefits of digital technologies for people aged 55 and over.

These cases provide valuable insights into benefits of artificial intelligence on seniors' daily lives.



Real-life Benefits Identified by Experts

- A senior used an AI-powered travel **planning** tool to organize a trip, specifying dates and personal interests (like museums or outdoor activities), receiving a detailed, tailored itinerary—making the trip easier and more enjoyable.
- AI-driven medical **diagnostic** tools identified early warning signs of health issues (such as irregular heart rhythms in pacemaker and diabetes patients), leading to timely medical intervention and improved well-being.
- Seniors leveraged AI personal **assistants** (like Alexa) for daily reminders (e.g., medication times and appointments), household management, and maintaining social contact, reducing loneliness and increasing independence.

Real-life Benefits Identified by Experts

- An example involved smart **wearable** devices (AI-powered wristbands) that continuously monitored key health metrics for seniors living alone, alerting caregivers or emergency services automatically in case of anomalies or emergencies.
- AI image **recognition** and search helped a senior identify an unknown plant in their garden, providing instant guidance on care, thus improving gardening skills and confidence.

Results - Czech Republic

Most Cited Online Threats for 55+

People aged 55 and over face unique challenges in the digital world, making them vulnerable to a variety of online threats. Understanding the most common and impactful dangers is essential to improving their cybersecurity awareness and protection.

Online threats for 55+

- Phishing attacks, including emails, SMS, and phone calls where attackers impersonate banks or trusted institutions to steal sensitive data.
- Fake online shops and scams targeting seniors with fraudulent offers and websites.
- Identity theft, where personal data is misused to gain money or impersonate the victim.
- Manipulation through short videos and disinformation, including fabricated news and subliminal messages.

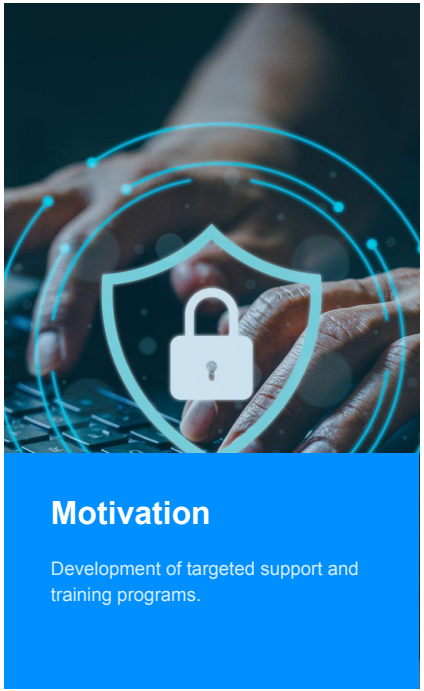
Online threats for 55+

- Inadequate IT maintenance, such as outdated firmware and ignored security updates, resulting in vulnerable systems.
- Fraud exploiting loneliness—scammers initiating fake friendships or romantic relationships.
- Unsafe synchronization between devices and storing passwords insecurely in browsers.
- Growing threat of AI-driven fraud, including cloned voices impersonating relatives for urgent financial help.
- Rising risks due to AI in antivirus programs, making configuration and secure usage critical for seniors.

Top 10 Concerns According to Experts

Experts highlighted key concerns that most affect people aged 55 and over when interacting with digital technologies.

Addressing these concerns is crucial for enhancing their confidence and safety in everyday online activities.



