AMERICAN NATIONAL

BANK & TRUST COMPANY

A Guide to Digital Security

Helpful Tips to Protect Yourself and your Finances Online

At **American National Bank & Trust Company**, we believe being local is more than just having an office in the community. It's about looking out for our customers with better banking options and responsive, helpful service. That's why we've compiled some information you need to protect yourself and your finances from online fraud.

AMERICAN NATIONAL

BANK & TRUST COMPANY

Table of Contents

Chapter 1 | Strategies to Prevent Online Fraud

Like sand through the hourglass, the world keeps on turning and scammers keep trying to trick consumers and businesses with online fraud. Whether the purpose is to steal your money, personal information, or gain access to your employer's data, becoming a victim of online fraud can have serious consequences. It's also a huge pain to sort out and recover from. So, follow these five strategies for spotting and avoiding Internet fraud.

When you receive an email, download files, or click a link, consider the following:

- Is the email genuine, such as **source address, spelling** and **context**?
- Is the file from a **trustworthy source**?
- Is the link legitimate, such as the **destination of the URL**?

What are the most common online scams?

Knowing what to look for is a good first step in preventing fraud. Here are the most common types of scams right now:

Malware

A malicious software that damages or disables your computer. Scammers may steal sensitive data from your computer or ask you for a ransom payment to have your computer restored.

Stay Safe: Avoid opening or downloading attachments you weren't expecting to receive. Before clicking on an unsolicited link, hover your mouse over it to view the complete URL. If it looks scammy, don't click or you could end up unintentionally downloading malware.

Ransomware

This is a form of malware usually delivered through phishing emails. If you end up with ransomware on your computer, you will be unable to access your data until/unless you pay the ransom to regain access to your data.

Phishing

Phishing is forged or faked electronic communications such as email, social media message, or text message. Scammers pose as legitimate businesses, such as your cellphone provider or bank to try and trick you into giving them sensitive information such as your account login credentials, credit or debit card numbers, or bank account number.

Stay Safe: Again, beware of clicking on links—always "think before you click" by viewing the full URL first. And remember that legitimate institutions will never ask for your login credentials, full account number or social security number, etc.

Charity Fraud

Fake charities often pop up in the wake of natural disasters, war, and other major events, though they can pose as legitimate charities. Charity fraud is a double tragedy because you are cheated out of your money, as are the people you intended to help.

Stay Safe: Do your research to find a legitimate organization to donate to. Don't just respond to random solicitations on social media or via email.

