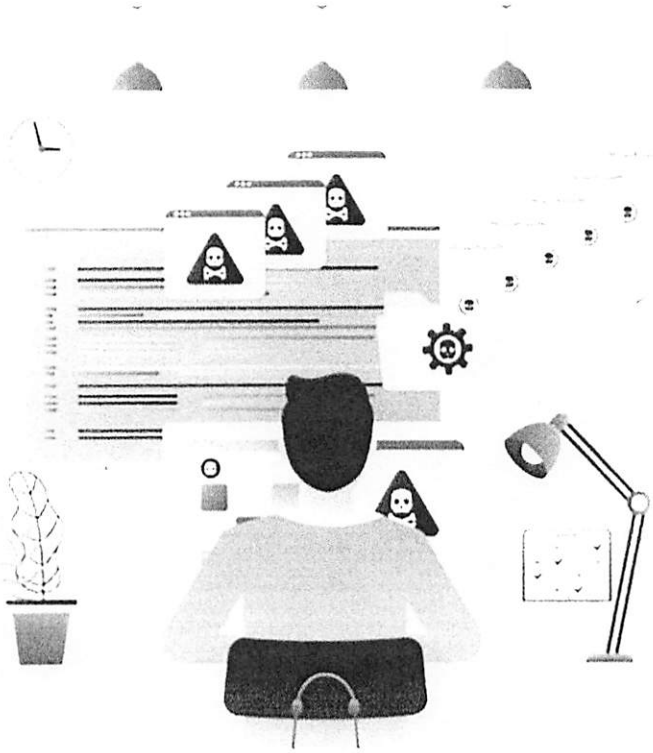
FDIC FEDERAL DEPOSIT INSURANCE CORPORATION

CONSUMER NEWS | OCTOBER 7, 2025

Protect Your Finances and Identity Online



Cybersecurity Keeps You Safe

According to the Federal Bureau of Investigation (FBI), cybercrimes are becoming increasingly common and many use sophisticated techniques. Preventing cybercrime requires consumers who are connected to the internet with a smart phone or computer to be aware and on guard. Most cyber criminals have two main goals – to steal your money and your identity. Knowing how to spot malicious cyber activities, how they work, and what you can do, are important to help protect yourself and your finances. Here is how to protect your personal and financial information:

Protect yourself when connecting to a public Wi-Fi network. Public Wi-Fi networks such as those offered by restaurants, cafes, or airports; may not use strong encryption or other security features, making them vulnerable to hackers. If possible, avoid making sensitive transactions, including purchases, on public networks. Also, you may consider using a virtual private network (VPN).

Don't send payments to unknown people or organizations. Never send electronic payments to people or organizations you are not familiar with, especially if they pressure you.

Don't open email or text messages from people or organizations you don't know. If you are unsure whether an email or text you received is legitimate, try contacting the sender directly via other means, such as going to the official website or calling a customer service number on a bill or credit card. Do not click on any links, pictures, or videos in an email or text unless you are sure it is safe.

Check the website addresses. Malicious website addresses may appear almost identical to legitimate sites. Scammers often use a slight variation in spelling or logo to lure you. It is also possible for search engines to provide advertisement links to malicious websites that appear similar to the one you are looking for. Malicious links can also come from friends whose email has unknowingly been compromised, so be careful and confirm a website address is accurate before clicking on it.

Secure your personal information. Don't provide any personal information, such as your date of birth, Social Security number, account numbers, or passwords to any person who contacts you. It could be a spoofing or phishing scheme. Legitimate organizations will never contact you unexpectedly to ask for that information. If you are uncertain, contact the organization directly through their official contact information to share information if needed.

Don't share personal information in online profiles and social media accounts. Sharing personal things like birthdates, pets' names, family members' names, locations and addresses, or employment information can give cyber criminals the hints they need to guess your passwords. FDIC Consumer News: Your Bank and Social Media has additional tips.

Use strong and unique passphrase or password for each online account. Strong passwords are critical to online security. Unique passwords will help isolate unauthorized access to online accounts, if one were to occur. Furthermore, periodically changing your passphrase or password is a proactive practice to mitigate security breaches to your important accounts.

Set up multi-factor authentication on all accounts that allow it. This provides an additional layer of security even when your password or

passphrase is compromised. It may also alert you of attempts to access your accounts without your permission. Consider passkeys when that is offered.