Top 10 Concerns According to Experts

- **Difficulty keeping up** with the complexity and rapid evolution of technology.
- **Fear of losing access** to personal data or finances and falling victim to scams.
- **Embarrassment** or loss of confidence when unable to use technology in front of family.
- **Dependence** on others (relatives or technicians) which hinders building independence.
- Public Wi-Fi safety, often used by seniors without **security awareness.**

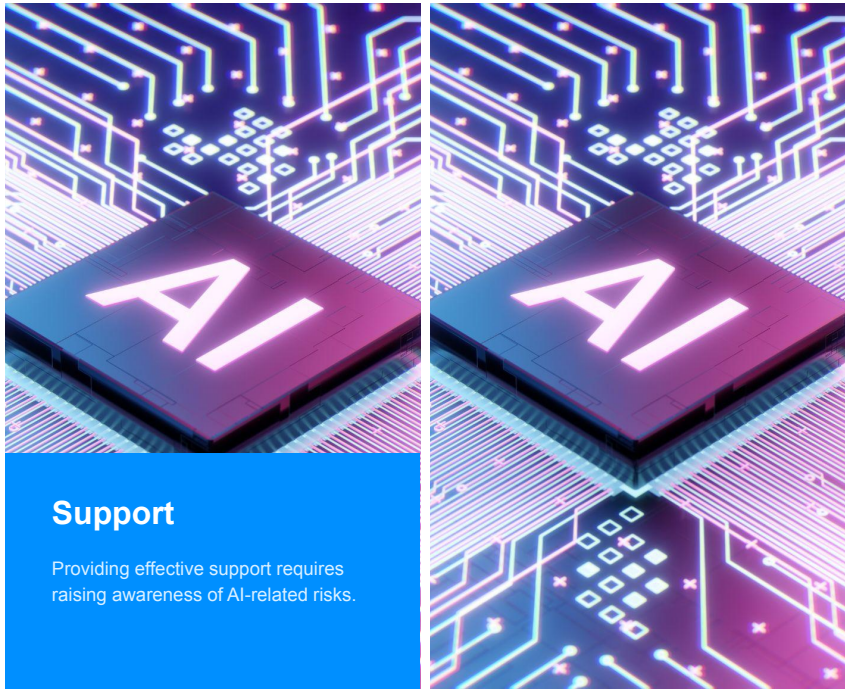
Top 10 Concerns According to Experts

- **Unsafe password** storage, such as using browsers instead of password managers.
- **Digital communication** replacing valued face-to-face contact, leading to social isolation.
- Disabling updates or security features due to **lack of understanding**, exposing devices to vulnerabilities.
- **Struggling with changing system** layouts, icons, or unexpected new features.
- Inability to recognize **suspicious or manipulated content**, making seniors more susceptible to deception.

Key AI Usage Areas and Cyber Risks

Artificial intelligence is increasingly integrated into many aspects of daily life, offering significant benefits but also introducing new cybersecurity risks.

Understanding the main AI application areas and their associated threats is essential for protecting vulnerable groups such as people aged 55 and over.



Support

Providing effective support requires raising awareness of AI-related risks.

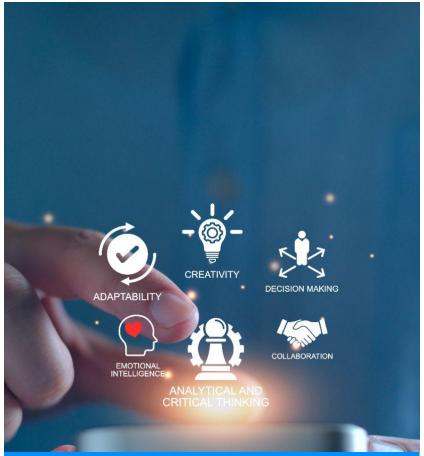
Key AI Usage Areas and Cyber Risks

- **AI in healthcare:** telemedicine, health monitoring, and translation for communication with family.
- **Daily support:** AI voice assistants, smart home devices, antivirus tools.
- Risk of **data manipulation**, deepfake attacks, and spread of disinformation.
- AI-enabled **voice cloning** impersonating relatives, leading to financial fraud.
- **Overreliance on AI tools** without understanding their limitations—AI should be seen as a tool, not an infallible authority.

