Security tips to protect yourself from hackers

> *Data breaches are becoming more common. Finding out you were part of one usually includes a laundry list compromised information, such as your password, username, and email address. What does that mean for your internet safety? What should you do? Learn how you can take control after a data breach and better protect your devices, online accounts, and personal data from cyber criminals.*

Home Breaches **Security Tips** Sign In

Protect your passwords from

cyber criminals, since that's
what they care about most.

Understand how hackers work

Forget about those hackers in movies trying to crack the code on someone's computer to get their top-secret files. The hackers responsible for data breaches start by targeting companies, not specific individuals. They want to get data from as many people as possible so they can use, resell, or leverage it to make money. It all starts with getting your password.

It's not personal. Not at first.

Hackers don't really care whose personal information and credentials they can get, as long as they can get a lot of it. That's why cyber criminals target massive companies with millions of users. These hackers look for a security weakness — the digital equivalent of leaving a door unlocked or window open. They only need to find one door or window to get inside. Then they steal or copy as much personal information as possible that lives in users' online accounts.

Once they get your data, cyber criminals can start their real work. We don't always know what they intend to do with the data, but usually they will find a way to profit from it. The effects to your online account might not be immediate. But they can be very serious.

All types of data can be valuable.

Some data — like banking information, bank card numbers, government-issued ID numbers, and PIN numbers — is valuable because it can be used to steal the victim's identity or withdraw money. Email addresses and passwords are also valuable because hackers can try them on other accounts. All sorts of data can be valuable in some way because it can be sold on the dark web for a profit.

What makes a password easy to guess.

If hackers can get a list of email addresses from a data breach, they already have a good start. All they have to do is pick their website of choice and try these emails with the most popular passwords. Chances are, they'll be able to get into quite a few accounts. So don't use any of these 100 Worst Passwords of 2018.

- 123456 and password are the most commonly used passwords. Don't use them.
- Switching a letter for a symbol (p@ssw0rd!) is an obvious trick hackers know well.
- Avoid favorite sports teams or pop culture references. Use something more obscure.
- Don't use a single word like sunshine, monkey, or football. Using a phrase or sentence as your password is stronger.

- Don’t use common number patterns like 111111, abc123, or 654321.
- Adding a number or piece of punctuation at the end doesn’t make your password stronger.

One exposed password can unlock many accounts.

Hackers know people reuse the same passwords. If your banking password is the same as your email password is the same as your Amazon password, a single vulnerability in one site can put the others at risk.

It’s why you should use different passwords for every single account. The average person has 90 accounts, and that’s a lot of passwords to remember. Security experts recommend using a password manager to safely store unique passwords for every site.

Hackers don’t care how much money you have.

Think you don’t need to worry because you don’t have much money to steal? Hackers couldn’t care less. There are countless ways to leverage all types of personal data for profit.

Through identity theft, cyber criminals can open new credit cards or apply for loans in your name. By getting your financial information, they can make purchases or withdrawals. These attackers can even find ways to target your friends and family once they gain access to your email.

@

Lock down your accounts to keep your information out of the wrong hands.

What to do after a data breach

You get an email, either from Firefox Monitor or a company where you have an account. There’s been a security incident. Your account has been compromised.

Getting notified that you’ve been a victim of a data breach can be alarming. You have valid cause for concern, but there are a **few steps you can take immediately to protect your account and limit the damage.**

Read the details about the breach.

Read closely to learn what happened. What personal data of yours was included? Your next steps will depend on what information you need to protect. When did the breach happen? You may receive the notice months or even years after the data breach occurred. Sometimes it takes awhile for companies to discover a breach. Sometimes breaches are not immediately made public.

If you haven’t yet, change your password.

Lock down your account with a new password. If you can’t log in, contact the website to ask how you can recover or shut down the account. See an account you don’t recognize? The site may have changed names or someone may have created an account for you.

If you’ve used that password for other accounts, change those too.

Hackers may try to reuse your exposed password to get into other accounts. Create a different password for each website, especially for your financial accounts, email account, and other websites where you save personal information.

Take extra steps if your financial data was breached.

Most breaches only expose emails and passwords, but some do include sensitive financial information. If your bank account or credit card numbers were included in a breach, alert your your bank to possible fraud. Monitor statements for charges you don't recognize.

Review your credit reports to catch identity theft.

If you have credit history in the United States, check your credit reports for suspicious activity. Ensure that no new accounts, loans, or cards have been opened in your name. By law, you’re permitted to one free report from the three major credit reporting bureaus every year. Request them through annualcreditreport.com. And don’t worry, checking your own credit report never affects your score.

Make your passwords strong,
secure, and hard to guess.

How to create strong passwords

passwords

Your password is your first line of defense against hackers and unauthorized access to your accounts. The strength of your passwords directly impacts your online security.

Combine unrelated words to make stronger passwords.

To create a strong password, try combining two or more unrelated words. It could even be an entire phrase. Then change some of the letters to special letters and numbers. The longer your password, the stronger it is.

A single word with one letter changed to an @ or ! (such as p@ssword!) doesn’t make for a strong password. Password cracking programs contain every type of these combinations, in every single language.