Be skeptical of emails, calls, and texts

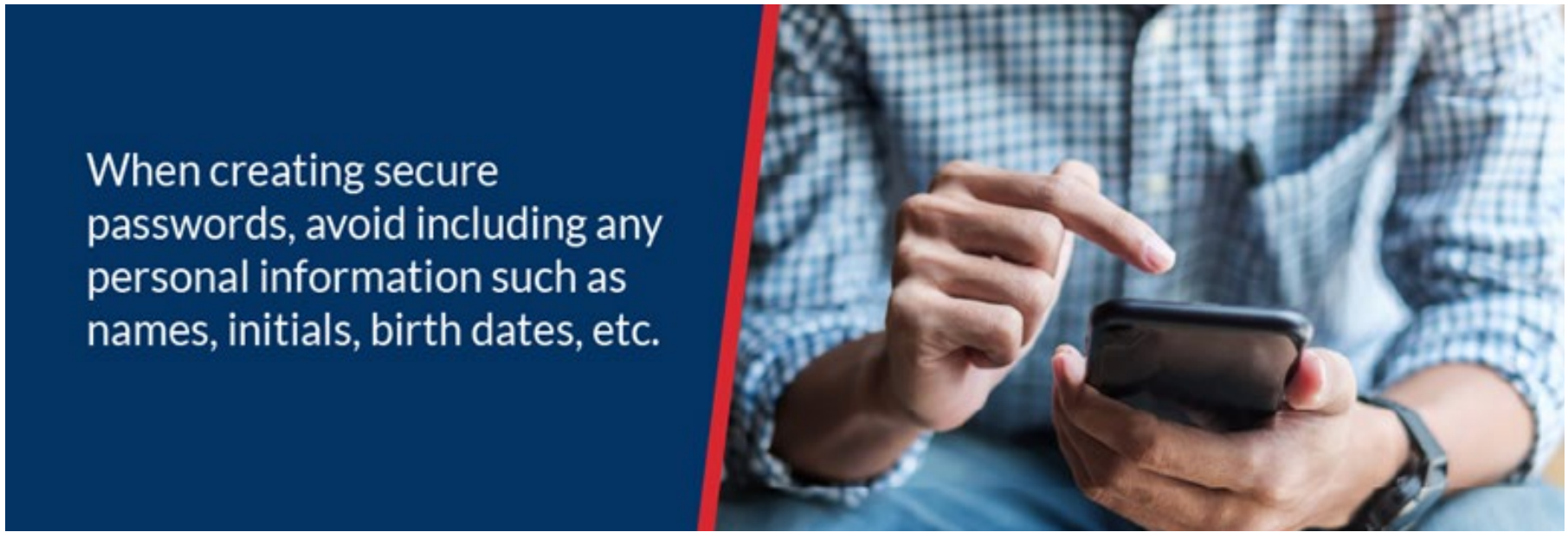
One of the primary ways scammers try to trick you is via phishing messages. So, the best way you can protect yourself is by maintaining a default skepticism toward any messages from strangers or purportedly from legitimate companies that you weren't expecting.
Don't be afraid to push back on requests—ask to speak to a supervisor, for example, if you are contacted by phone. If you receive an email or text message saying there's a problem with your account, contact the company directly by their publicly available customer service number to verify whether this is true. Scammers will use any cover story to convince you to give up your personal information, which can include promises of benefits or threats or punishment.

Stay Safe: Never give out your personal information to anyone over the phone, through email, or text unless you can absolutely verify that they represent an official organization. If you feel that you have been targeted with a scam, you can send a tip to the FBI via their website.

Practice positive password habits

It can be tempting to use the same password for multiple online accounts for the sake of convenience, but this makes it easier for hackers to access all your accounts if they steal your login credentials for one account.

Stay Safe: Consider using a password manager, like these recommended by C Net, to create and store unique passwords for each of your accounts for you.



If you do create your own passwords, try to use strong passphrases, combinations of numbers and letters, symbols, and avoid using personal data, like birth dates, social security numbers, etc. in your passwords. Also avoid common sequences such as “abc” and “123.”

Never give anyone remote access to your computer

Some scammers will pose as a legitimate IT business and offer to remotely access your computer to resolve an issue for you. This is almost always fraudulent, and could come in the form of them offering to update your computer, initiate a refund or payment from an online account, install a vital piece of software, or even access your online banking info to initiate a transfer. This is becoming a common strategy for modern scammers, who will use their remote access to your computer as an opportunity to lock you out and steal your vital information. This can later be used against you to access your accounts, blackmail you, or can be sold on the dark web to the highest bidder.

Keep your financial data separate

Fraudsters are after your data along with your money. So, storing financial data on your computer makes it vulnerable to theft. It’s best to use just one device to store financial documents and information on, such as an external hard drive that’s not even connected to the Internet. Store it in a secure place in your home, such as a locked filing cabinet or safe.

Dispose of your data properly

Finally, our last tip is for physically protecting your data by disposing of it properly. Physical documents containing sensitive personal and financial information should be shredded. You can buy a home shredder, pay for shredding at an office supply or shipping store, or take advantage of free community shredding events.

Stay Safe: Whatever you do, don’t just put intact documents out in the trash or recycling, as they could be stolen and your identity compromised.

Before getting rid of a computer, phone, or tablet device that contains important information, be sure to thoroughly wipe the hard drive before you get rid of it. Simply deleting your files isn’t always enough with today’s newer drives. You may even want to completely destroy the hard drive instead of simply wiping it if you are planning to dispose of the computer. Hard drive eraser utilities are also available for a stronger and more secure way to wipe your drive.

Chapter 2 | Beware of Phishing Scams – Know How to Spot the Signs

If you sometimes feel like you're experiencing "information overload," you're not alone. Thanks to the Internet and 24-hour news cycle, there is always a "breaking news" article to read and share with others. Unfortunately, scammers take advantage of our fractured attention to try and slip a phishing message past us undetected. Whether through email, text message, social media message, or phone call, learn to spot the signs of phishing so you can protect yourself from scams.