Critical Competencies for Seniors

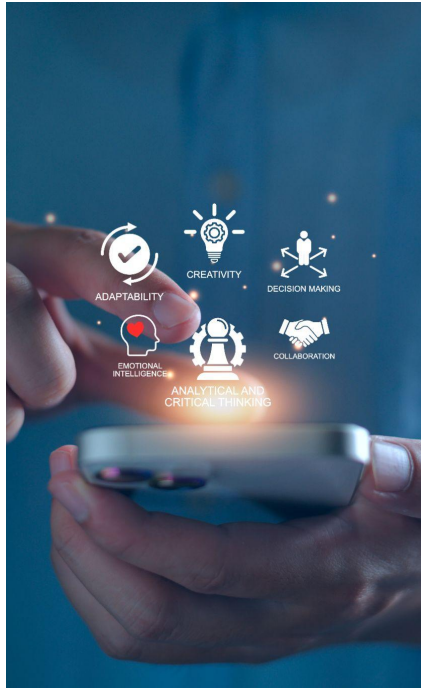
Developing essential digital competencies is vital to empower seniors to navigate the online world safely and confidently.

These skills help them effectively utilize technology to enhance their everyday life and resilience against cyber threats.



Competencies

Enable seniors to better protect themselves and confidently engage with modern technologies.

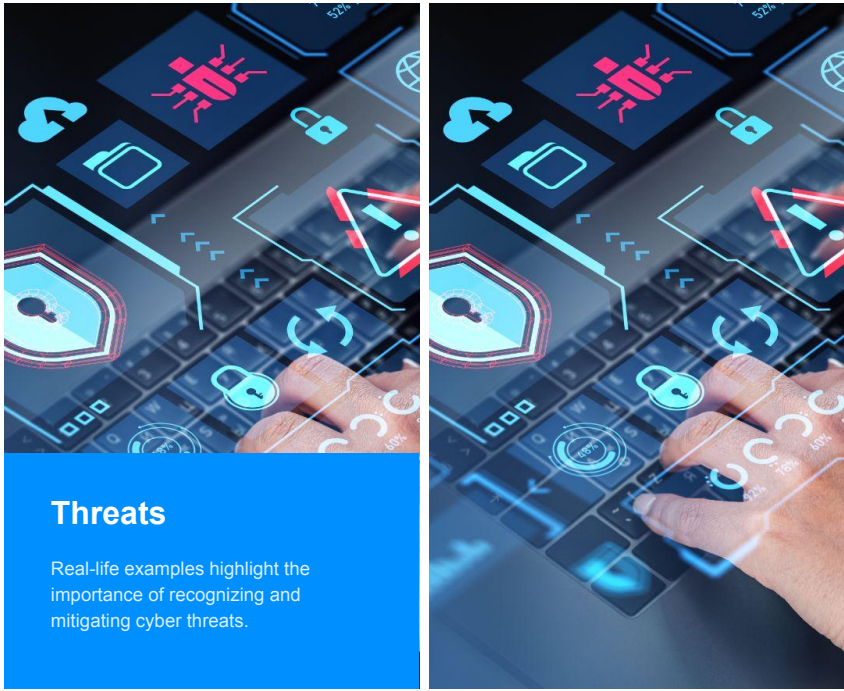


Critical Competencies for Seniors

- Establishing strong, unique passwords and **safety management** (avoid browser storage, use a password manager).
- Enabling **two-factor authentication** for securing accounts.
- Understanding and **configuring antivirus programs**, especially AI-based tools.
- **Recognizing** suspicious, manipulated or **fraudulent online content**.
- **Using AI assistants** practically but remaining critical of results.
- Basic **digital literacy**: updating devices, safe browsing, secure Wi-Fi use.
- **Building confidence** to reduce dependence on others and supporting ongoing digital education.

Real-life Threats Identified by Experts

Experts shared real-life examples illustrating both the risks and benefits of digital technologies for people aged 55 and over. These cases provide valuable insights into common cyber threats of artificial intelligence on seniors' daily lives.

