Cyber-Savvy Seniors

Content brought to you by:
Senior Housing Crime Prevention Foundation

The Top Scams Targeting Seniors:

How to Stay Safe in the Digital Age

Senior citizens, with their wealth of experience and often trusting nature, have unfortunately become prime targets for various scams in recent years. As technology advances, so do the methods employed by scammers, making it crucial for seniors to stay informed and vigilant. Here, we explore some of the top scams affecting senior citizens today, and provide tips on how to protect oneself from falling victim.

Social Security Scams
One of the most prevalent scams targeting seniors involves fraudsters impersonating officials from the Social Security Administration (SSA). These scammers often contact seniors via phone or email, claiming there is an issue with their Social Security benefits or that their Social Security number has been compromised. They may request personal information or even demand immediate payment to resolve the fictitious problem.

To avoid falling victim to Social Security scams, it's important for seniors to remember that government agencies will never demand immediate payment over the phone or threaten legal action. If contacted by someone claiming to be from the SSA, seniors should hang up and independently verify the legitimacy of the call by contacting the SSA directly.

Medicare Fraud
Scammers frequently target seniors through fraudulent schemes involving Medicare. These scams can take various forms, such as offering free medical equipment or services in exchange for Medicare information, billing Medicare for services that were never provided, or selling fake prescription drugs.

Seniors should be wary of unsolicited offers related to Medicare and never provide their Medicare number to anyone other than trusted healthcare providers. They should review their Medicare statements regularly for any unfamiliar charges and report suspicious activity to Medicare immediately.

Tech Support Scams

With the increasing reliance on technology, seniors are also vulnerable to tech support scams. In these schemes, scammers pose as technical support representatives from reputable companies, claiming that the senior's computer has been infected with a virus or malware. They then offer to fix the issue remotely for a fee or by gaining access to the senior's computer and stealing personal information.

To protect against tech support scams, seniors should be cautious of unsolicited calls or pop-up messages claiming to be from tech support. They should never give control of their computer to someone they don't know and trust, and always

The Top Scams Targeting Seniors

continued from page 1

rely on reputable sources for technical assistance.

Romance Scams
Seniors looking for companionship online are also at risk of falling victim to romance scams. Fraudsters create fake profiles on dating websites or social media platforms, establishing a relationship with the senior before requesting money for various reasons, such as medical emergencies or travel expenses.

To avoid romance scams, seniors should be cautious when interacting with individuals online, especially if they quickly profess love or ask for financial assistance. They should never send money to someone they haven't met in person, and they should consider conducting background checks on individuals they meet online.

Grandparent Scams
Grandparent scams prey on the emotions of seniors by exploiting their love for their grandchildren. Scammers often pose as grandchildren in distress, claiming to be involved in an accident or legal trouble and in need of urgent financial assistance. They may ask the grandparent to wire money or provide credit card information without verifying their identity.

To protect against grandparent scams, seniors should verify the caller's identity by asking personal questions that only their grandchild would know. They should also contact other family members to confirm the situation before taking any action.

Remember
Seniors must remain vigilant against the various scams targeting them in today's digital age. By staying informed about common scams and following basic safety precautions, seniors can protect themselves from falling victim to fraudsters seeking to exploit their trust and generosity. Additionally, family members and caregivers play a crucial role in educating seniors about potential scams and providing support to help them navigate the complex landscape of online threats. With awareness and proactive measures, seniors can reduce their risk of becoming victims and enjoy a safer online experience.

Cyber-Savvy Seniors

Content brought to you by:
Senior Housing Crime Prevention Foundation

Preventing Check Fraud

A Comprehensive Guide

As technology continues to advance, so do the tactics used by fraudsters to exploit unsuspecting victims. Senior citizens, often seen as more vulnerable due to their limited exposure to modern technology, are particularly at risk of falling prey to check fraud.

Check fraud is a type of financial scam that involves criminals using counterfeit or stolen checks to access funds from an individual's bank account. Here is how you can protect yourself from check fraud scams that are currently having a resurgence.

Education
Understanding the various forms of check fraud and how they can occur is the first line of defense. Be aware of common scams, such as lottery or sweepstakes fraud, where you may be asked to deposit a check and then send a portion of it back to the scammer. Be cautious about unsolicited check offers in the mail or online, as these may lead to financial losses. It is essential to consult with trusted financial advisors, family members, or friends who can provide guidance and help recognize potential scams. Workshops and seminars on financial security can also be beneficial in equipping seniors with the knowledge needed to protect themselves.

Vigilance in Check Handling
Exercise vigilance when handling checks, whether receiving payments or writing checks yourself. Here are some practical tips:

- Examine incoming checks: Carefully inspect checks received in the mail or from unfamiliar sources. Look for any signs of tampering, irregularities, or discrepancies.
- Verify the source: If someone requests payment through a check, especially if it's a stranger or an online transaction, take the time to verify their identity and the legitimacy of the transaction. Don't hesitate to contact the person or company to confirm the request.
- Use secure mailboxes: Install a secure mailbox to prevent theft of incoming checks or outgoing payments. This reduces the chances of checks falling into the wrong hands.
- Use a gel pen instead of a ball point pen when writing checks to prevent check washing by scammers who may come across one of your checks.
- Shred old documents: Dispose of old bank statements, canceled checks, and financial documents by shredding them rather than throwing them away intact. This prevents identity thieves from obtaining sensitive information.

Preventing Check Fraud

continued from page 1

- Monitor bank statements: Regularly review bank and credit card statements for unauthorized or suspicious transactions. Report any discrepancies to the bank immediately.

Implementing Security Measures

To protect yourself further, consider implementing security measures that can safeguard checks and financial information, such as:

- Opt for direct deposit: Whenever possible, use direct deposit for Social Security payments, pensions, or other income sources. This reduces the risk of physical checks being intercepted or lost in the mail.
- Use fraud protection services: Many banks offer fraud protection services that can help detect and prevent unauthorized transactions on your accounts. Enrolling in these programs can provide an added layer of security.
- Secure personal information: Keep personal and financial information, such as checkbooks, account numbers, and Social Security cards, in a secure location at home. Do not share this information with anyone unless absolutely necessary.
- Protect your Passwords: If conducting online banking or financial transactions, use strong, unique passwords for each account, and enable two-factor authentication whenever possible.

