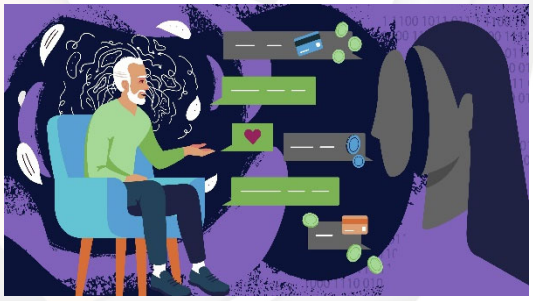
Beware These Online Scams Targeted At Elderly



Each year, as online shopping ramps up in the weeks before the holidays, so do online scams targeting the elderly. This season – in many ways unprecedented – is no different in this regard. In fact, COVID-19, Zoom meetings, vaccination recommendations and travel warnings all provide ample and unique precedent for social engineering attacks.

Not surprisingly, cybercriminals often target those least able to protect themselves. This could be those without antivirus protection, young internet users or, unfortunately, your elderly loved ones. The FBI reported nearly $1 billion in scams targeting the elderly in 2020, with the average victim losing nearly $10,000. This holiday season, it may be worth talking to elderly relatives about the fact that they can be targeted online. Whether they're seasoned, vigilant technology users or still learning the ropes of things like text messaging, chat forums, email and online shopping, it won't hurt to build an understanding of some of the most common elder fraud scams on the internet.

Most Common Types of Online Elder Fraud

According to the FBI, these are some of the most common online scams targeting the elderly. While a handful of common scams against older citizens are conducted in person, the majority are enabled or made more convincing using technology.

- **Romance scams:** Criminals pose as interested romantic partners on social media or dating websites to capitalize on their elderly victims' desire to find companions.
- **Tech support scams:** Criminals pose as technology support representatives and offer to fix non-existent computer issues. The scammers gain remote access to victims' devices and sensitive information.
- **Grandparent scams:** Criminals pose as a relative—usually a child or grandchild—claiming to be in immediate financial need.
- **Government impersonation scams:** Criminals pose as government employees and threaten to arrest or prosecute victims unless they agree to provide funds or other payments.
- **Sweepstakes/charity/lottery scams:** Criminals claim to work for legitimate charitable organizations to gain victims' trust. Or they claim their targets have won a foreign lottery or sweepstake, which they can collect for a "fee."

All the above are examples of "confidence scams," or ruses in which a cybercriminal assumes a fake identity to win the trust of their would-be victims. Since they form the basis of phishing attacks, confidence scams are very familiar to those working in the cybersecurity industry. While romance scams are a mainstay among fraud attempts against the elderly, more timely methods are popular today. AARP lists Zoom phishing emails and COVID-19 vaccination card scams as ones to watch out for now. Phony online shopping websites surge this time of year, and are becoming increasingly believable, according to the group.

Tips for preventing online elder scams

Given that the bulk of elder scams occur online, it's no surprise that several of the FBI's top tips for preventing them involve some measure of cyber awareness.

Here are the FBI's top tips:

- Recognize scam attempts and end all communication with the perpetrator.
- Search online for the contact information (name, email, phone number, addresses) and the proposed offer. Other people have likely posted information online about individuals and businesses trying to run scams.
- Resist the pressure to act quickly. Scammers create a sense of urgency to produce fear and lure victims into immediate action. Call the police immediately if you feel there is a danger to yourself or a loved one.
- Never give or send any personally identifiable information, money, jewelry, gift cards, checks, or wire information to unverified people or businesses.
- Make sure all computer anti-virus and security software and malware protections are up to date. Use reputable anti-virus software and firewalls.
- Disconnect from the internet and shut down your device if you see a pop-up message or locked screen. Pop-ups are regularly used by perpetrators to spread malicious software. Enable pop-up blockers to avoid accidentally clicking on a pop-up.
- Be careful what you download. Never open an email attachment from someone you don't know and be wary of email attachments forwarded to you.
- Take precautions to protect your identity if a criminal gains access to your device or account. Immediately contact your financial institutions to place protections on your accounts. Monitor your accounts and personal information for suspicious activity.

Pressure to act quickly is a hallmark of social engineering scams. It should set off alarm bells and it's important to let older friends or family members know that. Using the internet as a tool to protect yourself, as recommended by the second bullet, is also a smart play. But more than anything, don't overlook the importance of helping senior loved ones install an antivirus solution on their home computers. These can limit the damage of any successful scam in important ways. Don't wait until it's too late. Protect the seniors in your life from online scams this holiday season. You might just save them significant money and hassle.