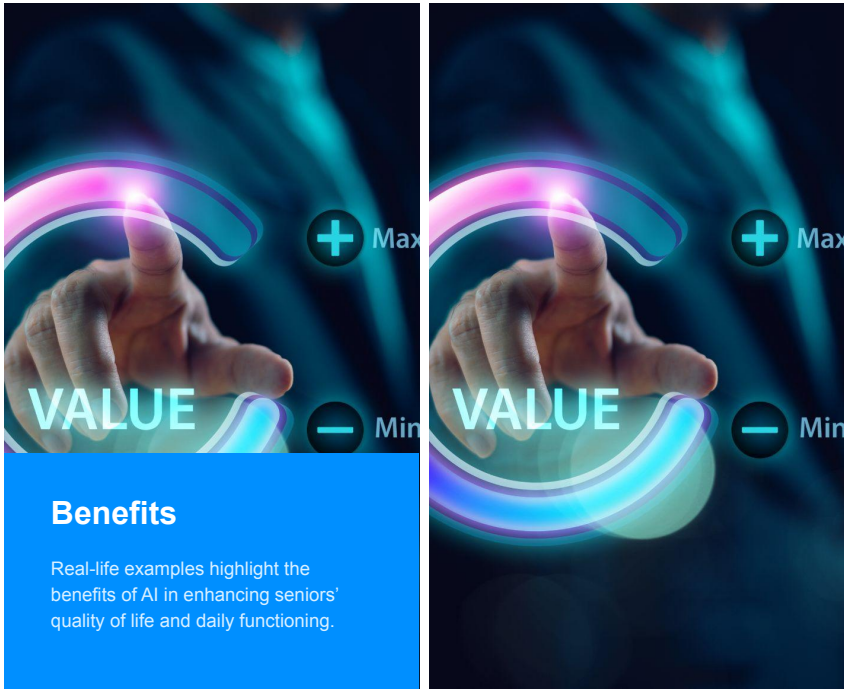


Real-life Threats Identified by Experts

- Example: An elderly woman was scammed when a caller used deepfake technology to clone her grandson’s voice and urgently requested cash, which she delivered to a courier.
- Romance or friendship scams exploiting emotional attachment, often through messages or calls.
- Disinformation spreading through videos or short messages, making it hard for seniors to verify authenticity.
- Poor IT maintenance or use of unsecured networks leading to real breaches.

Real-life Benefits Identified by Experts

Experts shared real-life examples illustrating both the risks and benefits of digital technologies for people aged 55 and over. These cases provide valuable insights into benefits of artificial intelligence on seniors' daily lives.



Real-life Benefits Identified by Experts

- A 72-year-old woman used a voice-based AI assistant for translation, allowing her to join and understand family video calls and feel included in international conversations.
- Seniors use AI for planning (e.g., Windows tips, home DIY), or chatbots in Alzheimer care centers.
- AI offers personalized advice and supports daily independence, but works best when combined with strong foundational skills.

Results - Iceland

Most Cited Online Threats for 55+

People aged 55 and over face unique challenges in the digital world, making them vulnerable to a variety of online threats. Understanding the most common and impactful dangers is essential to improving their cybersecurity awareness and protection.

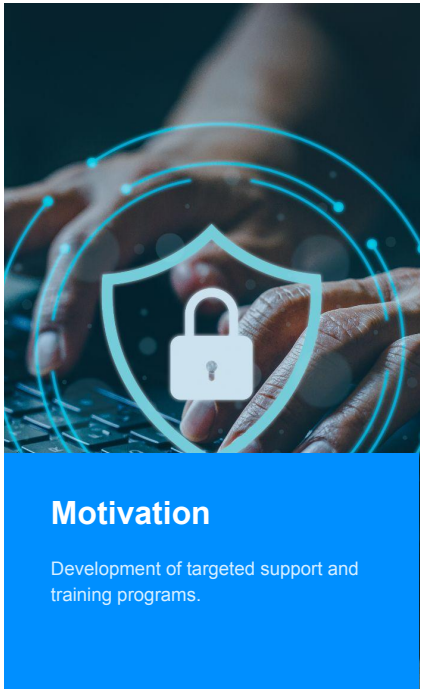
Online threats for 55+

- **Deepfake scams** featuring fake images and videos especially on WhatsApp, where criminals impersonate family members claiming urgent need for money.
- Sophisticated **phishing** evolved into social engineering via messaging apps with convincing fake phone calls and messages.
- **Love scams** on dating platforms targeting lonely seniors globally, including Iceland, leading to financial and emotional harm.
- Physical **impersonation by criminals** posing as tech support or bank representatives visiting seniors' homes.

