








The McAfee Safety Series

Credit Protection Guide



Table of Contents

	Protecting your credit—and your good name	3
	Credit protection basics	5
	How do thieves tap into your credit?	6
	What can you do about it?	7
	Securing your credit, online and off	8
	Steps for securing your credit online	8
	Steps for securing your credit while shopping in stores—and when offline too	12
	Monitoring and locking down your credit	14
	Monitoring your credit for unusual activity	14
	Credit lock and security freeze—two more powerful tools at your disposal	17
	Protecting your mobile wallets	18
	Steps for securing your mobile wallet	19
	What to do if you think you're a victim	20
	Six steps for recovering from credit theft or fraud	21
	You can take charge of your credit	23
	About McAfee	24



Protecting your credit—and your good name

Credit theft and fraud can creep up on you.

The bad news could come your way via a text alert from your credit card company about unusual activity. Or when you open your mail and see a suspicious charge on your statement. Maybe you receive a notice from a collection agency for an account you never opened. Worse yet, you get turned down for a loan because of a poor credit history—a poor history you weren't aware of and didn't create.

Credit theft and fraud affects millions of us. What can we do to prevent it? Plenty.

That's the trick with credit theft and fraud. People typically discover it after the damage is done. After that, they're stuck picking up the pieces, which can cost both time and money. Not to mention a potential knock to their credit score.

It happens often enough. Some figures estimate that for nearly every \$100 in purchases made with cards, somewhere around 7 cents of those purchases are connected with fraud or theft. As you can imagine that figure adds up quickly, to the tune of more than \$28 billion worldwide each year.¹

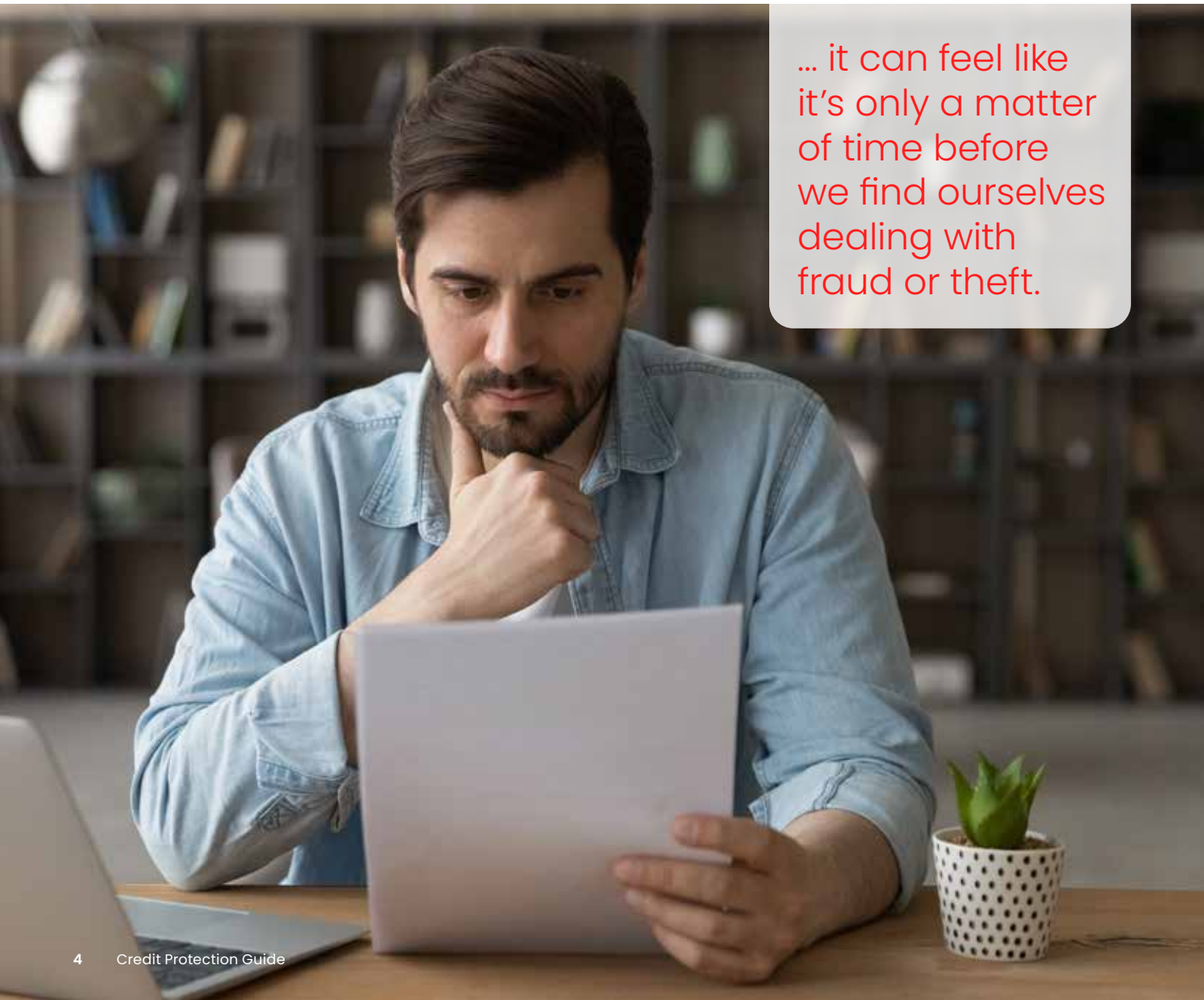
Whether the theft is large or small, it remains a problem. It means that one or more of your accounts has been compromised or that someone has gathered enough personal information about you to open a new account in your name—both of which require immediate action.