What is phishing?

Phishing, a play on the word "fishing," is a type of cybercrime in which scammers dangle "bait" to try and lure sensitive personal information from you such as account numbers, social security number, login credentials, and more.

While email phishing is the most common form, phishing scams can also arrive via text ("smshing"), video ("vishing"), and phone call. In fact, fake text phishing scams are becoming more prevalent.

In any type of phishing scam, the sender masquerades as a trusted or well-known company to trick you into thinking the message is actually from your bank or that retailer you frequently shop with.

Stay Safe: Stop and think before you click to verify whether the message is legitimate or fraudulent.

How to spot a phishing scam

Here's what to look for when determining whether a message is real or fraudulent:

- Is the offer too good to be true?
- Is there a sense of urgency and pressure?
- What is the link's actual URL? Hover your mouse over the link to find out.
- Were you expecting this attachment or not?
- Is the grammar or spelling a little bit off, suggesting a non-native English speaker or email address such as "info@targett.com"? The two 't's' might not jump out at you if you just skim, which is why it's important to look carefully before taking action.

Stay Safe: When in doubt, contact the company directly via the customer service number listed on their website. They can tell you if there's actually a problem with your account or a special offer. Remember that legitimate companies and banks will never ask for your full account number, social security number, or login credentials over the phone.

Chapter 3 | How to Prevent Phone Hacking

For many of us, our cell phones are within reach at almost every waking minute of the day. Our lives are centered around these small devices, whether we're checking in on work emails, ordering groceries, or moving money around in our online banking app. But with so much of our personal information now being held on our devices, also presents a significant security risk. Hackers know that your phone is a goldmine of data, so what can you do to stay protected? Let's take a look.

Implement two-factor authentication for critical apps

Having a strong password is no longer enough to keep your data safe. Wherever possible, you should set up two-factor authentication on your apps. This extra step may feel unnecessary in many cases, but it's an extra layer of protection against hackers if they manage to get past the initial login screen.

Two-factor authentication is particularly important for anything that holds your financial information, like banking or investment apps. This data is one of the biggest targets for hackers and scammers, so you need to do everything you can to keep this information private and safe.

Avoid unsecured wi-fi networks

An unsecured wi-fi network is one that doesn't need a username or password for connection. They're the ones that you're most likely to use when you're outside your home, like at a coffee shop, airport, or local library.
These networks can be convenient to use when you're in public spaces, particularly if you don't have the best phone signal. But they're also one of the easiest ways for hackers to gain access to your device.

Stay Safe: Always be aware of what network your phone is connected to and try to avoid online shopping or using your banking apps when on these networks. If you need to access these, try using a VPN instead to mask your network connection to any potential scammers.

Beware of email and text phishing

Links in both emails and text messages are two of the most common ways that hackers gain access to smartphones. If you receive a text message or email that looks suspicious or comes from an unrecognized source, never click on the links inside until you can verify that they're legitimate.

You may be familiar with this best practice on your computer and know that these links can install malware or spyware on your device. But these days, the same can happen on phones too. You could easily find yourself installing spam software on your device or going to a convincing website that encourages you to hand over your personal information.