Top 10 Concerns According to Experts

Experts highlighted key concerns that most affect people aged 55 and over when interacting with digital technologies.

Addressing these concerns is crucial for enhancing their confidence and safety in everyday online activities.



Top 10 Concerns According to Experts

- Difficulty with complex **login processes** including password requirements and frequent resets.
- Confusion and **resistance to two-factor authentication** among older users.
- **Poor email knowledge** hindering password recovery.
- **Small text size** and older phones limiting usability and security features.
- **Lack of clear instructions** from services requiring electronic ID or similar authentication.

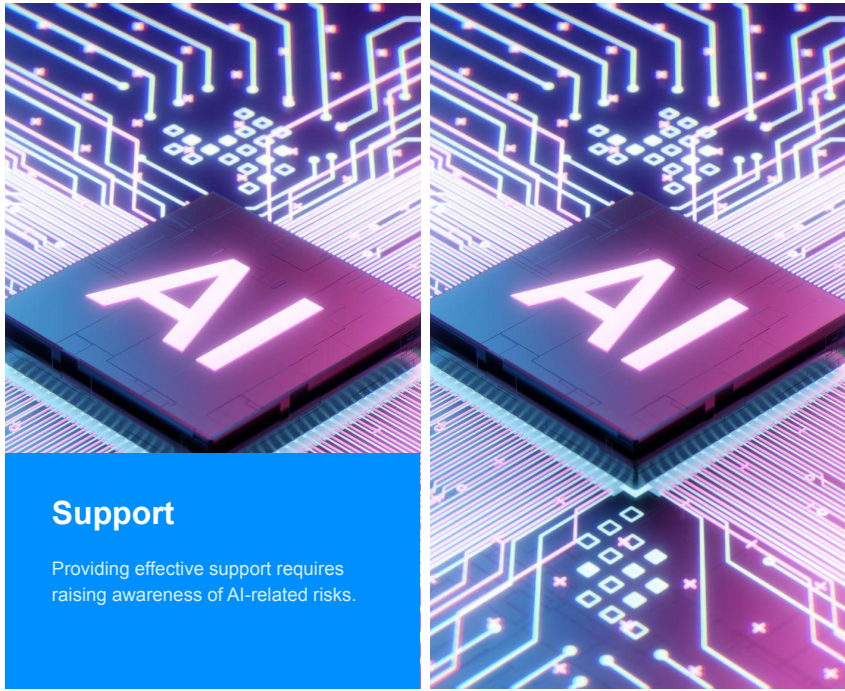
Top 10 Concerns According to Experts

- Seniors **reuse passwords** across critical sites, risking multiple account compromises.
- **Domain impersonation** creating convincing fake websites to steal sensitive data.
- Continuous unnoticed **credential compromises** from dark web monitoring.
- **General distrust** or misunderstanding of cybersecurity threats affecting seniors' responses.
- Barriers created by **technology complexity** reducing confidence and independence.

Key AI Usage Areas and Cyber Risks

Artificial intelligence is increasingly integrated into many aspects of daily life, offering significant benefits but also introducing new cybersecurity risks.

Understanding the main AI application areas and their associated threats is essential for protecting vulnerable groups such as people aged 55 and over.



Support

Providing effective support requires raising awareness of AI-related risks.