Protecting senior citizens from check fraud is a collective effort involving education, vigilance, and security measures. People must empower themselves with knowledge about common scams and stay alert to potential threats. By following best practices in check handling and implementing security measures, they can significantly reduce their vulnerability to check fraud. Additionally, seniors should maintain open communication with trusted individuals who can provide guidance and support in navigating the complex landscape of financial security. In doing so, senior citizens can enjoy greater peace of mind and safeguard their hard-earned assets from the ever-evolving tactics of fraudsters.

Cyber-Savvy Seniors

Content brought to you by:
Senior Housing Crime Prevention Foundation

Romance Scams:

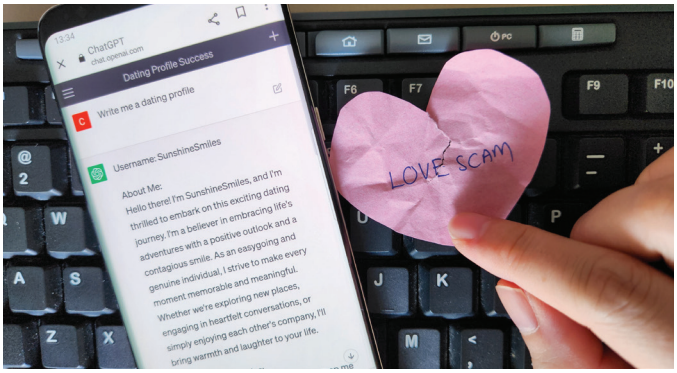
Strategies to avoid online con-artists trying to steal your heart and wallet

In an era where technology intertwines with daily life, online romance scams have become a prevalent threat, particularly targeting vulnerable populations like senior citizens. These scams exploit trust and affection, leading to emotional and financial devastation. However, with awareness and practical precautions, seniors can safeguard themselves against such deceitful schemes. Here, we will explore effective strategies for senior citizens to protect themselves from online romance scams.

Firstly, education is paramount. Senior citizens must understand the tactics used by scammers to manipulate emotions and gain trust. Learn to recognize these common red flags and suspicious behavior in online interactions:

Love bombing is a manipulative tactic used by individuals, often in romantic relationships, to overwhelm someone with affection, attention, and flattery. The term originates from the concept of "bombarding" someone with expressions of love and admiration to gain their trust and loyalty. Love bombing typically involves excessive compliments, declarations of love, and grand gestures designed to create a sense of euphoria and dependency in the recipient. However, behind the facade of affection lies a strategic intent to manipulate and control the individual's emotions and behaviors. Love bombing can be a precursor to more harmful forms of manipulation and exploitation, such as emotional abuse or financial coercion.

Sob stories refer to narratives or accounts of personal hardship, misfortune, or suffering that are often told with the intention of evoking sympathy, empathy, or pity from others. These stories typically emphasize emotional distress or difficult circumstances faced by the storyteller, such as financial struggles, health issues, family problems, or past trauma. The term "sob" conveys the idea of crying or expressing deep sorrow, indicating that the stories are often emotionally charged and designed to elicit an emotional response from the listener or reader. In some



contexts, sob stories may be genuine expressions of hardship, but they can also be used manipulatively to manipulate others' emotions or solicit assistance, favors, or financial support.

Online requests for money scams are a type of cybercrime where individuals attempt to fraudulently obtain money from victims through various deceptive tactics on the internet. These scams can take many forms, but they often involve manipulating victims into sending money under false pretenses, often assuring the victim that they will soon be repaid after "temporary" circumstances are resolved.

Secondly, seniors should prioritize skepticism and caution when communicating with strangers on the internet. Verifying the identity of individuals

→

Romance Scams

continued from page 1

through multiple channels, such as video calls or social media profiles, can help confirm their legitimacy. It is essential to remember that not everyone online is who they claim to be, and maintaining a healthy level of skepticism can prevent falling prey to deceitful intentions.

Seniors should protect their personal information vigilantly. Scammers often use information shared online to build rapport and credibility. Hence, refraining from disclosing sensitive details such as financial information, home address, or social security number is crucial. Additionally, seniors should be cautious about sharing intimate photos or engaging in intimate conversations with individuals they have not met in person, as these can be used for extortion or further exploitation.

Not just seniors, but everyone, should leverage privacy settings and security features on social media platforms and dating websites. Adjusting privacy settings to limit the visibility of personal information can reduce the risk of being targeted by scammers. Similarly, enabling two-factor authentication and regularly updating passwords can enhance the security of online accounts, minimizing the likelihood of unauthorized access and potential exploitation.

Additionally, seniors should consult trusted family members or friends before making significant decisions or financial transactions with individuals they have met online. Seeking a second opinion can provide an external perspective and help identify any potential warning signs that may have been overlooked. Family members can also offer support and guidance in navigating online relationships safely. Consider seeking professional advice from financial advisors or legal experts when faced with requests for money or investments from individuals met online. These professionals can provide objective guidance and help assess the legitimacy of financial opportunities, preventing seniors from falling victim to fraudulent schemes.

It is important that seniors remain vigilant for warning signs of online romance scams, such as inconsistencies in stories, reluctance to meet in person, or sudden emergencies requiring financial assistance. Trusting instincts and being willing to walk away from suspicious situations is crucial in protecting oneself from emotional and financial harm. Seniors should not feel obligated to continue communicating with individuals who exhibit concerning behavior or make unreasonable demands.

Furthermore, seniors should stay informed about current trends and developments in online scams through reputable sources such as government agencies, consumer protection organizations, or cybersecurity experts. Being aware of new tactics employed by scammers can empower seniors to adapt their strategies and remain one step ahead of potential threats.

Protecting oneself against online romance scams requires a combination of awareness, skepticism, and proactive measures. By educating themselves about common scam tactics, exercising caution in online interactions, safeguarding personal information, seeking support from trusted individuals, and staying informed about emerging threats, senior citizens can reduce their vulnerability to exploitation and enjoy safer online experiences. It is imperative for seniors to prioritize their safety and well-being in the digital age, and by implementing these strategies, they can mitigate the risks associated with online romance scams.

Cyber-Savvy Seniors

Content brought to you by:
Senior Housing Crime Prevention Foundation

How to Tell Fact from Fiction:

Tips for Being News Savvy Online

In our digital age, the internet has become the primary source of news and information for many people. With the vast amount of content available online, it's crucial to be discerning and news savvy to separate fact from fiction, and to stay well-informed about current events. Being news savvy online is not just about consuming news but also about critically evaluating the sources and information you encounter. These tips will help you become more news savvy online.

