

12 Credit Card Fraud Prevention Tips - Panda Security

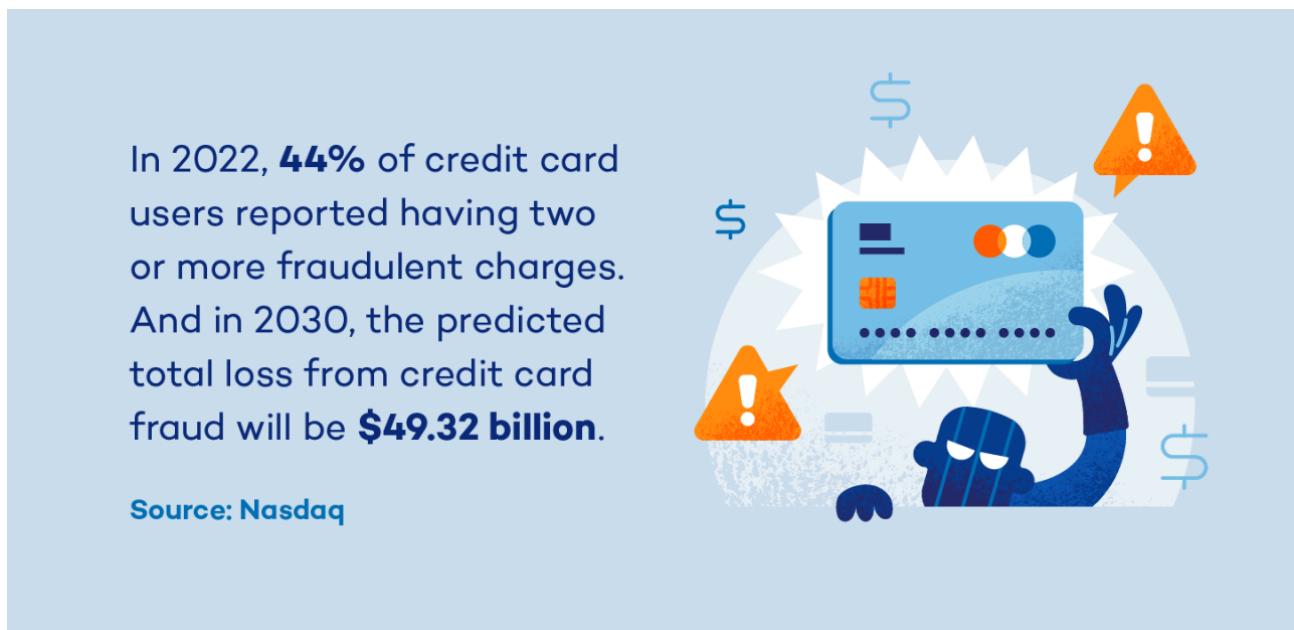
By Panda Security

Published: 2023-07-28 · Archived: 2026-04-06 03:15:27 UTC

In today's day and age, it's more important than ever to keep financial information close to the chest. Anyone can become a victim of credit card fraud, which is why it's critical to acquaint yourself with prevention tactics.

Credit card fraud is a form of theft where someone uses your credit card or bank information to purchase something without your authorization. Common warning signs include:

- Fraudulent charges or unauthorized transactions on statements
- Credit report changes such as new credit searches, accounts or address registrations
- [Stolen identities](#), receiving collection notices or invoices for accounts you didn't open



Safeguard yourself by implementing these 12 effective and practical tips for credit card fraud prevention.

1. Review Your Statements Regularly

Monitor your bank statements for signs of fraud, like purchases you don't recall making yourself, monthly if not more regularly. If possible, ask your bank to notify you of any suspicious or abnormal activity. This will help you promptly nip potential fraud in the bud.

2. Monitor Your Credit Report

A quick dip in your credit score can be indicative of activity from a malicious third party. Set up automatic score updates with your bank, or set monthly or even weekly personal reminders to check your score. To make this

easier, consider downloading your bank app to your smartphone. If you notice any anomalies, contact your bank and ask if they can shed some light on what might be causing them.

3. Report Lost Cards or Stolen Cards

If you notice one of your cards is missing, you should act immediately. Call your [credit card issuer](#) and report your lost card as soon as possible to prevent the escalation of fraudulent activity. The bank will deactivate the card and send you a new one. Once you receive your new card, continue to monitor your accounts for any suspicious activity.

4. Protect Your Account Information

Your account has delicate and private information like your name, address, [PINs](#), saved fingerprint data, and passwords. Avoid sharing or leaving this information to other people. You should also [avoid easy passwords](#) that other people can guess (like your birthday) and be careful when online shopping.