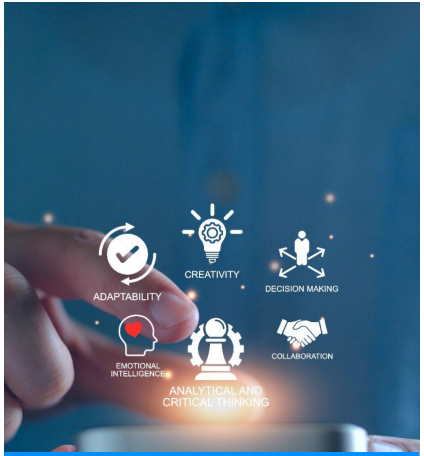
Key AI Usage Areas and Cyber Risks

- **Education** on the risk of AI-generated fake internet content, particularly videos claiming family emergencies.
- **Advising** seniors to verify urgent messages by calling family directly, stressing that real emergencies usually involve phone calls, not texts.
- **Awareness** that AI can imitate any data including videos and images, requiring skepticism and alternative verification.
- Risks from **oversharing personal information** in AI chatbots and tools like ChatGPT, where data is stored.
- Emphasis on **maintaining critical thinking** and verifying information via other communication channels.

Critical Competencies for Seniors

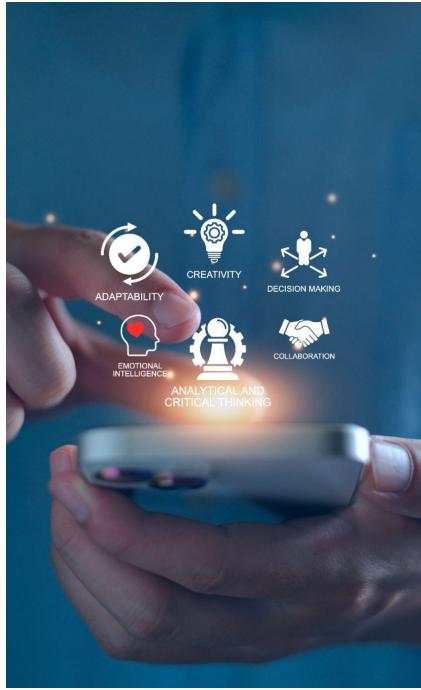
Developing essential digital competencies is vital to empower seniors to navigate the online world safely and confidently.

These skills help them effectively utilize technology to enhance their everyday life and resilience against cyber threats.



Competencies

Enable seniors to better protect themselves and confidently engage with modern technologies.