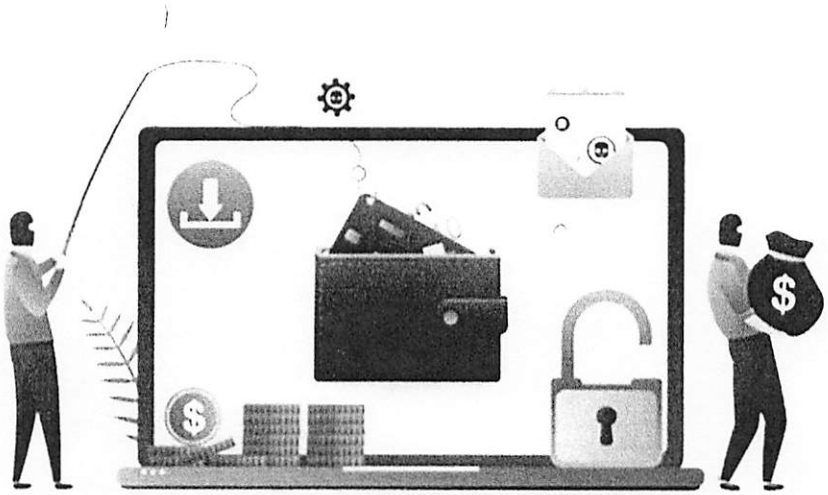
Keep your software programs up to date and maintain preventative software programs on all electronic devices. Install software that provides antivirus, firewall, and email filter services. Make sure your operating systems and applications are up to date. Older and unpatched versions of operating systems and software are the target of many hacks. Read the Federal Trade Commission's (FTC) online privacy and security

Stay informed on the latest cyber threats. Keep yourself up to date on current scams. Visit the FBI's Do yourself a favor: be crime smart for more updates.

Put these tips to work to protect yourself from some of the most common scams because criminals perpetrating these crimes often exploit weaknesses in personal cybersecurity practices or lack of awareness.

Imposters

Impostor scams are when a scammer pretends to be someone you know or trust to convince you to send them money. They may even claim they are with the FDIC or another government agency. These scams are communicated through emails, phone calls, letters, text messages, faxes, and social media. The messages might ask you to "confirm" or "update" confidential personal financial information, such as bank account numbers. In other cases, the messages might target people who recently lost money through a scam and are in need of assistance. The scammer will require an upfront payment in return for a deceptive promise to investigate or recover your losses. Some scams request that you file official looking forms, such as insurance claims, or pay taxes on prize winnings. They might claim that your financial accounts are under investigation for ties to a crime and demand that you provide access to the accounts for investigative purposes. Some schemes may claim that you have an unpaid debt and threaten you with a lawsuit or arrest if you don't pay. Other recent examples of scams include check endorsements, bankruptcy claimant verification forms, stock confirmations, and investment purchases.



Artificial Intelligence-Related Scams

Scammers may use artificial intelligence to create audio or images of family members or work contacts to convince you to send them money. Visit Tips on AI Scams for more information.

Online Dating and Professional Networking Sites

Scammers create fake profiles and try to develop romantic or professional relationships with people they target through online dating apps, social networking websites, or professional networking sites. Once the relationship develops and they have earned your trust, the scammer makes up a story and asks for money. Be aware that scammers are lurking in these areas, so you can keep yourself and your money safe. FDIC's Money Smart for Older Adults has additional information on scams.

Online Investment Scams

Scammers may create fake investment websites or fake investment assets and encourage you to invest in them, including new or emerging opportunities like cryptocurrencies. At first, they may show you making money to encourage you

to invest even more. Eventually, they take your money and disappear. More information can be found at the FTC.

Check Fraud

Unfortunately, checks can be stolen, altered, or forged in fraudulent schemes by bad actors who may exploit sensitive information like the account owner's name, account number, address, and signature. Fraudsters can attempt to digitally manipulate an image of a stolen check, even allowing them to make multiple fraudulent checks from a single original copy. The FTC's How to Spot, Avoid, and Report Fake Check Scams can be helpful in preventing check fraud.

Maintaining your cybersecurity will help prevent you from falling for identity theft and potential financial loss. Staying current on the latest types of scams can help you to identify the risks and learn how to avoid them, so you can protect yourself and your finances.

Additional Resources

- Money Smart for Older Adults: Avoiding Telephone and Internet Scams
- American Bankers Association Foundation: Banks Never Ask That! Fraud Prevention
- Federal Trade Commission: IdentityTheft.gov

Read Online