Diversify Your Sources
One of the key principles of being news savvy is to diversify your sources. Relying on a single news outlet or platform can result in a biased or one-sided perspective. Seeking out a variety of sources with different viewpoints and editorial styles will provide you with a more comprehensive understanding of an issue and help you avoid the pitfalls of echo chambers.

Fact-Check Before Sharing
The ease of sharing information on social media has led to the rapid spread of fake news. Before sharing any news article or information, take a moment to fact-check. Use reputable fact-checking websites such as Snopes, PolitiFact, or FactCheck.org to verify the accuracy of the claims made in the article. Promote responsible sharing by only passing along information that is well-sourced and verified.

Be Skeptical of Clickbait
Clickbait headlines are designed to attract attention and generate clicks, often at the expense of accuracy or context. Be skeptical of sensational headlines and dubious claims. Read the full article and check for credible sources to ensure that the information is reliable. Don't fall for the temptation to click on flashy headlines without scrutinizing the content.

Learn Media Literacy
Media literacy is the ability to analyze, evaluate, and critically interpret the news and media you consume. Educate yourself about media literacy concepts, including bias, objectivity, and credibility. Information and resources are available online for media literacy, which can be invaluable in navigating the digital news landscape.

Check the Publication Date
Online content can sometimes be outdated or no longer relevant. Always check the publication date of news articles and reports to ensure you are getting the most current information. Old news can lead to misunderstandings and misinterpretations of events.

Cyber-Savvy Seniors

Content brought to you by:
Senior Housing Crime Prevention Foundation

How to Tell Fact from Fiction:

Tips for Being News Savvy Online

continued from page 1

Avoid the Comment Section
Comment sections on news websites and social media can be breeding grounds for misinformation, trolling, and heated arguments. While they can sometimes offer valuable insights, they are often not the best place for thoughtful, constructive discussions. It is more productive to engage with news in a more controlled and respectful environment.

Verify the Source
Be vigilant in verifying the credibility of the news source. Reputable news outlets adhere to ethical journalism standards, have established editorial boards, and disclose their sources. Avoid sources with a history of spreading false information, sensationalism, or extreme bias.

Follow Journalists and Experts
Many journalists, scholars, and experts maintain active social media profiles where they share their insights and analyses. Following them can provide you with direct access to credible sources and expert opinions.

Use Aggregator Sites
News aggregator websites gather the latest news stories from various sources, creating a personalized news feed in one location. They allow you to customize your news feed by selecting topics and sources of interest. These platforms can help you stay organized and informed by gathering headlines from various sources in one place.

Engage in Critical Thinking:
Critical thinking is a fundamental skill for being news savvy. Question the information you encounter, consider its source, weigh the evidence, and think critically about its implications. Don't accept information at face value; instead, ask questions and seek the full context.

Being news savvy online is essential for navigating the vast and often overwhelming digital news landscape. By diversifying your sources, fact-checking, and embracing media literacy, you can develop the skills necessary to separate credible news from misinformation. Engaging with news responsibly is not only a personal responsibility but also a vital part of preserving the integrity of our information ecosystem. Stay curious, stay critical, and stay informed.

Cyber-Savvy Seniors

Content brought to you by:
Senior Housing Crime Prevention Foundation

Typo-Squatting

Unveiling the Threat, Exposing the Scam, and Fortifying Your Defense

In the vast landscape of the internet, where every click and keystroke can lead to new opportunities or unforeseen dangers, users must navigate with caution. One insidious threat that preys on our human tendency to make typographical errors is typo-squatting. Typo-squatting, short for "typographical squatting," involves the registration of domain names similar to popular websites with the intention of exploiting users who make innocent spelling mistakes. This deceptive practice has the potential to scam unsuspecting individuals, compromise sensitive information, and tarnish the online experience. Here, we explore the nature of typo-squatting, the tactics employed by cybercriminals, and offer practical advice on how to avoid falling victim to this deceitful scheme.

The Nature of Typo-Squatting
Typo-squatting capitalizes on the inevitability of human error in typing, especially when users hastily enter URLs or perform searches. Cybercriminals strategically register domain names that resemble those of well-known websites or brands, counting on users to make mistakes such as transposing letters, omitting characters, or misspelling words. For instance, a typo-squatter might register a domain like "googgle.com" or "facebok.com," hoping that users will unwittingly visit these sites instead of the authentic ones.

How Typo-Squatting Scams You
Once a user lands on a typo-squatted website, the potential for scams and malicious activities skyrockets. Cybercriminals can employ a variety of tactics to exploit visitors, ranging from phishing attacks to the distribution of malware.

• Phishing Attacks
Typo-squatted sites often mimic the appearance of legitimate websites to trick users into providing sensitive information such as login credentials, credit card details, or personal data. Unsuspecting users may enter their information, thinking they are on a trusted site, only to fall victim to identity theft or financial fraud.

• Malware Distribution
Some typo-squatted websites are designed to infect visitors' devices with malware. These malicious programs can range from ransomware that locks users out of their systems until a ransom is paid, to spyware that steals personal information without the user's knowledge. Inadvertently visiting such sites puts users at risk of compromising the security of their devices and data.

• Financial Scams
Cybercriminals may use typo-squatted domains to engage in various financial scams. This could include

→

Cyber-Savvy Seniors

Content brought to you by:
Senior Housing Crime Prevention Foundation

Typo-Squatting

Unveiling the Threat, Exposing the Scam, and Fortifying Your Defense

continued from page 1

fake online stores selling counterfeit goods, investment scams, or fraudulent fundraising campaigns. Victims may lose money, receive substandard products, or unknowingly contribute to criminal enterprises.

How to Avoid Typo-Squatting
Protecting oneself from the perils of typo-squatting involves adopting a combination of awareness, diligence, and technological aids. Here are some practical tips to avoid falling victim to typo-squatting:

• Double-Check URLs
Before clicking on a link or entering a URL, take a moment to carefully examine the spelling and structure. Check for subtle variations, misspellings, or additional characters that might indicate a typo-squatting attempt.

• Use Bookmarks
Whenever possible, access websites through saved bookmarks or favorites rather than typing the URL manually. This reduces the risk of making typos and inadvertently landing on a malicious site.

• Implement Security Software
Invest in reputable antivirus and anti-malware software that can detect and block access to potentially harmful websites. Keep these security tools updated to ensure they can recognize the latest threats, including typo-squatting attempts.

• Stay Informed
Keep abreast about current phishing and scam trends. Regularly check for updates from trusted sources, such as cybersecurity blogs, to stay ahead of emerging threats and understand the tactics used by cybercriminals.