Use strong passwords

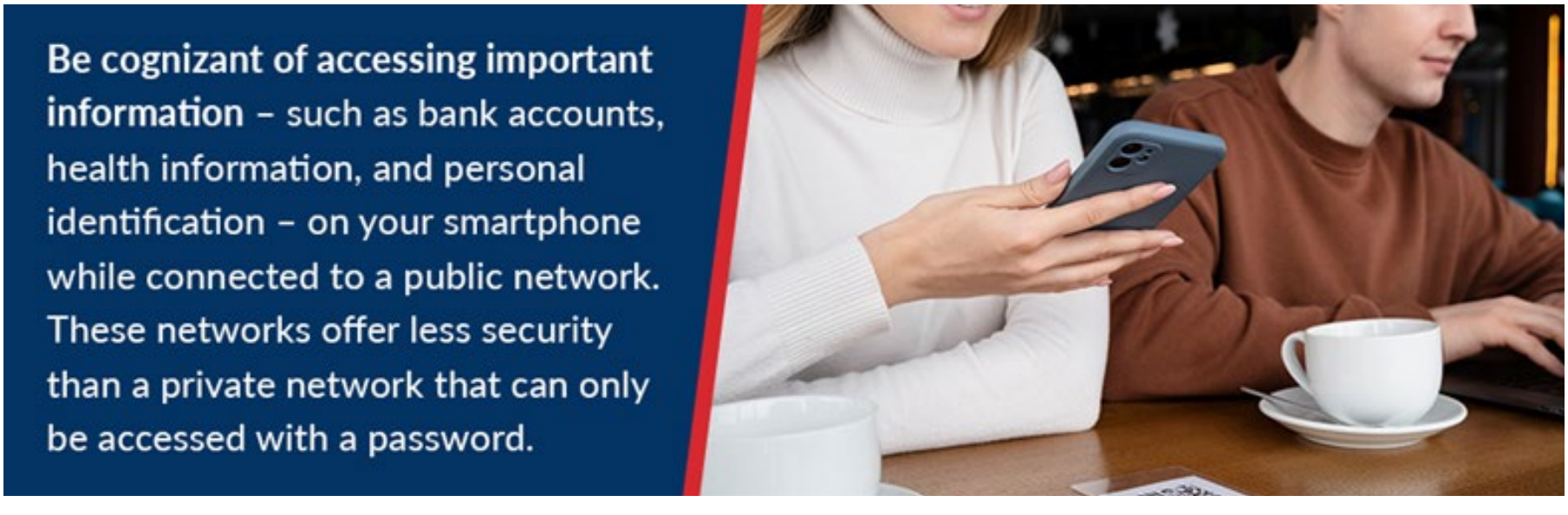
Having strong passwords is one of the best ways to prevent hackers from accessing your phone, and that goes for your lock screen too!

Avoid using obvious numbers like 1111 or 1234, or something that you use in a secure setting like your card pin number. If your device allows you to do so, set up biometric authentication like a fingerprint unlock or facial recognition.

Avoid common security mistakes

Some businesses or websites that you frequently use may have an app that you can download onto your phone to access their products and services. Although most have these listed and linked on their websites, it's best to avoid these direct downloads and, instead, find the app within the official app store for your device.

Links online can be easily edited and manipulated by hackers to give them backdoor access to your device through fraudulent apps. Once the app is installed, scammers can then read and copy your personal data and passwords. However, apps within the app store are verified and have been through security measures in order to be listed, so downloading from there is recommended.



Chapter 4 | Lessons to Teach Your Kids About Cybersecurity

According to the Department of Homeland Security, kids between the ages of 8 and 18 spend an average of 7 hours and 38 minutes each day online. But the sheer amount of time spent online is only one of the many issues revolving around digital exposure. Most parents are painfully aware of how nefarious navigating the internet can be: from cyberbullying to inappropriate content, to damaged self-esteem. And children are also especially vulnerable to burgeoning cyber security issues, where hackers and scammers can gather sensitive information putting both you and your child at risk for identity theft, wire fraud, and other crimes.

As your children become more independent with their online presence, it's important to provide them with a strong foundation to understand the importance of safeguarding themselves and their information. Here are three important lessons every parent should impart to their child to help ensure their online safety.

Don't Overshare

We already know to teach our children to be careful about what they post—you never know where an image or comment will end up or who will see it. Oversharing on the internet is one of the biggest mistakes that people of all ages—but especially young adults—can make.

It's equally important for your children ***not to share personal information***, even if they don't think it will be public. Certain information can be not only used to locate the child or login to accounts, but can also help hackers verify the accounts they are trying to break into. This information includes:

- First and last names
- Address and phone numbers
- Birthdays
- Passwords and passcodes
- Social Security numbers
- Names of schools, places of employment (parent or child), and any other locations that anyone in the family frequents (church, rec center, hangout location, etc).

Lastly, remind your child not to share their phone itself, except in the case of an emergency. Another person—even a trusted friend—could inadvertently allow a third party to access sensitive information.

