THE Wealth REPORT

The rise of digital payments has made more Americans vulnerable to online fraud. Take these proactive steps to help protect your money and identity from being stolen by scammers and cybercriminals.

PROTECTING YOURSELF FROM CYBERCRIME

Eight tips for preventing hackers from stealing your money and identity.

Key Takeaways:

- Digital payment platforms have made it easier for scammers to part people from their money. Fortunately, you can make yourself a smaller target for fraud through vigilance and diligence.
- Treat digital payments like cash. Once you send money through payment apps, it may be gone for good. Always double-check the recipient and amount before hitting send.
- Monitor your accounts closely, checking all financial transactions at regular intervals and reporting suspicious activity immediately.
- Use strong, unique passwords by employing a password manager. Update passwords immediately after a breach.

Overview

As digital payment platforms become more widespread, hackers are looking to take a cut of the action. Around 65% of U.S. adults say they use a digital form of payment at least once a month, and in 2024, around $98 billion was transferred using digital platforms like PayPal, Venmo, Apple Pay and Samsung Pay.[1]

While it's easy and convenient to pay for products and services via digital transactions, it's not always the most secure method. Nearly 34% of Americans say they experienced financial fraud or a scam in 2024, with 37% of those people saying they lost money.[2]

Fortunately, it is possible to avoid scammers as long as you're vigilant. Here are our top suggestions for protecting your money and identity from would-be thieves.

Tips for Preventing Online Theft

1. Treat app-based transfers like cash payments.

Some apps don't allow you to cancel transactions once they're in progress. This makes it more difficult to get your money back once it's transferred out of your account. Before hitting "send" on a payment, double-check that it's going to the correct recipient and the amount of the transfer is correct.

2. Manage your passwords wisely.

Lots of people use the same password across many websites, including for our logins for financial accounts. But reusing the same password makes you more vulnerable to hackers, especially if the password is easy to guess.

The best practice is to use a complex, unique password every time you set up login credentials to a site. And don't write them down; instead, use a password manager to store all your login details, including usernames and passwords. If you do choose to write them down, keep the list in a safe, locked place.

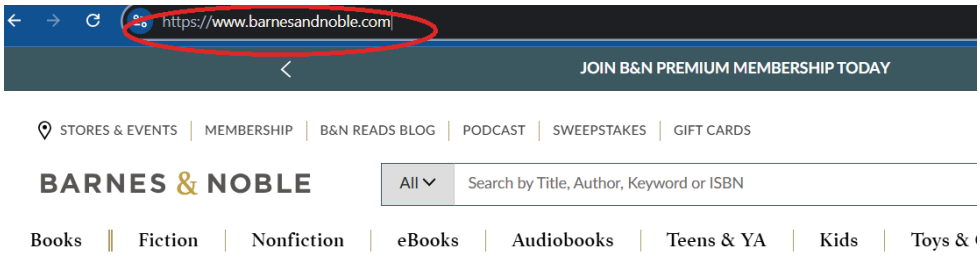
The other mistake many people make with passwords is not updating them frequently enough. Many cybersecurity experts recommend changing passwords every three months.[3] If you receive a notification from a retailer or financial institution that your account has been compromised, you should change your password immediately to avoid (or mitigate) loss.

3. Don't give out your information to people who contact you.

Have you ever received a phone call or email saying there's a problem with your account and asking you to verify sensitive information? Financial institutions and official organizations like the IRS will never ask you for details such as date of birth, Social Security number, account numbers or passwords in contact they initiate. If you receive communication requesting this information, call the institution directly to verify the legitimacy of the request.

4. Stay on guard for fakes.

Cybercriminals are smart — and they've gotten good at creating fake websites, emails and even in-app notifications that look like the real thing. If something looks or feels "off" about a message, trust your gut and don't complete the transaction. When you're shopping online, always look for the lock symbol and "https" in the website's address, indicating you're shopping at a secure site.



5. Manage your devices.

"Malvertising" is a form of malicious software in which hackers create seemingly innocuous advertisements infected with malicious codes. Once you click on the ad, hackers can use the malware to steal your identity or even take control of your device. Download ad blockers to prevent these ads from being displayed and reduce the chances of interacting with a malicious ad.

Also, don't ignore notifications that an update is available for your device. Many of these updates are fixing bugs and patching potential security holes. Install updates as soon as they are available to prevent data leaks.

6. Be wary of public Wi-Fi.

Public Wi-Fi is handy when you're out running errands or working in a coffee shop, but it can also provide a gateway for hackers to access your device. Avoid logging into financial websites or other sites where your sensitive information might be exposed until you're back on a private, secure network.

7. Embrace multifactor authentication.

You may have noticed that your bank, brokerage firm or other financial provider requires you to provide multiple identifying details when you call about your account. Likewise, many websites also use this multifactor authentication approach to verify your identity, requiring you to input a six-digit code or answer an additional security question. These steps may seem like a minor annoyance, but they are in place to protect you from fraud.

And speaking of security questions: Most really aren't that secure. A motivated hacker could probably find out your mother's maiden name or child's date of birth with a little sleuthing. Instead, choose security questions that aren't easily guessed or findable, such as the color of your first car.

8. Review transactions regularly.

The best deterrent to fraud is early detection. It's good practice to log in to your financial accounts weekly to review transactions and verify their legitimacy. Report any unexpected incoming payments to your financial institution; scammers sometimes use these to test whether your account is active before attempting to withdraw funds.

Final Thoughts

If you have been the victim of identity theft or online fraud, notify every financial institution where you have an account, including banks, credit unions, investment brokerages, etc. You can also place a 90-day fraud alert with the nationwide credit-reporting agencies:

- Equifax: www.equifax.com
- Experian: www.experian.com
- TransUnion: www.transunion.com

In addition, contact your financial professional to let them know your data has been breached. They can keep an eye out for any unusual transaction requests and help protect your hard-earned savings from potential scammers.

Sources

[1] CapitalOne Shopping Research. Jan. 26, 2025. "Digital Wallet Statistics." https://capitaloneshopping.com/research/digital-wallet-statistics/. Accessed May 28, 2025.

[2] Katie Kelton, CCC. Bankrate. March 3, 2025. "Survey: More than 1 in 3 Americans have faced a financial scam or fraud in the past year." https://www.bankrate.com/credit-cards/news/financial-fraud-survey/. Accessed May 28, 2025.

[3] McAfee. "How Often Should You Change Your Passwords?" https://www.mcafee.com/learn/how-often-should-you-change-your-passwords/. Accessed May 28, 2025.

6/25-4547037