SECURITY GUIDE

With the rampant rise of data breaches and the many ways we pay and shop for things online, it can feel like it's only a matter of time before we find ourselves dealing with fraud or theft. That maybe preventing theft and fraud is largely out of our control.

However, you can take control.

The reality is that you have several preventative measures you can take to keep credit fraud and theft from happening in the first place. In this guide, we'll cover these measures in detail, show how they can protect you, plus walk through what you can do if you think you've fallen victim to fraud or theft. We'll start with a look at the basics ...



... it can feel like it's only a matter of time before we find ourselves dealing with fraud or theft.



Credit protection basics

Central to protecting your credit is protecting your identity.

The two share a close relationship, as identity theft and identity fraud can both target your credit. What's the difference between the identity theft and fraud? Well, it's subtle, so much so that it's easy to use them nearly interchangeably. While both can take a bite out of your wallet, they are different—and knowing the differences can help you know understand what's at stake.

Let's start with some definitions and a few examples of each.

Identity theft is ...

- When someone uses your personal information to open new accounts or services in your name—or possibly to impersonate you in other ways.
- Example:
 - A criminal uses your personal information to open a new line of credit at a retailer under your name and then makes purchases against the line of credit.

Identity fraud is ...

- When someone steals or misuses your personal information to exploit a credit card or debit card account you already have.
- Examples:
 - A criminal gets ahold of your debit card information from a data breach and makes purchases with it against your bank account.
 - A criminal gains access to one of your credit cards via a phishing attack and then makes purchases with it.

So, there's that subtle difference we mentioned. Identity theft involves stealing your personal information, which is then used to impersonate you in some way, such as opening new credit accounts in your name. Identity fraud involves misuse of an existing account, such as a credit or debit card you already have.

How do thieves tap into your credit?

It can happen in several ways:



Physical Theft

One of the readiest examples involves losing your wallet or debit card—or having them stolen outright. There are also instances where thieves will go through trash for bills and statements to gather personal information from them. Mailbox theft is in the mix too. Thieves will simply grab sensitive pieces of mail before you can get to them. And in more extreme cases, thieves will register a change of address with a bank, credit card, or utility to have your mail routed to them, where they can harvest your personal information and put it to their own illegal use.



Digital Theft

Life online opens a multitude of avenues for the theft of personal information. Data breaches at retailers, healthcare providers, insurance companies, financial institutions, and so forth can pump millions of credit and debit card numbers into the hands of bad actors—in addition to other pieces of highly useful personal information—whether directly or when purchased on dark marketplaces online.

Additionally, thieves may eavesdrop on public Wi-Fi and steal credit and debit information from people who're shopping or banking online without the security of a VPN. Also in public, hackers may compromise point-of-sale terminals and ATMs so that they can “skim” credit or debit card information during the transaction.

