

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

Overview

Digital payments are on the rise — and hackers are looking for a cut. More than 80% of Americans made a digital payment in 2021, using available payment platforms such as Zelle, PayPal and Venmo.¹ They also lost roughly \$6.9 billion to cybercrime in that same time frame.² And during the 2020 holiday season, 25% of Americans reported being the victims of scammers.³

It's easy and convenient to pay for things via digital transactions, but how can you protect yourself from being a victim of cybercrime? Here are our top eight suggestions for protecting your money and your identity from online thieves.

Eight Tips for Preventing Online Theft

1. Treat app-based transfers like cash payments.

Some apps, like Zelle, 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.

Let's face it: Most of us use the same password across many websites, including those from our financial institutions. But reusing the same password makes you more vulnerable to hackers, especially if the password is easy to guess. Instead, choose a complex, unique password every time you add or update a login. And it's best practice not to physically write them down; instead, tools such as LastPass can 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 most of us make with our passwords is not updating them frequently enough. Online security expert McAfee recommends changing passwords every three months.⁴ If you receive notification from a retailer or financial institution that your account has been compromised, you should change your password immediately.

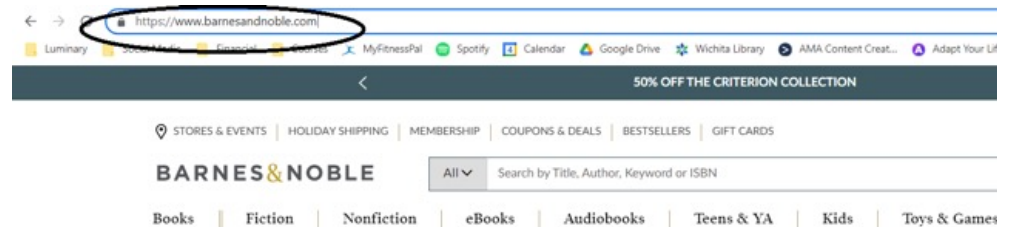


3. Don't give out your information to people who contact you.

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 such as the IRS or Social Security 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 requiring 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 over 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 Wi-Fi network.



7. Embrace multifactor authentication.

You may have noticed that your bank, brokerage or other financial firms require you to provide multiple identifying details when you call about your account. Likewise, some 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 security questions aren't really 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 best practice to log in to your financial accounts weekly to review transactions and verify their legitimacy. Report any unexpected 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 requests for transactions and help protect your hard-earned savings from potential scammers.



¹ Vaibhav Goel, et al. McKinsey & Company. Oct. 26, 2021. "New trends in US consumer digital payments." <https://www.mckinsey.com/industries/financial-services/our-insights/banking-matters/new-trends-in-us-consumer-digital-payments>. Accessed Nov. 14, 2022.

² Katherine Skiba. AARP. March 22, 2022. "FBI: Nearly \$7 Billion Lost to Cybercrime in 2021." <https://www.aarp.org/money/scams-fraud/info-2022/fbi-internet-crime-report.html>. Accessed Nov. 14, 2022.

³ Stefan Lembo Stolba. Experian. Nov. 18, 2020. "1 in 4 Americans Report Falling Victim to Fraud During the Holidays." <https://www.experian.com/blogs/ask-experian/survey-some-consumers-would-risk-identity-theft-for-an-online-holiday-deal/>. Accessed Nov. 14, 2022.

⁴ McAfee. Sept. 23, 2022. "How Often Should You Change Your Passwords?" <https://www.mcafee.com/blogs/tips-tricks/how-often-should-you-change-your-passwords/#:~:text=But%20how%20often%20should%20you,has%20access%20to%20your%20account>. Accessed Nov. 14, 2022.

This content is provided for informational purposes. It is not intended to be used as the sole basis for financial decisions, nor should it be construed as advice designed to meet the particular needs of an individual's situation. None of the information contained herein shall constitute an offer to sell or solicit any offer to buy a security. Individuals are encouraged to consult with a qualified professional before making any decisions about their personal situation. The information and opinions contained herein provided by third parties have been obtained from sources believed to be reliable, but accuracy and completeness cannot be guaranteed by AE Wealth Management. Neither AEWM nor the firm providing you with this report are affiliated with or endorsed by the U.S. government or any governmental agency. Investing involves risk, including the potential loss of principal. No investment strategy can guarantee a profit or protect against loss in periods of declining values. AE Wealth Management, LLC ("AEWM") is an SEC Registered Investment Adviser (RIA) located in Topeka, Kansas. Registration does not denote any level of skill or qualification. The advisory firm providing you this report is an independent financial services firm and is not an affiliate company of AE Wealth Management, LLC. AEWM works with a variety of independent advisors. Some of the advisors are Investment Adviser Representatives (IARs) who provide investment advisory services through AEWM. Some of the advisors are Registered Investment Advisers providing investment advisory services that incorporate some of the products available through AEWM. Information regarding the RIA offering the investment advisory services can be found at <http://brokercheck.finra.org>.

11/22-2592532