Be Skeptical of Outside Calls, Emails, and Texts

Your child may know not to share passwords or sensitive information with others, but they may not be aware of the lengths hackers and phishers will go to obtain that data, disguising themselves as legitimate businesses and institutions. Teach your children this important rule of thumb: Trusted institutions will never contact you first and then ask for your personal information.

Here are some ways to stay safe and avoid scams:

- Don't send cash, or use gift cards or cryptocurrency to pay someone without first verifying the request or entity is legitimate. Contact the person or business at a publicly known number to be sure who you are speaking with.
- Don't give your financial or other personal information to someone who calls, texts, or emails even if they say they are from a bank, trusted business or government.
- Don't trust your caller ID. Fraudsters can spoof phone numbers to make it look like they are calling from a place you recognize.
- Don't click on links in unexpected emails or text messages.

This last tip is an important one to keep in mind—actively giving away information isn't the only way hackers and phishers can get it. Simply clicking on a link can infect your device with malware, which can track your keystrokes and obtain sensitive information. The amount of spam sent each day is astronomical; according to Forbes.com, "some 320 billion spam emails are sent every day, and 94% of malware is delivered via this medium." Using ***reputable email providers*** like Gmail with built in spam-controls can stop a significant number of these emails, but it's also necessary to ***be aware of common phishing techniques***, like the ones listed on this FTC guide, for email, text, and private messages.

Use Strong Passwords

Even if your child doesn't give away their information or click on a phishing link, if their password is weak, it could still leave them vulnerable. ***Passwords containing personal information are especially in danger of being hacked***, so avoid items like birthdays, names or initials, or other details that can be easily guessed by others. However, it's not just individual hackers out there, guessing one password at a time. For instance, a significant portion of the 134 million customers whose personal information was leaked in the 2017 Equifax hack came from an artificial intelligence program scanning LinkedIn profiles. Any basic combinations of words and letters that contain personal information can be guessed by these programs.

Creating ***longer or more complex passwords***—with upper and lowercase letters, numbers and symbols—can help. ***Choosing to use a passphrase*** (a sentence or phrase instead of one word) adds complexity while making it easier to remember. Savvy Cyber Kids also recommends using an authenticator app like those created by Google or Microsoft. These apps use a two-step or two-factor verification system to insure the person logging in is using an authorized device. And using a ***password manager***, like these recommended by C Net, that can generate and store complex passwords, adds an additional layer of protection. For more information on how to create strong passwords, check out this handy primer from Harvard Information Security.

Lastly, don't forget the security of the device itself. If the screen is easy to unlock or uses no locking function at all, anyone who finds or steals your child's phone can easily access their personal information. Encourage your child to ***use fingerprint verification or face ID***, with a complex passcode as backup. Remember, you can set more than one fingerprint to unlock a phone—your child's and your own!

Ultimately, your child's safety is your responsibility and for your children to have the most secure cyber experience, it's crucial for you to remain active in and aware of their digital usage and presence. But imparting these simple lessons to your children, early and often, will ensure that they can keep themselves and their assets safe for years to come.

Chapter 5 | Digital Fraud Scams Targeting Seniors

The American Journal of Public Health published studies in 2017 revealing that approximately 5 percent of the elderly population in the US had reported falling victim to a financial scam. Given that scamming increased during COVID and many seniors never file a report when they are scammed, the reality is that a large number of seniors lose money to strangers each year. Whether you are an older adult, a senior caregiver, or have aging family members, the team at AMNB wants to help keep our community safe from financial harm. Sharing your knowledge with those you care for and checking in often can help protect your loved ones of all ages. Here are five of the most common scams targeting seniors in Virginia and North Carolina.