Lastly, bad actors make use of malware and scams to steal credit card information. They may inject spyware onto your device with a bogus email attachment or by steering you to a sketchy website. They'll also prop up phony online stores that fail to deliver the goods and steal your card number to boot. And then there are the phishing attacks via email, text, and direct message—all to pressure you into handing over your login and account information under entirely false pretenses.

What can you do about it?

Plenty. Knowing some of the ways hackers, scammers, and thieves can get a hold of your information nowadays gives you several other ways you can prevent it from happening.

As we go through the next sections of this guide, you'll see that some preventative measures call for heightened awareness on your part, others call for online protections you can put into place, while yet more are services that can monitor your credit to spot problems before they bloom out of control. Further, you can put additional protections in place that can help you recover far more quickly should credit card theft or fraud happen to you.





Securing your credit, online and off

We just covered several of the tricks that hackers, scammers, and thieves use to pry your credit information from you—anywhere from phishing attacks to riffling through your mail or garbage for old statements.

That calls for a mix of online protection and physical protection, and you can have several preventative steps at your disposal that can help keep you safer.

Steps for securing your credit online

Stick with known, legitimate retailers online

This is a great one to start with. Directly typing in the correct address for online stores and retailers is a prime way to avoid scammers online. In the case of retailers that you don't know much about, the U.S. Better Business Bureau (BBB) asks shoppers to do their research and make sure that retailer has a good reputation.² The BBB makes that easier with a listing of retailers you can search³ simply by typing in their name.

Look for the lock icon in your browser when you shop

Secure websites begin their address with “https,” not just “http.” That extra “s” stands for “secure,” which means that it uses a secure protocol for transmitting sensitive info like passwords, credit card numbers, and the like over the internet. It often appears as a little padlock icon in the address bar of your browser, so double-check for that. If you don't see that it's secure, it's best to avoid making purchases on that website.

Use a VPN if you're shopping on public Wi-Fi

Public Wi-Fi in coffee shops and other public locations can expose your private surfing to prying eyes because those networks are open to all. Using a virtual private network (VPN) encrypts your browsing, shopping, and other internet traffic, thus making it secure from attempts at intercepting your data on public Wi-Fi, such as your passwords and credit card numbers. [A VPN like ours can connect you automatically on unsecure networks](#), which makes keeping you and your device that much simpler.

What's more, a VPN masks your whereabouts and your IP address, plus uses encryption that helps keep your activities private. As a result, companies and [data brokers](#) can potentially learn far less about you, your shopping, your travels, your habits, and any other information that they could possibly collect and otherwise profit from.

Spot and avoid phishing attacks

Phishing attacks are one of the primary ways identity thieves steal personal information. Whether they come via a direct message, social media, email, text, or phone calls, thieves use them to harvest your personal info by posing as a legitimate organization—[such as in this recent IRS phishing scam](#) in the U.S. The best advice is don't click. If you get a notification that appears to be from one of your accounts, go directly to their website and log in from there to follow up. Also, be wary that [many phishing attacks play on emotions and sense of urgency](#). That's another sign the message could be bogus. [Comprehensive online protection software like ours](#) will also provide you with safe browsing features that can help you steer clear of malicious links and downloads.



Public Wi-Fi in coffee shops and other public locations can expose your private surfing to prying eyes ...

Clean up your personal data online

Yes, it's true. Your information gets collected, bought, and sold online. In fact, personal information fuels a global data trading economy estimated at \$200 billion U.S. dollars a year.⁴ Run by data brokers that keep hundreds and even thousands of data points on billions of people,⁵ these sites gather, analyze, buy, and sell this information to other companies as well as to advertisers. Likewise, these data brokers may sell this information to bad actors, such as hackers, spammers, and identity thieves who would twist this information for their own purposes.

Getting your info removed from these sites can seem like a daunting task. (Where do I start, and just how many of these sites are out there?) Our [Personal Data Cleanup](#) can help by regularly scanning these high-risk data broker sites for info like your home address, date of birth, and names of relatives. It identifies which sites are selling your data, and depending on your plan, automatically requests removal.