In the dynamic and interconnected realm of the internet, users must be vigilant to protect themselves from the ever-evolving landscape of cyber threats. Typo-squatting stands as a prime example of how cybercriminals exploit human error for their malicious intents. By understanding the nature of typo-squatting, recognizing the potential scams it can lead to, and adopting proactive measures to avoid falling victim, users can fortify their defenses against this deceptive practice. The key lies in cultivating a cybersecurity mindset, combining awareness with practical precautions to navigate the digital world safely and securely.

Cyber-Savvy Seniors

Content brought to you by:
Senior Housing Crime Prevention Foundation

Tips for Keeping Your Data Safe Online

Create Complex Passwords

Downloading a password manager will create and store encrypted passwords and protect your accounts by keeping your passwords in a secure location. Make a habit of also regularly changing your passwords.

Protect Personal Information

Never give out personal information over the phone or through text. Most agencies, organizations, and companies would never ask for such information in this manner.

Beware of Links

Be cautious before clicking on links! Hover over any hyperlinks you receive in email or on web pages to preview their locations. Hackers disguise hyperlinks to look legitimate so people are enticed to click on them.

Two-Factor Authentication

Always enable two-factor authentication on your accounts. It might be tedious, but this is an extra layer of security designed to ensure that you're the only person who can access your accounts, even if someone knows your passwords.

Update Regularly

Update your phone, app, and browser software as often as you can. These updates often include new security updates that your current software may not have.

Cyber-Savvy Seniors

Content brought to you by:
Senior Housing Crime Prevention Foundation

Tips for Keeping Your Data Safe Online

Secure Accounts

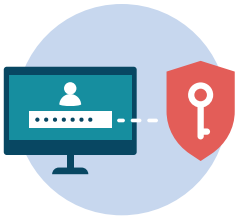
continued from page 1

Set up the security configurations of your social network accounts. For example, in Facebook, you can prohibit third-party companies to collect your data.

Maintain Privacy

Publish minimal personal information to social networks. Do not click on advertising links and do not take entertainment tests. Consider using a VPN (Virtual Private Network) for browsing the internet to maintain anonymity online.

Ensure Encryption



Make sure that the web pages you visit are “HTTPS” encrypted. If the URL starts with only HTTP without the S, do not log in, and never enter sensitive data to the page.

Watch out for Wifi

Avoid using public Wifi hotspots, since most often, data is being collected through them. For example, shopping online in an airport using public wifi could potentially put your credit card information at risk.

Antivirus Protection

Antivirus protection software fends off computer viruses and ransomware that could encrypt your files and demand payment to restore them. You need antivirus to avoid Trojan horse programs that seem valid, but steal your private information.

Cyber-Savvy Seniors

Content brought to you by:
Senior Housing Crime Prevention Foundation

Gift Card Scams

How to spot, avoid, and resolve gift card scams

Gift cards are great, right? Birthdays, Christmas – no worries about needing to return or exchange anything if it doesn't fit. That's why they are so popular for gift giving. The keyword here is Gift. Gift cards are for giving as gifts. They are not intended as a form of payment. If you are ever asked to make a payment with gift cards, know that you are getting scammed. Neither reputable businesses, nor the government will ever ask to be paid by gift card.

Imposters may call or email, claiming they are from the IRS, saying that you owe taxes or fines. They might pretend to be offering technical computer support. Some even try to impersonate family members in trouble that need some emergency funds. What scammers like this usually have in common is that they demand that you act **RIGHT NOW!** In the past, these scammers would often ask for a wire transfer of money, but increasingly, they have shifted to gift cards.

Typically, one of the more popular scams goes like this: the caller will instruct that you buy gifts cards with a popular brand name like Amazon, Google Play, or iTunes at a retailer near you, like CVS or Walmart. They might even ask to stay on the phone with you while you go into the store. Once you buy the cards, they'll ask you to read the gift card numbers and PINs to them. That allows them immediate access to the money you just put onto them. Once that happens, your money is simply gone.

Another scam reported is one where you list a gift card for sale either in the classifieds or on various online forums. When a "buyer" makes you an offer to pay for the card, they will ask you to put them on a three-way call with the card merchant to confirm there really is the right balance on the card. However, as they listen to the call, they record the touch tones used to verify the card number. Then they can use the card without ever paying for it.

Other kinds of scammers demanding payment by gift card include:

- callers pretending to be from a utility company, telling you to pay your bill by gift card or they'll cut off your power or water
- sellers on online auction sites who ask for gift cards to "buy" big items like cars, motorcycles, boats, RVs, tractors and electronics
- someone posing as a service member to get your sympathy, claiming they have to sell something quickly prior to a deployment and need you to pay by gift card

- callers who say you've won a so-called prize, for a sweepstakes you probably never entered – but first, you have to use a gift card to pay fees or other charges
- someone buying something from you, probably online, who sends a check for more than the purchase price – and asks you to give them the difference on a gift card. (That check, by the way, will turn out to be fake.)

These are all scams. In fact, if anyone tells you to pay by gift card, or by wiring money – for any reason – that's a sure sign of a scam. Without exception.

Cyber-Savvy Seniors

Content brought to you by:
Senior Housing Crime Prevention Foundation

Gift Card Scams

continued from page 1

How do you avoid gift card scams?

If you get or give a gift card, here are some steps to follow:

1. Buy gift cards from sources you know and trust.
2. Inspect a gift card before you buy it.
3. Keep the receipt with the gift card.
4. Read the terms and conditions of the gift card.
5. Use the card as soon as you can.
6. Treat gift cards like cash.

Quick Tips

Hang Up on Fake Callers
No reputable company nor government agency (including the IRS) will ever demand payment with gift cards. If someone claims to be from the IRS, hang up. (Don't believe emails either.)

Balance Check in Private
If someone asks to listen as you call to confirm the balance of a gift card, it is likely a scam.

Inspect Gift Card Packaging
If the packaging looks tampered with or the PIN is revealed, turn the gift card into the cashier and pick a different card.

Check the Activation Receipt
Be sure the gift card number listed on the activation receipt matches the gift card you receive. Alert the manager if it's not a match.

Only Buy from Reputable Resellers
Only buy discount gift cards from a gift card reseller that has customer service and will give you a money-back guarantee on purchases.

Save Activation Receipt
Whenever you buy a gift card, save the purchase and activation receipt until the gift card is redeemed.

Where do I report a gift card scam?

In addition to reporting gift cards used in a scam to the companies that issued the gift cards, also report it to the FTC at ftc.gov/complaint.

Can you get your money back?

