Protecting Yourself From Technology-Related Scams

By Lewis Lang

As technology has become an essential part of life, it has brought with it numerous benefits and conveniences, along with a variety of risks. This is particularly true for seniors, who can sometimes be more vulnerable to scams. Scams using technology to target older individuals have become increasingly prevalent, making it crucial for them to stay aware and informed. Below are some ways to protect yourself.

Educate Yourself and Stay Informed: The first step in safeguarding against scams is to acquire knowledge. Keep up with the latest trends and techniques that scammers use to deceive unsuspecting individuals. Resources such as government websites, law enforcement agencies, and reputable organizations can provide valuable information and updates on common scams. Stay informed through newsletters, community workshops, or online forums specifically designed to educate seniors about online safety.

Protect Personal Information: Everybody, regardless of age, should be cautious about sharing personal information online. Scammers often attempt to get access to sensitive data, such as social security numbers, banking details, or login credentials, through deceptive tactics.

One example is the fake tech support scam. This scam involves a caller who claims to be from a reputable tech company, such as Microsoft or Apple, and tells the victim that their computer has a virus or a problem that needs to be fixed. The caller then asks the victim to give them remote access to their computer, or to pay a fee for their service. The caller may also ask for the victim's credit card information, passwords, or other sensitive data. The caller is not a real tech support agent but a scammer who wants to steal the victim's money or identity, or install malware on their computer.

Do not give personal information on suspicious websites or respond to unsolicited requests via email or phone calls. When in doubt, verify the legitimacy of the request through known channels or by directly contacting the organization in question. If someone calls or emails you on behalf of a bank, the government, or a company you do business with, do not give them any personal information. Hang up and call or email the organization yourself with the phone number/email you have on file for them.

Online Account Security: Create strong, unique passwords for each of your online accounts and change them regularly. Use a combination of uppercase and lowercase letters, numbers, and special characters to enhance the complexity of the password. Enable two-factor authentication whenever possible, which adds an extra layer of security by requiring a secondary verification step, such as a fingerprint or a unique code sent to a trusted device, such as your mobile phone.

Exercise Caution with Emails and Attachments: Emails are a common medium for scammers to deploy their schemes. Be wary of emails from unknown senders, especially those requesting personal information or money.

One example is the phishing scam. This scam involves an email or a text message that looks like it comes from a legitimate source, such as a bank, a government agency, or a familiar company. The message may ask the victim to click on a link, open an attachment, or provide some personal information. The link or the attachment may lead to a fake website that looks like the real one, or may download malware on the victim's device. The personal information may be used to access the victim's accounts or commit identity theft.

Do not open suspicious attachments or click on links embedded in emails unless they are from trusted sources. Hover the cursor over hyperlinks to verify their destination before clicking. If you have any doubts, delete the email.

Phone Scams: Phone scams targeting seniors are very common, with scammers impersonating government officials, tech support representatives, or family members in distress. With new artificial intelligence (AI) technology, these kinds of phone calls can seem legitimate. However, you should never provide personal information or financial details over the phone unless you have made the call yourself. Hang up and call the organization or a family member directly using a verified phone number. If at all possible, call someone you trust, and explain the call you have received. The strategy of these kinds of scams is to make you nervous and afraid. Hang up the phone if you have any doubt.

Exercise Safe Online Shopping Practices: When shopping online, stick to reputable websites and vendors, such as Amazon, with secure payment options. Look for the padlock symbol in the website's address bar, indicating a secure connection, and install an adblocker on your browser (Edge, Chrome, Safari, etc.) Do not give your credit card information through email or unencrypted websites. Check customer reviews and ratings before making a purchase, and be cautious of deals that appear too good to be true.

Social Media and Online Dating: Be cautious with your online relationships through social media or online dating platforms. One common scam involves a person who creates a fake profile on an online dating site or app and pretends to be interested in a romantic relationship with the victim. The person may use stolen photos and fake details to make themselves seem more attractive and trustworthy. They may also

(continued on next page)