“Shred” your digital documents

For things like electronic tax forms, financial records, and other sensitive data on your computer, simply deleting a file is not enough. That data remains on the drive until it is written over or otherwise removed permanently. One way to go about that is with a digital document shredder that renders the data practically unusable when you're ready to trash the file. Comprehensive online protection software will often include such a feature, such as our own file shredder.



... simply deleting a file is not enough.

Create strong, unique passwords for every account

Comprehensive online protection software often includes a password manager that can generate strong, unique passwords for each of your accounts and remember them for you, which comes with our [online protection plans](#). [Use MFA \(multi-factor authentication\) on the accounts that give you the option](#), which makes it harder for a thief to crack your accounts, even if they have your password.

Use protection while you shop

A complete suite of [online protection software like McAfee+ can offer layers of extra security while you shop](#). In addition to the VPN, identity and credit monitoring, and other features mentioned above, it includes web browser protection that can block malicious and suspicious links that could lead you down the road to malware or a phishing scam—along with a password manager that can create strong, unique passwords and store them securely as well. Taken together, McAfee+ offers all-in-one online protection for your identity, privacy, and security that can keep you far safer when you shop online—and as you spend your time online in general.



Steps for securing your credit while shopping in stores—and when offline too

Use your phone's mobile wallet to make payments

Mobile wallets allow you to make an in-person payment with a wave of your phone, all while protecting your credit and debit card transactions in several ways. We'll cover them in more detail later in this guide, however, it's good to know about one strong form of protection they offer. Mobile wallets use unique encryption for each purchase, so if a bad actor intercepts the transaction, they're left with a string of effectively useless information. This differs from swiping your physical card where the terminal reads your credit card information from the magnetic strip on the back—information that a bad actor can steal and re-use.

Watch out for skimmers

Skimming occurs when credit card thieves install a reader device on an ATM, fuel pump, or point-of-sale device that lets them capture credit card information during a transaction. From there, the thief can make a counterfeit card or simply use the card information for online purchases. One thing to look for is if the terminal you're using looks like it's been tampered with in some way. Maybe the card reader looks bolted on or is loose or crooked in some way. Other skimming devices blend in far better and remain difficult to detect. One way to avoid skimmers is to use devices in places that are highly monitored, which would make it difficult for bad actors to install a skimmer on them. For ATMs, consider using an indoor terminal at a bank or making a cash withdrawal from a teller.



Invest in a paper shredder

Sensitive documents come in all forms. Top-of-the-line examples include things like tax returns, bank statements, and financial records. Yet there are also things like your phone and utility bills, statements from your doctor's office, and offers that come to you via mail. Together, these things can contain personal information such as account numbers, your full Social Security Number, the last four digits of your Social Security Number (which can still be useful to thieves), and other information that may uniquely identify you.

You'll want to dispose of sensitive documents like these so that they can't be harvested by hackers. For physical documents, consider the low-cost investment of a paper shredder to help ensure they don't fall into the wrong hands when you are done with them. (And let's face it, they're fun to use!)

Secure your mailbox

Thieves still loot mailboxes for documents that can help them steal your identity or gain access to your accounts. Depending on your situation, a locking mailbox may help prevent such theft. Also, if you're travelling, have a trusted person collect your mail or have the post office put a temporary hold on your mail. Another thing you can consider is going paperless with as many bills, statements, and invoices as possible, which will keep them out of your home's mailbox in the first place.

Thieves still loot mailboxes for documents that can help them steal your identity or gain access to your accounts.



Monitoring and locking down your credit

Another aspect of credit protection involves monitoring, where you keep an eye out for any purchases you didn't make or for entirely new accounts that you didn't apply for. Additionally, you can take steps to freeze or lock your credit report—a strong measure that can help prevent identity theft, such as when thieves take out loans or open new credit cards in your name.

Monitoring your credit for unusual activity

Check your bills and statements

Whether they come in the mail, email, or if you simply look them up online when it comes time to pay them, give your bills and statements a close review. Not every case of identity theft comes with a big-ticket purchase or outlandish charge. Even the smallest of suspicious charges could indicate a larger problem. If you spot an unknown charge, follow up with the company or institution in question and file a fraud report with them as needed.