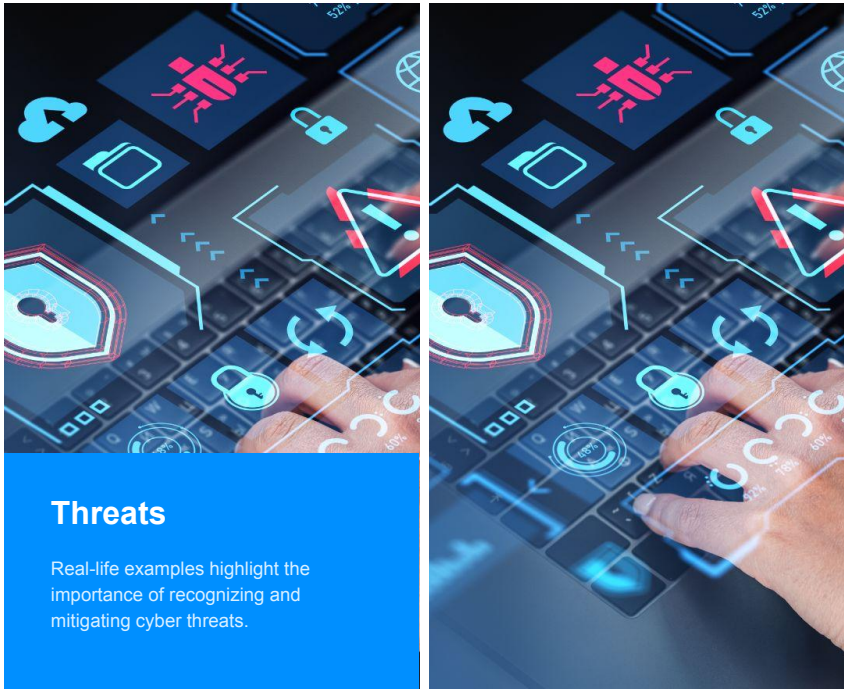


Critical Competencies for Seniors

- Understanding the **importance of verification** before responding to urgent requests through digital media.
- Basic **digital skills** including secure password management and awareness of AI risks.
- **Ability to question** and verify unexpected or emotional messages, especially those appearing urgent or distressing.
- **Skepticism** towards online content authenticity, especially AI-generated media.
- Enhancing trust-building with family members for **direct communication** and help.

Real-life Threats Identified by Experts

Experts shared real-life examples illustrating both the risks and benefits of digital technologies for people aged 55 and over. These cases provide valuable insights into common cyber threats of artificial intelligence on seniors' daily lives.

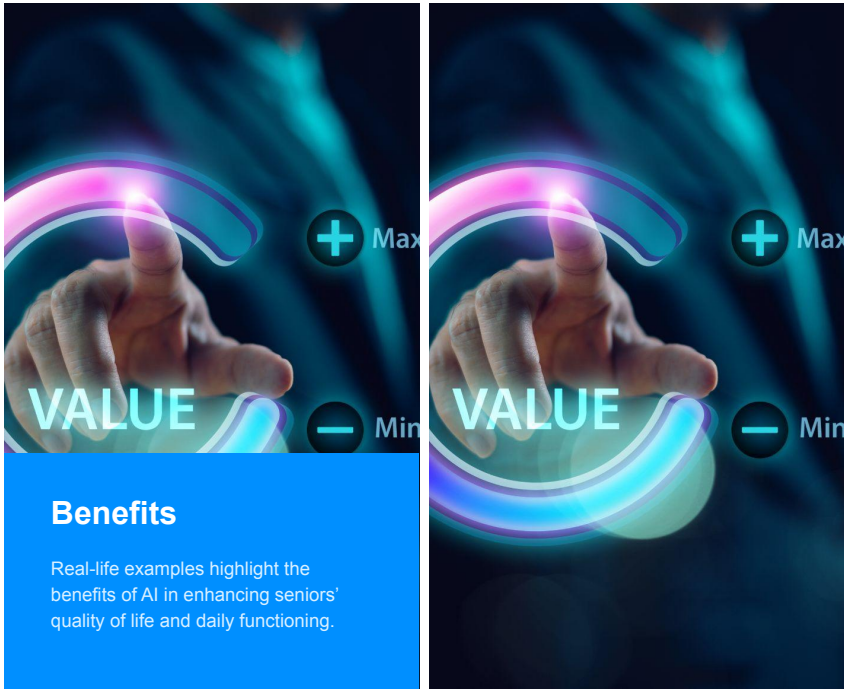


Real-life Threats Identified by Experts

- Examples of victims losing savings to deepfake romance scams using AI-generated celebrity likenesses.
- WhatsApp scams involving fake messages about sick relatives needing money deposits, sometimes stopped by family intervention.
- Social media and dating app love scams leading seniors to pay for fake healthcare or travel abroad for nonexistent partners.
- Job scams stealing credit card information through voice-cloned fraudulent employment offers.
- Cases of vulnerable individuals unintentionally posting compromising content online without understanding consequences.

Real-life Benefits Identified by Experts

Experts shared real-life examples illustrating both the risks and benefits of digital technologies for people aged 55 and over. These cases provide valuable insights into benefits of artificial intelligence on seniors' daily lives.



Real-life Benefits Identified by Experts

- AI assisting seniors with practical daily life advice such as cleaning, home repairs, and quick problem-solving.
- AI chatbots providing emotional support and companionship, offering round-the-clock availability for anxiety relief and general conversation.
- Use of AI tools like ChatGPT for verifying suspicious emails or messages related to cybersecurity.
- Success of AI adoption varies greatly depending on seniors' individual tech skills and trust in technology.

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.