If you paid a scammer with a gift card, report it as soon as possible. Call the company that issued the gift card and tell them the gift card was used in a scam. Ask them if money is still on the card, and if they can refund your money. It's very difficult to get your money back but the sooner you report it, the better your chances. Be aware that some companies will not return any money even if the gift card hasn't been used. Remember to keep the gift card itself, and keep the gift card receipt. Also, tell the store where you bought the gift card as soon as possible.

Lastly, do not be afraid or embarrassed. Scammers are hoping to make you feel this way so you will not ask other people for help. Do not fall for it. These people are very good at what they do (unfortunately), but there are many more good people in the world who are willing and wanting to help.

Cyber-Savvy Seniors

Content brought to you by:
Senior Housing Crime Prevention Foundation

Phlushing Phish

Recognizing and avoiding fraudulent attempts to obtain your sensitive information

No – don't flush the pet goldfish! What we are talking about here is Phishing. That is a cybercrime where targets are contacted by phone, online, email, or text message by someone posing as a legitimate institution, or someone you know to lure you into providing sensitive data like personally identifiable information, banking and credit card details, and passwords. The Phishers then use the personal data to access important accounts. This can result in identity theft as well as loss of money or property.

What Lures catch the most Phish?

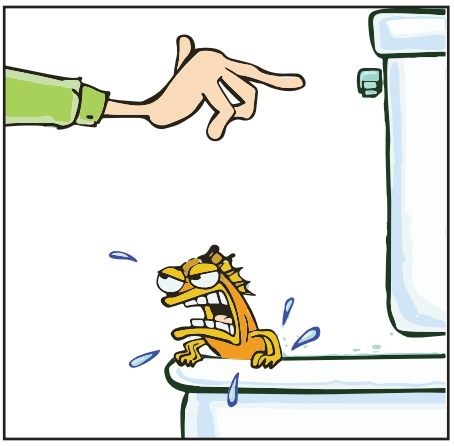
- Company or family names that sound familiar.
- Links to click to enter banking info or passwords. Either the info is stolen directly, or the links install malware that infect your computer and steal other information found there.
- Pressure tactics to hurry you into thinking if you don't act quickly there will be negative consequences.

Don't get hooked; do your research.

- You can always end a conversation and turn around and call the entity that reached out to you to determine if it is legitimate or not.
- You can ask the caller for a number to call back, but you need to look up the real customer service number for the bank or credit card or whatever entity the caller claimed to represent.
- Know that the IRS never makes outbound calls – they reach out to taxpayers by mail.
- Also educate yourself about your bank or your credit issuers business practices. There are questions they would never ask that scammers will.

Phish-tales – the telltale signs that something might be amiss:

- *Personal Information Requests* - You are asked for things like passwords, mother's maiden name, date of birth, etc.
- *Too Good To Be True* - Lucrative offers and eye-catching or attention-grabbing statements are designed to attract people's attention immediately. For instance, many claim that you have won an iPhone, a lottery, or some other lavish prize. Just don't click on any suspicious emails. Remember that if it seems too good to be true, it probably is!
- *Sense of Urgency* - A favorite tactic amongst cybercriminals is to ask you to act fast because the super deals are only for a limited time. Some of them will even tell you that you have only a few minutes to respond. When you come across these kinds of emails, it's best to just ignore them.



Sometimes, they will tell you that your account will be suspended unless you update your personal details immediately. Most reliable organizations give ample time before they terminate an account and they never ask patrons to update personal details over the Internet. When in doubt, visit the source directly rather than clicking a link in an email.

- *Hyperlinks* - A link may not be all it appears to be. Hovering over a link shows you the actual URL where you will be directed upon clicking on it. It could be completely different, or it could be a

→

Phlushing Phish

continued from page 1

popular website with a misspelling, for instance www.bankofarnerica.com - the 'm' is actually an 'r' and an 'n', so look carefully.

- *Attachments* - If you see an attachment in an email you weren't expecting or that doesn't make sense, don't open it! They often contain payloads like ransomware or other viruses.
- *Unusual Sender* – A message might come from a company claiming you've done business with them when you know you haven't. Or a message to you might be missing your name, misspelling it, or uses bad grammar or what might sound like computer translations from another language. Whether it looks like it's from someone you don't know or someone you do know, if anything seems out of the ordinary, unexpected, out of character or just suspicious in general don't click on it!

Wear your lifejacket: some phishing scams are quite convincing, so be wary and protect yourself.

- Ensure that your computer security and virus protection is updated and that you have a backup of all of your important files and information – an external hard drive storage device is good for this.
- Make use of multi-factor authentication when available– that is a second step to verify who you are, like a code texted to your phone.
- If you believe any of your passwords have been compromised, change them immediately and don't use them for any other accounts. It is a good practice to use complicated passwords and update them frequently.

The Phishing Report

You can forward phishing emails to spam@uce.gov and reportphishing@apwg.org as well as report problems to the FTC at ftc.gov/complaint. More info available at ftc.gov/phishing

Cyber-Savvy Seniors

Content brought to you by:
Senior Housing Crime Prevention Foundation

Power Of Attorney

What you need to know regarding Power of Attorney and your aging loved ones

Great news! America is getting old. If that doesn't sound great to you, consider the alternative. What I'm talking about here is the continuing increase in the percentage of Americans aged 65 and above. As those of the Baby Boomer generation reach retirement age, more and more families find themselves in care-giving roles. By 2030, all baby boomers will be older than 65, and the Census Bureau projects that will grow the size of the older population so much that 1 in 5 people in the U.S. will be retirement age. According to the latest population projections, by 2035 adults 65 and older will outnumber children for the first time in U.S. history. And by 2040, adults 85 and older will increase by 126%. Along with the responsibility to help keep our loved ones happy, healthy, and cared for often comes the responsibility to assist in handling financial matters. That is why **it is important, despite the fact that it can be a difficult topic, we should all have conversations with our loved ones about designating Power of Attorney rights when necessary.**

With the increasing age of our population, something else is also increasing: financial exploitation of the elderly. Numbers vary depending on the source, but it is estimated that at least $2.9 Billion is lost each year to elder financial exploitation. There are a variety of ways to help protect against this, but one of the simplest and most important things you can do to protect the financial affairs in your family is to arrange for another person to manage finances if anyone should become incapacitated for any reason. Although many people overlook this important step, **if you don't set up a financial power of attorney, assets could be thrown into chaos if unforeseen circumstances arise.** Many years of hard work spent building an estate could be left at the mercy of the courts who will decide how to handle affairs. Americans do not like to talk about money. A Lexington Law poll found that we are more likely to talk about any other subject—including romance, politics, and religion—than money. Though a serious and unexpected health crisis could occur, and no one would know how to access a parent's finances to do simple things like pay household bills. There are steps that families can take ahead of time that can help caregivers save time and energy when stressful events arise.