Consider using a credit monitoring service

In addition to keeping an eye on your bills and statements as they come in, a credit monitoring service keeps tabs on your credit report. While you can do this manually, there are limitations. First, it involves logging into each bureau and doing some digging of your own. Second, there are limitations as to how many free credit reports you can pull each year. A service like [our own credit monitoring can check your credit for you regularly](#) without impacting your credit score depending on your location and plan⁶ for signs of identity theft.

Monitor your identity

Earlier, we brought up the dark web where personal information is bought and sold, stored, and exchanged. The problem is that it's particularly difficult for you to determine what, if any, of your PII is on the dark web where hackers and thieves can get their hands on it. Identity monitoring can help.

[McAfee's identity monitoring helps you keep your personal info safe by alerting you if your data is found](#), an average of 10 months ahead of similar services.⁷ If your information gets spotted, you'll get an alert, along with steps you can take to minimize or even prevent the damage if the information hasn't already been put to illegal use.

Take advantage of identity protection

[Identity theft protection and restoration through McAfee takes identity monitoring a step further by offering financial coverage for losses and expenses due to identity theft](#)—in addition to hands-on help from a recovery professional with limited power of attorney who can do much of the identity restoration work for you (U.S. only).

If you become the victim of fraud or theft after a data breach, a licensed recovery specialist can help you restore your credit and identity. If you've ever dealt with fraud or theft before, or know someone who has, recovery can be a time-consuming and stressful process if you undertake it alone. Working with an expert can lend you extra peace of mind in a couple of ways. First, you'll know that a professional is working on your case—a person who knows exactly where to start and what needs to happen for the best possible outcome. Second, you'll get precious time back, time you'd otherwise have to spend if you took on the process yourself.

A licensed recovery specialist can help you restore your credit and identity.



Find out your Protection Score

One of the trickiest parts of staying safe online is knowing exactly how safe you are. *Do I have the right protection in place? Is there more I could be doing?* Those are good questions to ask, and now you can get the answers to them with your Protection Score. As part of your McAfee subscription,⁸ the [Protection Score gives you a clear and easy-to-read overview of the health of your online safety](#). Next, it identifies and helps you fix security weak spots with simple instructions and then offers personalized feedback that helps you maintain healthy online protection.

For example, one way your Protection Score can help keep your identity secure is in the case of data breach. If your information is found in a data breach, your Protection Score goes down and your app sends you an alert. It then assists you in resolving the breach, your Protection Score goes back up, and monitoring continues, maintaining a lookout for future breaches and issues.



Credit lock and security freeze—two more powerful tools at your disposal

Consider a credit lock

As mentioned above, identity thieves can open new accounts in your name and damage your credit along the way. A credit lock can help keep that from happening. The protection offered will vary depending on where you live and the credit reporting agencies involved, yet it restricts access to your credit reports. This keeps companies from accessing your credit report, which can prevent thieves from opening accounts in your name. A credit lock will also prevent you from opening new accounts when it's in place, so using a lock takes some careful planning if you're about to rent an apartment, take out a car loan, apply for a new credit card, and so on.

For more information, check with the credit bureaus in your country—in the U.S., the major three being Equifax, TransUnion, and Experian. Likewise, depending on your location and plan,⁹ you can establish a credit lock from your McAfee online protection software (and lift it as needed), which prevents unauthorized people from opening accounts in your name.

Note that when using McAfee's credit lock feature, remember to freeze the other two credit bureaus in conjunction with the Credit Lock to ensure all three bureaus are covered.

Look into a security freeze

Another feature offered by McAfee depending on your location and plan¹⁰ is a [security freeze, which provides proactive protection in three ways](#):

- Credit freeze: Stops creditors from accessing your info to open new loans or credit cards.
- Bank freeze: Prevents fraudsters from opening a bank account in your name.
- Utility freeze: Prevents someone from opening a telecom, electric, water or other utility in your name.





