Cybersecurity Made Simple: Key Takeaways for Staying Safe Online

Cybercrime targeting older adults is rising sharply: In 2023, Americans over 60 reported losing $3.4 billion to scams—an 11% increase over 2022, with average losses per victim exceeding $33,000. Scams are increasingly sophisticated, exploiting trust, fear, and new technologies like AI voice cloning. Many incidents go unreported, making education and prevention critical.

Keep Devices Updated

- Enable automatic updates for your operating system and apps.
- Install updates promptly and restart devices to complete installations.

Use Antivirus & Security Software

- Use built-in protections or reputable antivirus programs.
- Ignore unsolicited virus alerts or tech support calls.

Be Scam-Aware

- Watch for red flags like urgent requests, suspicious caller IDs, and payment via gift cards or crypto.
- Never give out personal data or send money in response to unsolicited messages.

Safe Social Media Use

- Set profiles and posts to private or friends-only.
- Avoid sharing sensitive details or announcing vacations publicly.

Password Safety & Two-Factor Authentication (2FA)

- Use long, complex, and unique passwords for every account.
- Enable 2FA wherever possible and never share passwords or verification codes.

Secure Your Home Wi-Fi Network

- Change default router passwords and use WPA2/WPA3 encryption.
- Use a guest network for visitors and monitor connected devices.

Stay Vigilant and Share Knowledge

- Trust your instincts and verify suspicious requests.
- Report scams and share cybersecurity tips with others.

CyberSafe Checklist for Staying Safe Online

- Automatic system updates are ON for all computers, smartphones, and tablets.
- Automatic app updates are enabled in app stores.
- Antivirus software is installed, active, and updated.
- Never give out personal data or send money in response to unsolicited calls, emails, or messages.
- Watch for red flags: urgent requests, threats, suspicious sender details.
- Set social media profiles to private and avoid oversharing.
- Use long, complex, and unique passwords for every account.
- Enable two-factor authentication on important accounts.
- Secure your Wi-Fi network with strong passwords and encryption.
- Monitor connected devices and use guest networks for visitors.
- Trust instincts—pause and verify anything suspicious.
- Report scams to authorities and share knowledge with others.