It should come as a relief to know that **setting up power of attorney documents is *not* difficult.** Some states allow you to complete forms on your own while other states may require a more formal process. In all cases, you'll need to make sure the proper document is signed in front of witnesses and then notarized. A

separate but equally important consideration is a power of attorney related to healthcare, giving a trusted individual the right to make health-related decisions on another's behalf if that ever becomes a necessity. One can note specific wishes about treatments, or even to deny treatment, such as adding a Do Not Resuscitate Order.

Legally, a power of attorney is a document that allows a principal to appoint an agent to act for them should they become incapacitated. The agent is expected to

→

Power Of Attorney

continued from page 1

place the principal's interests ahead of his or her own, which is why it is important for you and your loved one to pick a trusted individual. There are multiple types of decisions that the agent can be given the power to make, including the power to:

- Make financial decisions
- Make gifts of money
- Make healthcare decisions, including the ability to consent to giving, withholding, or stopping medical treatments, services, or diagnostic procedures. (Note: your loved one can also make a separate "health care power of attorney" to give only this power to another individual.)
- Recommend a guardian

There are four types of power of attorney that each have their own unique purpose:

1. *General Power of Attorney*
   In this situation, the agent can perform almost any act as the principal, such as opening financial accounts and managing personal finances. A general power of attorney arrangement is terminated when the principal becomes incapacitated, revokes the power of attorney, or passes away.
2. *Durable Power of Attorney*
   This arrangement designates another person to act on the principal's behalf and includes a durable clause that maintains the power of attorney after the principal becomes incapacitated.
3. *Special or Limited Power of Attorney*
   In this instance, the agent has specific powers limited to a certain area. An example is a power of attorney that grants the agent authority to sell a home or other piece of real estate.
4. *Springing Durable Power of Attorney*
   In some states, a "springing" power of attorney is available and becomes effective when a specified event occurs such as when the principal becomes incapacitated.

Power of attorney is flexible and can take effect at any time, not just after you sign it. For example, a financial power of attorney may kick in only after a doctor certifies that a person has become incapacitated. The person selected to have a power of attorney then becomes your agent and has legal authority to act on your behalf regarding your financial affairs.

The ability to give broad-based authority to a designated agent is available, or can be limited to only certain functions such as dealing with real estate, or securities or other specific elements of an estate. The key is to remember that a power of attorney ends with death, after which time the executor of the estate takes charge of assets. It's helpful to have these conversations in happy times, when your loved one is well so you can determine their wishes for their financial security and healthcare should a time come when they are unable to make the choices for themselves.

Cyber-Savvy Seniors

Content brought to you by:
Senior Housing Crime Prevention Foundation

Putting a Stop to Robocalls

Phone ringing off the hook with unwanted calls?

OK – most phones don't have hooks anymore. Here, we'll share some tips on how to rid both landlines and cell phones of those awful robocalls that continue to proliferate. Preventing these kinds of calls reduces your risk of common telephone scams, and sales pitches that aim to part you with your money.

Let's start with landlines. If your phone has a small screen that displays the incoming number, you may have noticed that often callers show as "anonymous", "blocked", "private", "unknown", or even "telemarketer". Most legitimate calls from actual people come up with a genuine phone number, so it's likely that you won't miss much at all if you reject unidentified calls. Most landline carriers offer Anonymous Call Rejection. You can activate it my dialing *77. Once you hear three beeps and hang up, any future incoming calls with hidden numbers will be rejected. This does vary by carrier, and some charge for the service, so you'll want to check with your provider for details. Please note that this tip only works for landlines. Using *77 on a mobile phone will have different results depending on where you are, including connecting with emergency services, so save this trick for your house telephone.

The National Do Not Call Registry works for any kind of phone number. There are a couple of ways to get on their list that makes it illegal for telemarketers to call you. While not all scammers follow the rules or respect this list, it does offer a measure of protection previously unavailable. You can visit donotcall.gov and enter any number that you'd like for the unwanted calls to be blocked (note this

doesn't work for fax numbers). Or, you can dial **1-888-382-1222** from any phone you wish to be included on the Do Not Call Registry. Any number you submit remains on that list until you ask for it to be removed or once you release the number. It may take some time to realize the benefit of the registry, as some telemarketing firms only update their lists periodically, so expect a gradual reduction in unwanted calls.

Note also that if you have done business with a company within the last 18 months, you are considered a customer and that business has a right to reach out unless you ask them not to. Be aware that often, a company that you have done business with (for example a mortgage lender or insurance company) may be owned by another larger company that offers different products or

Putting a Stop to Robocalls

continued from page 1

services. Those calls are technically allowed even if they seem unrelated or unwanted. If you do happen to answer an unwanted call, you can ask the caller to "please put me on your 'Do Not Call' list" and they must honor that request. Another note, political, charity, and survey calls are permitted so you won't be able to prevent calls like that through the Do Not Call Registry.

Harder to block are calls that mask their number with a false one. This is called "spoofing". Often, these numbers appear to be from your own area code, or look similar to your own phone number, so they seem more trustworthy than an out-of-state number. You can reach out to your phone carrier to determine options for blocking these calls. It can be challenging since you may block an incoming number, but the same scammer uses a different "spoofed" number each time.

Cell phone/wireless carriers have a combination of free/included with your plan protections against robocalls, and also supplemental plans with extra protection for a small monthly fee. Check with your carrier to learn what kinds of options are available to you.

There are also a number of third-party call blocking apps you can download to your cell phone. These apps can identify who is calling you and block the unwanted calls that show up on crowd-sourced spam and robocall lists. Many offer a free trial so you can experiment to see which ones work best for you before you subscribe to anything. One example is **Nomorobo.** It works on both Apple and Android platforms and is free for the first two weeks, then costs either $1.99 per month, or just $19.99 for the whole year if you sign up for 12 months. Others to try include **Truecaller** and **Hiya.**

If even after you have entered your numbers on the registry, experimented with call blocking apps, and your phone carrier settings, some calls are still making it through, you still have a couple of options. Let calls go to voicemail. You'll be able to tell by the message left (if one is left at all) if a call seems legitimate, without missing out on any real, important calls.