Phishing Scams

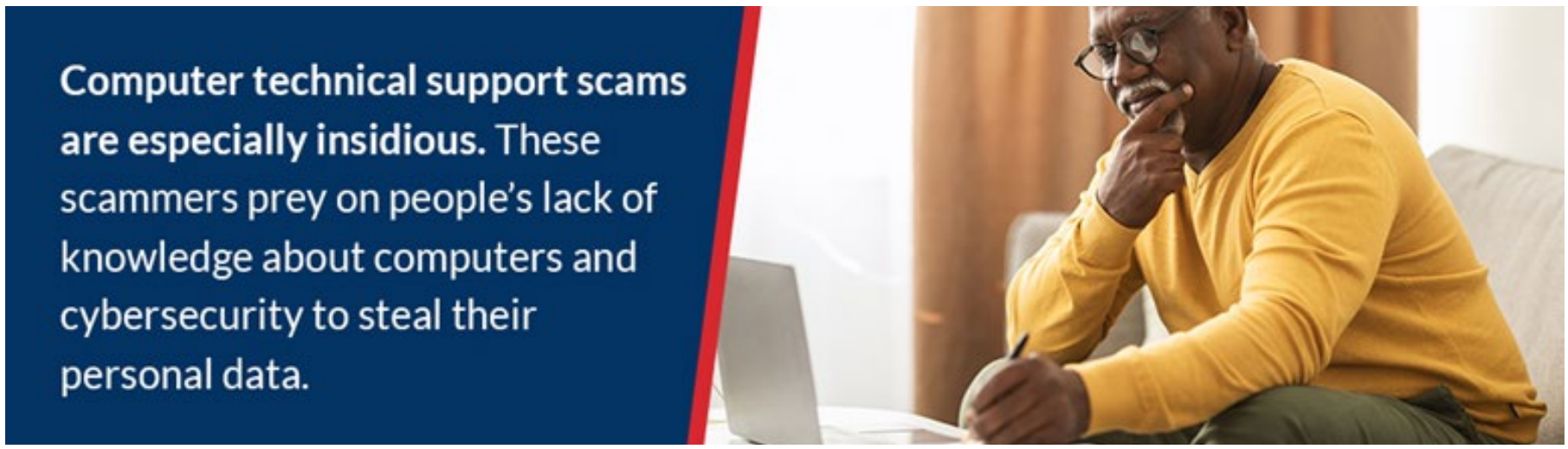
Phishing scams come in all shapes and sizes but have one thing in common, they lure unsuspecting victims into sharing their personal information. Fraudsters have become experts at creating official looking emails from recognizable banks, utility companies, and Medicare. Seniors often click through the links sent in the email to "verify their account information" or "update their payment method" and enter personal details that allow scammers full access to their financial accounts.

Romance Scams

Romance scams have increased over the last few years with the rise of social media and dating apps. According to the National Academies of Sciences, Engineering, and Medicine over one third of adults over the age of 45 reports feeling lonely. Fake dating profiles attract victims of all ages and skillfully engages them in meaningful conversation to create trusting relationships. Once a relationship is established online, the fraudsters convince their victims to provide financial assistance. Some scams include using the victim as an unwitting money mule to launder funds from illegal activities while others simply offer to plan a wedding and disappear with the money.

Computer Repair Scams

In this type of scam, fraudsters contact seniors to patch a security breach or update software on the senior's computer or phone. The scammer convinces the victim to allow them access to their device via a remote connection that looks like a Zoom call. Thinking they will be at risk if they don't fix the computer problem, victims grant access to their devices and unknowingly allow the scammer full access to their files and keystrokes.



Fake Grandchildren Scams

When a senior answers the phone and hears "Hi Grandma!" their first instinct is not to question the caller's identity. From phone calls to email, scammers are posing as grandchildren to convince seniors that they need financial assistance. By appearing in distress, fraudsters are convincing seniors to send money quickly to help them out of an emergency situation.

COVID Scams

COVID related scams peaked when vaccination appointments first became available. Scammers would contact members of the elderly population offering vaccination appointments for a fee. Victims would give their personal information online or over the phone, desperate to get a vaccination appointment and unaware that it was a scam. COVID scams continue to be a problem for seniors with emails promising at home COVID tests and vaccination booster appointments in Virginia.

Avoiding Scams

When it comes to avoiding financial scams, teach family members not to click on links sent in emails. If they are convinced it is a reputable request for information, suggest that they call the bank or institution directly and speak to someone about the email. Keep in touch with the seniors in your life and help them navigate the challenges of modern technology and social media. Loneliness, lack of technological knowledge, and declining mental health puts the elderly community at risk for financial harm.