

Phishing Scams Examples

Understanding Real-Life Scams

Targeting Older Adults

Programs @ The Blue Marble



Phishing scams often arrive through email and text messages

Phishing scams have become a common threat, especially for older adults who may be less familiar with the latest online dangers. These scams trick people into giving away personal information, money, or access to accounts by pretending to be trustworthy sources.

Recognizing how these scams work and seeing real examples can help older adults protect themselves and their loved ones.

What Is Phishing and Why Are Older Adults Targeted?

Phishing is a type of scam where fraudsters send fake messages, often by email or text, that look like they come from banks, government agencies, or well-known companies. The goal is to trick people into clicking links or sharing sensitive information like passwords, Social Security numbers, or credit card details.

Older adults are often targeted because scammers assume they may be less familiar with technology or more trusting of official-looking messages. Many older adults also have

retirement savings or assets that scammers want to access.

Common Phishing Examples That Affect Older Adults

Understanding specific examples helps make the threat clearer. Here are some real-life phishing scams that have targeted older adults:

Fake Social Security or Medicare Alerts

Scammers send emails or calls claiming there is a problem with Social Security or Medicare benefits. They warn of account suspension or fraud and ask the recipient to verify personal information immediately.

Example: An older adult receives an email that looks like it's from the Social Security Administration. The message says their benefits will stop unless they confirm their Social Security number and bank details through a provided link. The link leads to a fake website designed to steal information.

Bogus Bank or Credit Card Notifications

These phishing messages claim there is suspicious activity on a bank or credit card account. The message urges the recipient to log in quickly to "secure" their account.

Example: A senior gets a text message saying their bank account was locked due to unusual transactions. The message includes a link to a site that looks like the bank's login page. When the person enters their username and password, scammers capture the details and use them to steal money.

Prize or Lottery Scams

Scammers tell older adults they have won a prize or lottery but must pay fees or taxes upfront to claim it. These messages often come by email, phone calls, or letters.

Example: An older adult receives a call saying they won a large sum of money in a lottery they never entered. The caller asks for personal details and a payment to cover "processing fees." Once the payment is made, the scammer disappears.

Tech Support Scams

Fraudsters pretend to be tech support agents from well-known companies. They claim the person's computer has a virus or security issue and offer to fix it remotely — for a fee.

Example: An older adult gets a phone call from someone claiming to be from Microsoft. The caller says the computer is infected and asks for remote access. After gaining

control, the scammer installs malware or steals sensitive data.

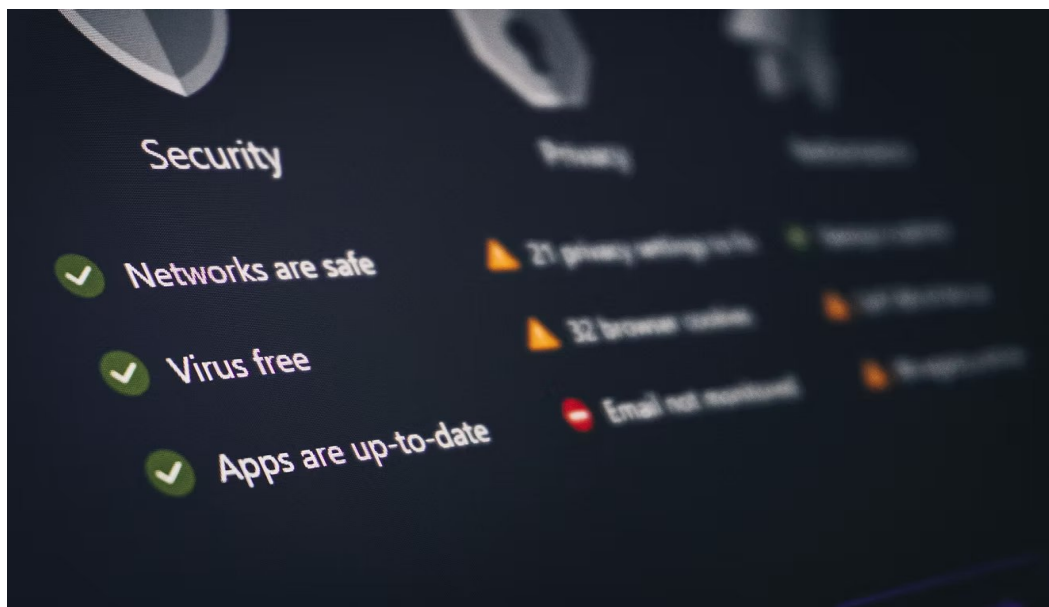
How to Spot Phishing Scams

Older adults can protect themselves by learning to recognize common signs of phishing:

- **Unexpected requests for personal information:** Legitimate organizations rarely ask for sensitive details by email or phone.
- **Urgent or threatening language:** Scammers try to create panic to rush decisions.
- **Suspicious links or attachments:** Hover over links to see the real URL before clicking.
- **Poor spelling and grammar:** Many phishing messages contain errors.
- **Unusual sender addresses:** Check if the email or message comes from a legitimate source.

Practical Steps to Stay Safe

- **Verify directly:** Contact the company or agency using official phone numbers or websites.
- **Use strong passwords:** Avoid using the same password across multiple accounts.
- **Enable two-factor authentication:** Adds an extra layer of security.
- **Keep software updated:** Regular updates fix security vulnerabilities.
- **Be cautious with links and attachments:** Don't open anything suspicious.
- **Ask for help:** Talk to trusted family members or friends if unsure.



Keeping your devices secure and up-to-date protects against phishing attacks

Encouraging Awareness and Support

Phishing scams can cause serious financial and emotional harm. Older adults should feel confident asking questions and seeking help when they encounter suspicious messages. Family members and caregivers can play a key role by sharing information and checking in regularly.

Community centers, libraries, and local organizations often offer workshops or resources on online safety tailored for older adults. Taking advantage of these can build knowledge and reduce the risk of scams.