If a bad call makes it through, do not engage. Be your own Robocop. The only thing you ever need to say is "put me on your 'Do Not Call' list", and you can always just hang up. You can't hurt a robot's feelings.

Cyber-Savvy Seniors

Content brought to you by:
Senior Housing Crime Prevention Foundation

What is Smishing?

Combating text-based phishing attempts

Have you been "smished"? You might be familiar with the term "phishing" (see another one of our resources titled ***Phlushing Phish***). That is when scammers try to get your personal information by sending fraudulent links to you by email. Smishing is a term referring to phishing attempts that happen on your phone via text messages. **According to Norton Security, smishing attacks have increased 300% in the last two years.**

Your phone is an important, convenient tool. People are increasingly reliant on all the functionality that a phone can pack into your fingertips. Scammers understand that phones are increasingly where more commerce happens. Therefore, they know that it is likely there are passwords in your phone they'd like to get a hold of, along with your credit card information and any other personal data that could be used to steal your identity. They want access to data about you that is stored in apps that you use for things like banking and shopping.

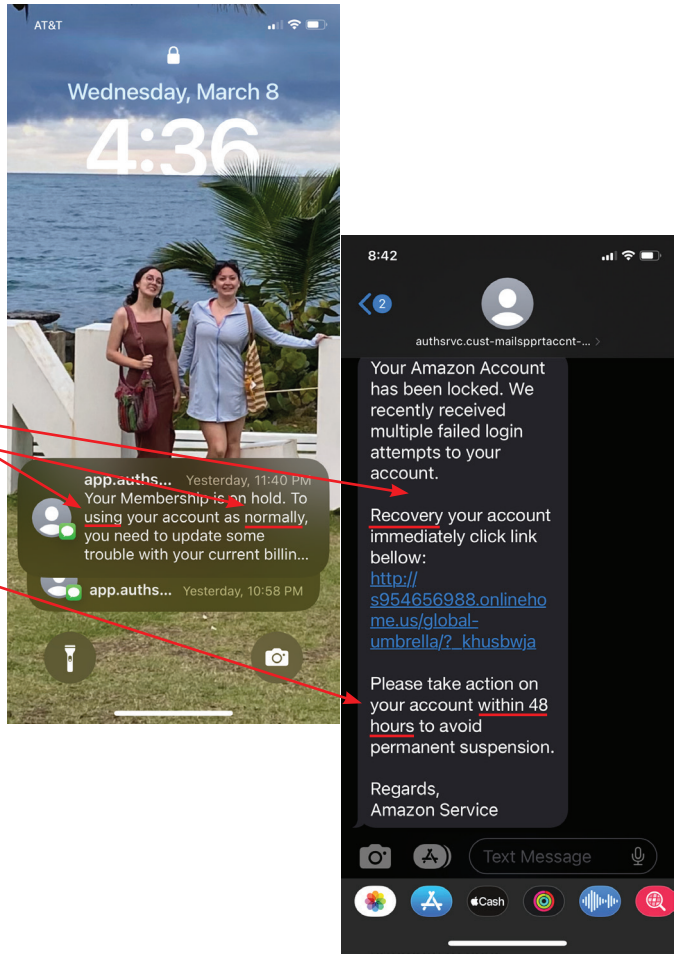
You'll find some of the characteristics of smishing resemble those of phishing attempts.

- Word often misspelled
- Grammar errors
- Refers to an account you haven't used lately
- Package/product you didn't order
- Urges you to act fast
- Originates from unknown phone number frequently repeated, often late at night – phone numbers might not be formatted in the typical way
- Weird looking links that don't match name

Smishing attempts tend to fall into certain categories:

You've Won! If you've received a "Congratulations" message, you'll be familiar with this scam. This tactic advertises a fake contest giveaway you've won and try to get you to click on a malicious link to claim your prize. Once you continue to their site, malware could make its way onto your device and compromise your system and the information attached. Example: Be the first person to visit this link and win a free gaming system!

Confirmation smishing scams use fake confirmation requests to get you to compromise sensitive information. This could be for an online order, an upcoming appointment, or an invoice for business owners. The message may contain a link directing you to a site that asks you to input login credentials or other sensitive data to verify your appointment or purchase.



Cyber-Savvy Seniors

Content brought to you by:
Senior Housing Crime Prevention Foundation

What is Smishing?

continued from page 1

Customer support smishing scams send smishing texts posing as any company a person may trust — not just banks or credit card companies. They may pose as representatives from online businesses or retailers notifying you of an issue with your account. They'll provide directions to solve the issue, which typically includes you going to a fake site infected with spyware to record any information you type in.

Financial/banking services smishing scams leverage the fact that more and more people are managing their finances online. These smishing messages pose as legitimate and trustworthy banking institutions to get you to compromise sensitive data like Social Security numbers, addresses, phone numbers, passwords, and emails. Example: ATTENTION! Reactivate your credit card at this link NOW.

Tips

- Have a locking code or face ID activated on your phone
- Don't store sensitive information like passwords, credit card numbers and social security numbers on your phone.
- Don't click links!
- Don't use public wifi, especially if you are using a credit card for a transaction, or entering sensitive personal info. Hackers can intercept your data from these networks.
- Don't set up apps to automatically log you in, and be sure to log out of apps once you are done using them.
- Always keep track of your phone – don't leave it out where just anyone could access it. Consider loading the Find my iPhone app or Lookout for Android phones to help you find a phone if one goes missing.
- If your phone does disappear, call your phone provider and let them know it is lost or stolen. If you did happen to store credit card or other sensitive information on your phone, contact your bank or card servicer immediately.

Cyber-Savvy Seniors

Content brought to you by:
Senior Housing Crime Prevention Foundation

Tech Support Scams

A technical support scam, or tech support scam, is a type of fraud in which a scammer claims to offer a legitimate technical support service. Victims contact scammers in a variety of ways, often through fake pop-ups resembling error messages or via fake "help lines" advertised on websites owned by the scammers. Technical support scammers use social engineering and a variety of confidence tricks to persuade their victim of the presence of problems on their computer or mobile device, such as a malware infection, when there are no issues with the victim's device. The scammer will then persuade the victim to pay to fix the fictitious "problems" that they claim to have found. Payment is made to the scammer through ways which are hard to trace, such as gift cards, and have fewer consumer protections in place which could allow the victim to claim their money back.