Protecting your mobile wallets

An increasingly popular form of payment involves a mobile wallet kept on a smartphone. A mobile wallet acts as a financial transaction app that stores your account information on your smartphone, so you can pay with your phone even if you don't have your cards on you. Several well-known mobile wallets include:

- Apple Pay
- Google Pay
- Samsung Pay
- PayPal
- Venmo
- Walmart Pay
- AliPay
- Dwolla
- Vodafone-M-Pesa

The terms, conditions, and methods of moving funds in and out of a mobile wallet may vary from service to service, yet the technology that drives it remains the same. Using a mobile device's capabilities like Bluetooth connectivity, Wi-Fi, and encrypted magnetic signals, [you can pay securely](#) from your device to a point-of-sale terminal.

Despite all the encryption and security measures digital wallets make use of, there are potential downsides, such as the loss or theft of the mobile device, which could give a thief access to the cards stored in your mobile wallet. Accordingly, it falls on you to secure your phone—and take measures of your own to protect it if you're ever separated from it.

Steps for securing your mobile wallet

1. Lock your devices with a passcode.

Our recent worldwide study found that only [58% of adults protect their computers with a passcode and only 56% do the same on their smartphones](#). When you consider all the personal and financial information we keep on these devices, a lost or stolen device becomes an open book for an identity thief. Using a passcode, facial ID, PIN, or other form of locking your devices can make life tough on a thief in the unfortunate event of loss or theft.

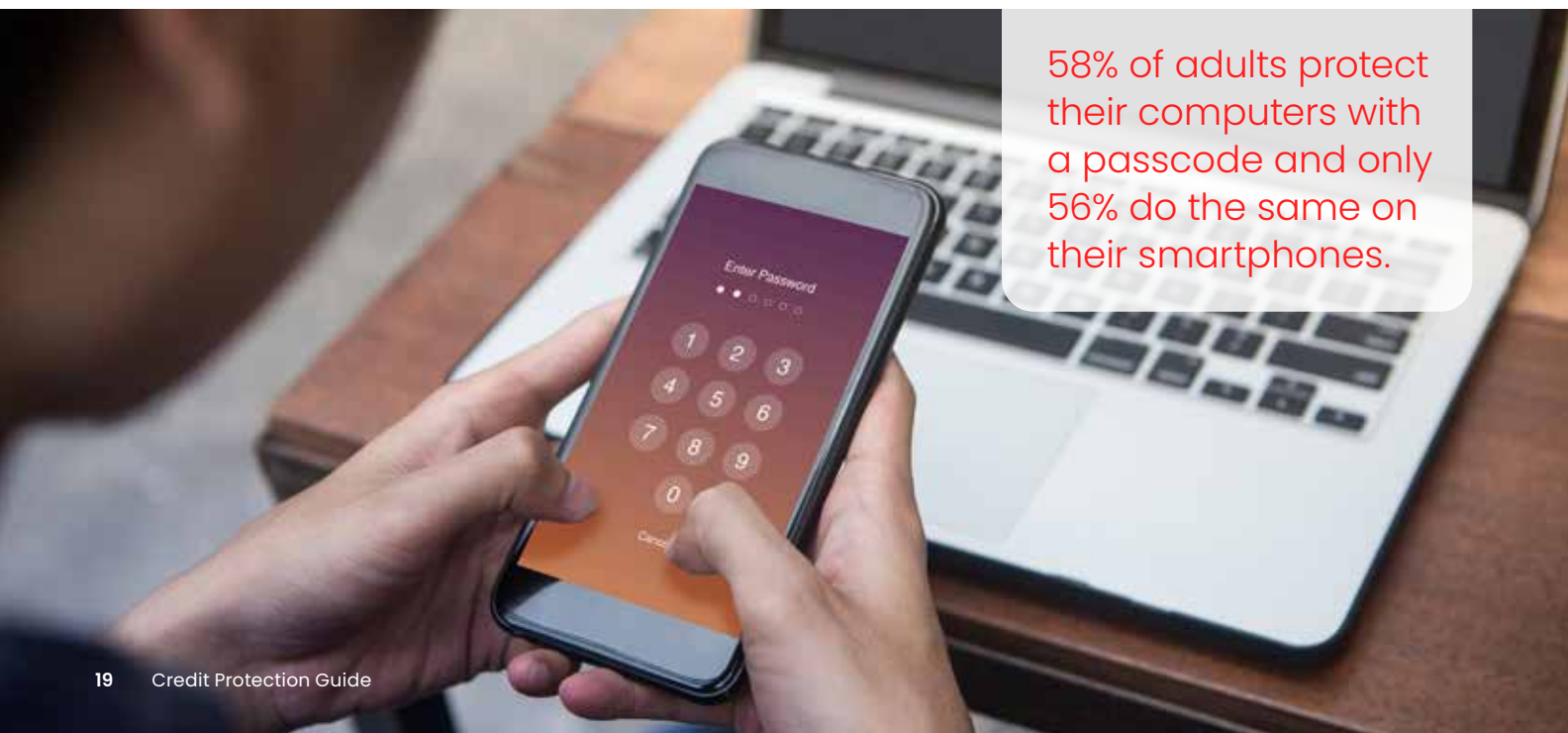
2. Learn how to remotely lock and wipe your devices.