5. Destroy Old Financial Documents

The last thing you want is someone rummaging through your trash to steal your personal financial information. Instead of throwing sensitive financial documents in the trash, you can take the extra step to cut them up or put them through a shredder. Financial documents you should shred include:

- Receipts
- Bank statements
- Credit reports
- Tax returns older than 7 years
- Insurance claims
- Medical bills

6. Sign Up for Transaction Alerts and Payment Limits

Leverage features like transaction alerts offered by online bank services. You can receive real-time notifications regarding your card activity, like suspicious transactions and large payments or withdrawals. Plus, implementing a payment limit adds an extra layer of security.

Tips to Prevent Credit Card Fraud

Part 1

- Review your statements regularly
- Check your credit report
- Report lost cards or suspected fraud
- Protect your account information
- Destroy old financial documents
- Sign up for transaction alerts and payment limits



7. Don't Carry Cards You Won't Use

Though you may feel like you need all of your cards on you at one time, this is rarely the case. Avoid carrying around all your credit or debit cards to reduce the risk of theft or loss. Only go out with the ones you'll need to use, and store the other ones in a safe place.

8. Avoid Phishing Scams

You can find suspicious phishing scams in emails, phone calls, or text. They pretend to be your bank or someone else [demanding money](#), trying to obtain your personal information, or getting you to click a link or downloadable file to infiltrate your system.

9. Look Out for Skimming Devices

Get into the habit of approaching card readers with a healthy level of suspicion. Data thieves can attach skimming devices to these readers that copy credit card information when a card is inserted. If you notice the machine looks off, whether that be certain parts bulging out, misaligned, or broken, think twice before inserting your card, as it may have been tampered with.

10. Use Different Cards: Autopay vs. Everyday Spending

Splitting costs and automatic payments between several credit cards is a great way to prevent fraud from deeply affecting you before it even begins. If information from one gets stolen, quickly canceling it won't be nearly as big a deal as it would be if you made all your purchases using the same card.

11. Only Shop on Secure Websites

Secure websites have HTTPS (Hypertext Transfer Protocol Secure) before the URL — avoid using the ones that don't. HTTPS indicates that the website is secured and encrypts your data so malicious hackers don't have access to you or your financial information.

12. Be Wary of Public Wi-Fi

It's a good idea to avoid using public Wi-Fi since it rarely offers the same caliber of security as home networks, opening the door to malware. If you have to use it, avoid performing credit card transactions or accessing your bank account. Cybercriminals can intercept public Wi-Fi networks and access your information.



Tips to Prevent Credit Card Fraud

Part 2

- Don't carry cards you won't use
- Avoid phishing scams
- Look out for skimming devices
- Use different cards: autopay vs. everyday spending
- Only shop on secure websites
- Avoid public Wi-Fi

What to Do if You Become a Victim of Fraud

Credit card fraud has become so sophisticated that it may feel impossible to avoid. If you fall victim to credit card fraud, it is imperative to implement the right damage control tactics and do it fast. Follow these steps:

Damage Control for Credit Card Fraud



Notify the Credit Card Company



Contact Credit Bureaus



Update Security Information



Report Fraud to Law Enforcement

- **Notify your credit card company:** Don't hesitate to contact your bank and report your concerns. They're here to help and guide you through disputing charges and repairing your card security.
- **Contact the credit bureaus:** These may include Equifax®, Experian®, and TransUnion®. Report the incident and ask them to place a fraud alert on your credit file to prevent more accounts from being opened with your name in the future.
- **Update your security information on all accounts:** Change your passwords, security questions and PINs to add an extra layer of security and prevent more damage.
- **Report fraud to law enforcement:** Report all instances of fraud and [identity theft](#) to law enforcement. Provide relevant information and evidence about the fraud incident and file a report.

- **Continue monitoring:** Even though you did all the necessary reports, it's essential to keep monitoring all your accounts since your information got exposed.

Protect Your Financial Information With Panda Security

Safeguarding your financial information is crucial in today's digital landscape. Make a habit of implementing the 12 tips above to prevent credit card fraud.

[Panda Security's VPN](#) protects your online browsing so you can shop and use your credit cards in public places with peace of mind. With our expertise and [next-generation digital protection](#), you'll receive cybersecurity tailored to your wants and needs. Stay secure, stay protected!

Panda Security specializes in the development of endpoint security products and is part of the WatchGuard portfolio of IT security solutions. Initially focused on the development of antivirus software, the company has since expanded its line of business to advanced cyber-security services with technology for preventing cyber-crime.

Source: <https://www.pandasecurity.com/mediacenter/malware/poscardstealer-malware-pos/>