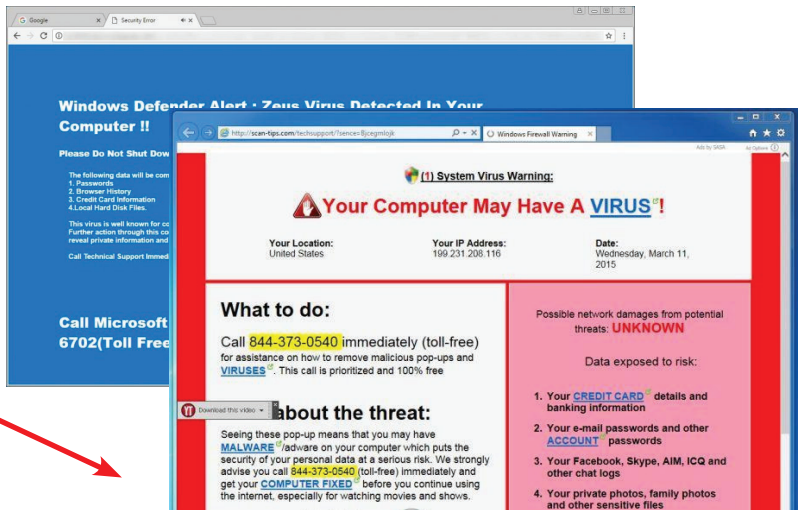
It could start with a pop-up in your internet browser that looks like a

blue screen error

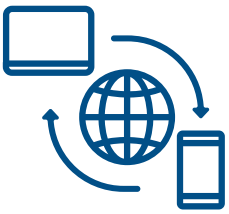
or

anti-virus software

and will likely urge you to call a toll-free number IMMEDIATELY and may make threats that you could lose your personal data if you don't call right away.



If the scammer is lucky enough to get a call from you, they will likely:



request that you grant them remote access,

act like they are running diagnostic testing,

pretend they have found a virus or other security breach,

and attempt to sell you repair service or a new security subscription.

Cyber-Savvy Seniors

Content brought to you by:
Senior Housing Crime Prevention Foundation

Tech Support Scams

continued from page 1

You'll be asked to pay a fee, but the "services" you'll get are at best worthless, and at worst, malicious.

- things you can get elsewhere for free
- things you already have
- "fixing" a problem that doesn't exist
- subscriptions that don't do anything
- installing malware

What Can Be Done?

If you get a pop-up, call, spam email or any other urgent message about a virus on your computer, stop.

- Don't click on any links or call a phone number.
- Don't send any money.
- Don't give anyone control of your computer.

Microsoft does not display pop-up warnings and ask you to call a toll-free number about viruses or security problems.

Report it at ftc.gov/complaint. Include the phone number that you were told to call.

Keep your security software up to date. Know what it looks like so you can spot a fake.

Tell someone about this scam. You might help them spot it and avoid a costly call.

Cyber-Savvy Seniors

Content brought to you by:
Senior Housing Crime Prevention Foundation

What To Do

FEDERAL TRADE COMMISSION
CONSUMER ADVICE

if you've been scammed

originally published by the Federal Trade Commission

Scammers can be very convincing. They call, email, and send us text messages trying to get our money or sensitive personal information — like our Social Security or account numbers. And they're good at what they do. Here's what to do if you paid someone you think is a scammer or gave them your personal information or access to your computer or phone. If you paid a scammer, your money might be gone already. No matter how you paid, it's always worth asking the company you used to send the money if there's a way to get it back.

IF YOU PAID A SCAMMER

Did you pay with a credit card or debit card?
Contact the company or bank that issued the credit card or debit card. Tell them it was a fraudulent charge. Ask them to reverse the transaction and give you your money back.

Did a scammer make an unauthorized transfer from your bank account?
Contact your bank and tell them it was an unauthorized debit or withdrawal. Ask them to reverse the transaction and give you your money back.

Did you pay with a gift card?
Contact the company that issued the gift card. Tell them it was used in a scam and ask them to refund your money. Keep the gift card itself, and the gift card receipt.

Did you send a wire transfer through a company like Western Union or MoneyGram?
Contact the wire transfer company. Tell them it was a fraudulent transfer. Ask them to reverse the wire transfer and give you your money back.

MoneyGram at 1-800-926-9400
Western Union at 1-800-448-1492
Ria (non-Walmart transfers) at 1-877-443-1399
Ria (Walmart2Walmart and Walmart2World transfers) at 1-855-355-2144

Did you send a wire transfer through your bank?
Contact your bank and report the fraudulent transfer. Ask them to reverse the wire transfer and give you your money back.

Did you send money through a money transfer app?
Report the fraudulent transaction to the company behind the money transfer app and ask them to reverse the payment. If you linked the app to a credit card or debit card, report the fraud to your credit card company or bank. Ask them to reverse the charge.

Did you pay with cryptocurrency?
Cryptocurrency payments typically are not reversible. Once you pay with cryptocurrency, you

→

Cyber-Savvy Seniors

Content brought to you by:
Senior Housing Crime Prevention Foundation

What To Do

if you've been scammed

continued from page 1

can only get your money back if the person you paid sends it back. But contact the company you used to send the money and tell them it was a fraudulent transaction. Ask them to reverse the transaction, if possible.

Did you send cash?
If you sent cash by U.S. mail, contact the U.S. Postal Inspection Service at 877-876-2455 and ask them to intercept the package. To learn more about this process, visit USPS Package Intercept: The Basics.

If you used another delivery service, contact them as soon as possible.

IF YOU GAVE A SCAMMER YOUR PERSONAL INFORMATION

Did you give a scammer your Social Security number?
Go to IdentityTheft.gov to see what steps to take, including how to monitor your credit.

Did you give a scammer your username and password?
Create a new, strong password. If you use the same password anywhere else, change it there, too.

IF A SCAMMER HAS ACCESS TO YOUR COMPUTER OR PHONE

Does a scammer have remote access to your computer?
Update your computer's security software, run a scan, and delete anything it identifies as a problem. Then take other steps to protect your personal information.

Did a scammer take control of your cell phone number and account?
Contact your service provider to take back control of your phone number. Once you do, change your account password.

Also check your credit card, bank, and other financial accounts for unauthorized charges or changes. If you see any, report them to the company or institution. Then go to IdentityTheft.gov to see what steps you should take.

REPORT A SCAM TO THE FTC

When you report a scam, the FTC can use the information to build cases against scammers, spot trends, educate the public, and share data about what is happening in your community. If you experienced a scam — or even spotted one, report it to the FTC at ReportFraud.ftc.gov.

Check out what's going on in your state or metro area by visiting ftc.gov/exploredata.