Mobile devices have location tracking services to help find a lost device—in addition to features that let you remotely lock or even wipe the contents of the device if you fear it's lost for good or fallen into the wrong hands. When storing debit and credit cards on your phone, you'll certainly want to know how you can do this—and do it quickly.

- [Apple provides iOS users with a step-by-step guide for its devices](#).
- Google offers up a guide for Android users as well.

3. Use online protection software.

Given all the banking and shopping we do on our phones, let alone all the other activities that leave a trail of our personal information in their wake, [installing and using comprehensive online protection software is a must these days](#). It puts several layers of security in place, such as creating complex passwords automatically, antivirus, protecting your privacy and data online like [connecting with a VPN](#), and a host of other features for keeping you safe. In short, online protection software acts as a solid first line of defense.



58% of adults protect their computers with a passcode and only 56% do the same on their smartphones.



What to do if you think you're a victim

Another hard and fast truth about credit theft and fraud is that there's no sure-fire way of keeping them from happening entirely—even with precautions in place.

Whether you spot some unusual activity, or if you receive an alert from your monitoring service, there are several steps you can take if you think you've fallen victim:

- Notify the companies involved.
- File a police report.
- Contact your governmental anti-fraud or trade organization.
- Place a credit freeze or lock.
- Continue to monitor.
- Work with a recovery pro.

Realizing that you've become a victim carries plenty of emotion with it, which is understandable—the thief has stolen a part of you to get at your money, information, or even reputation. Once that initial rush of anger and surprise has passed, it's time to get clinical and get busy.

Think like a detective who is building—and closing—a case. That's exactly what you're doing. Follow the steps, document each one, and build up your case file as you need. Staying cool, organized, and ready with an answer for any questions you'll face in the process of restoring your identity will help you see things through.

Six steps for recovering from credit theft or fraud



1. Notify the companies involved.

Whether you spot a curious charge on your bank statement, discover potentially a fraudulent account when you check your credit report, or when you get an alert from your monitoring service, let the bank or organization involved know you suspect fraud or theft. With a visit to their website, you can track down the appropriate number to call and get the investigation process started. You can either work with the companies themselves, or if you have identity protection with McAfee, a recovery pro can work with them on your behalf, depending on your location and plan.



2. File a police report.

Some businesses will require you to file a local police report to acquire a case number to complete your claim. Beyond that, filing a report is a good idea in itself. Identity theft is still theft and reporting it provides an official record of the incident. Should your case of identity theft lead to someone impersonating you or committing a crime in your name, filing a police report right away can help clear your name down the road. Be sure to save any evidence you have, like statements or documents that are associated with the theft. They can help clean up your record as well.



3. Contact your governmental anti-fraud or trade organization.

In the U.S., the Federal Trade Commission's (FTC) identity theft website at www.identitytheft.gov is a fantastic support resource should you find yourself in need. In addition to keeping records of the theft, the FTC can provide you with a step-by-step recovery plan—and even walk you through the process if you create an account with them. Additionally, reporting theft to the FTC can prove helpful if debtors come knocking to collect on any bogus charges in your name. With a copy of your report, you can ask debtors to stop. Likewise, other nations have similar resources available and [our knowledge base article on identity theft offers suggestions for the specific steps you can take in specific countries](#), along with helpful links for local authorities that you can turn to for reporting and assistance.

Also contact your national tax or revenue agency as well if you believe your tax ID number was involved in identity fraud or theft. They will have their own reporting mechanisms and processes to assist you with the recovery process.



4. Put on a credit freeze or lock.

An instance of identity fraud or theft, suspected or otherwise, is a good time to review your options for a credit freeze or lock. As mentioned earlier, see what the credit bureaus in your region offer, along with the terms and conditions of each. With the right decision, a freeze or lock can help minimize and prevent further harm.



5. Continue to monitor.

Strongly consider using a monitoring service like the one we described earlier to take this on for you. The unfortunate fact of identity theft and fraud is that it can mark the start of a long, drawn-out affair. One instance of theft can possibly lead to another, so even what may appear to be an isolated bad charge on your credit card calls for keeping an eye on your identity all around.

Many of the tools you would use up to this point still apply, such as checking up on your credit reports, maintaining fraud alerts as needed, and reviewing your accounts closely—along with utilizing an identity monitoring service and the services of a recovery pro as needed.



6. Work with a recovery pro.

A recovery service can help you clean up your credit in the wake of fraud or theft, all by working on your behalf. Given the time, money, and stress that can come along with setting your financial record straight, leaning on the expertise of a professional can provide you with much-needed relief on several counts.





You can take charge of your credit

Just as the hackers, scammers, and thieves have several ways they can compromise your credit, you have several ways you can protect it.

While this may require some up-front work on your part, many of the security measures take care of themselves once you put them into place. This is particularly true if you're using online protection software that monitors your credit, identity, and personal information for you, which can help you stay safer and give you a little time back to yourself as well.

Any effort you put into prevention and monitoring now can pay off huge dividends later—particularly when you contrast that with the stress, costs, and time required to restore your credit in the wake of theft or fraud.

With all the payments we make and shopping we do online, part of the responsibility for staying safe falls on us. While businesses, banks, and organizations put precautions in place, relying on those alone is not enough. Data breaches happen. Hackers break into otherwise secure systems. And thieves continue to harvest bits and pieces of data so they can commit theft and fraud in our name. By shoring up your own defenses, you can take steps to stay safer and keep your credit intact.

In all, you can take charge of your credit in more ways than you might think.

For more on protecting your identity and online protection overall, our blog offers you and your family a terrific resource across a wide range of topics from online banking, gaming, and shopping to tough yet important topics like cyberbullying and which apps are safe for kids.

Our aim is to help you think about what's best for your family and the steps you can take to see it through so that you can make everyone's time online safer and more enjoyable.

Visit us any time!

<https://www.mcafee.com/blogs>

About McAfee

McAfee is a worldwide leader in online protection. We're focused on protecting people, not devices. Our solutions adapt to our customers' needs and empower them to confidently experience life online through integrated, easy-to-use solutions.

www.mcafee.com



For more information about
online protection, visit us at
mcafee.com/blogs

1. <https://www.paymentsdive.com/news/card-industry-faces-400b-in-fraud-losses-over-next-decade-nilson-says/611521>
2. <https://www.bbb.org/article/tips/14147-bbb-tip-black-friday>
3. <https://www.bbb.org/search>
4. <https://www.latimes.com/business/story/2019-11-05/column-data-brokers>
5. <https://sites.sanford.duke.edu/techpolicy/wp-content/uploads/sites/17/2021/08/Data-Brokers-and-Sensitive-Data-on-US-Individuals-Sherman-2021.pdf>
6. Credit monitoring is not available in all plans or locations.
7. Not all identity monitoring elements are available in all countries.
8. Protection Score is not available in all plans or locations. For more information on what factors affect your Protection Score and how it is calculated, see our [Protection Score page and FAQs](#). An excellent score does not guarantee total safety. No connected life can be totally secure, but an excellent score does show you're doing a good job of preventing and handling risks.
9. Credit lock is not available in all plans or locations.
10. Security freeze is not available in all plans or locations.



6220 America Center Drive
San Jose, CA 95002
888.847.8766
www.mcafee.com

McAfee and the McAfee logo are trademarks or registered trademarks of McAfee, LLC or its subsidiaries in the United States and other countries. Other marks and brands may be claimed as the property of others. Copyright © 2023 McAfee, LLC.
gd-credit-protection_0423 APRIL 2023