SECURITY TIP:

Steer clear of the 100 most-used passwords.

Every year, SplashData evaluates millions of leaked passwords and compiles the 100 most common ones. The most recent list includes password, 123456, and other passwords you shouldn’t use.

Certain words should be avoided in all passwords.

Many people use familiar people, places, or things in passwords because it makes their passwords easy to remember. This also makes your passwords easy for hackers to guess.

According to a study conducted by Google, **passwords that contain the following information are considered insecure because they’re easy to figure out.** You can find much of this info after reviewing someone’s social media profiles.

- Pet names
- A notable date, such as a wedding anniversary
- A family member’s birthday
- Your child’s name
- Another family member’s name
- Your birthplace
- A favorite holiday

- Something related to your favorite sports team
- The name of a significant other
- The word “Password”

Use different passwords for every account.

To keep your accounts as secure as possible, it’s best that every single one has a unique password. If one account gets breached, then hackers can’t use those login credentials to gain access to other accounts.

While no one can stop hackers from hacking, you can stop reusing the same password everywhere. It makes it far too easy for cyber criminals to attack one site and get your password for others.

Use a password manager to remember all your passwords.

Do you really need to remember 100 passwords? Not at all. A password manager is a piece of software that keeps all your password safe, encrypted, and protected. It can even generate strong passwords for you and automatically enter them in to websites and apps.

Password managers act like a digital safe-deposit box for all your online accounts. You just need one key to get into your accounts: A single, easy-to-remember but hard-to-guess password. That password unlocks the safe.

But what if your password manager gets hacked? A good one keeps your passwords encrypted behind a password they don’t know (only you do). They don’t store any of your credentials on their servers. While no single tool can guarantee total online safety, security experts agree that using a password manager is far more secure than using the same password everywhere.

Add an extra layer of security with two-factor authentication.

Many websites offer two-factor authentication, also known as 2FA or multi-factor authentication. On top of your username and password, 2FA requires another piece of information to verify yourself. So, even if someone has your password, they can’t get in.

Withdrawing money from an ATM is an example of 2FA. It requires your PIN code and your bank card. You need these two pieces to complete the transaction.

Websites that support 2FA include Google and Amazon. When you have 2FA enabled, the site will text you a code to enter after your password. Other forms of 2FA include YubiKeys USB ports and security apps like DUO.

When you set up 2FA, many sites will give you a list of backup codes to verify your account. A password manager is a great place to store these codes.

Password do’s and don’ts

Do	Don't
Do combine two or more unrelated words. Change letters to numbers or special characters.	Don’t use the word “password,” or any combination of it. “P@ssword!” is just as easy for hackers to guess.
Do make your passwords at least 8 characters long. Aim for 12-15 characters.	Use short, one-word passwords, like sunshine, monkey, or football.
Do use a combination of upper- and lower-case letters, numbers, and symbols.	Don’t place special characters (@, !, 0, etc.) only at the beginning or the end.
Do include unusual words only you would know. It should seem nonsensical to other people.	Don’t include personal information like your birthdate, address, or family members’ names.
Do keep your passwords protected and safe, like encrypted in a password manager.	Don’t share your passwords. Don’t put them on a piece of paper stuck to your computer.
Do spread various numbers and characters throughout your password.	Don’t use common patterns like 111111, abc123, or 654321.
Do create unique and complex passwords for every site.	Don’t use the same password everywhere.
Do use an extra layer of security with two-factor authentication (2FA).	Don’t think a weaker password is safer because you have 2FA.

Understand the most common threats and know what to look out for.

Steps to take to protect your identity online

Data breaches are one of many online threats. Using secure internet connections, updating your software, avoiding scam emails, and employing better password hygiene will help you stay safer while you browse.

Be wary of public Wi-Fi networks.

You can get Wi-Fi almost anywhere. But these open networks are the most vulnerable and tend to be the least secure. This includes the free Wi-Fi at restaurants, libraries, airports, and other public spaces. If you can avoid it, don't use public Wi-Fi. Most importantly, don't use these networks to log in to financial sites or shop online. It's easy for anyone to see what you're doing.

Instead, we recommend using a Virtual Private Network (VPN), which lets you use public Wi-Fi more securely and keeps your online behavior private. A VPN routes your connection through a secure server that encrypts your data before you land on a web page.

Run software and app updates as soon as they're available.

Updating software on your computer or phone can seem like a pain, but it's a crucial step to keeping devices safe. These updates fix bugs, software vulnerabilities, and security problems. Regularly updating your smartphone apps and operating systems makes your devices more secure.

Tips for keeping all your online accounts secure:

- Use unique, strong passwords for every account
- Use a password manager to remember all your passwords for you
- Turn on two-factor authentication for an extra layer of security
- Use a VPN (Virtual Private Network) when using public Wi-Fi
- Update to the latest version of all software and apps

SECURITY TIP:

Turn on automatic updates.

You can set your computer, browser, apps, and phone to update automatically as soon as new updates become available. Set it and forget it!

Be vigilant about emails that seem even a little bit strange.

Phishing is a type of email scam that is becoming increasingly common. In these emails, hackers impersonate a service or company you trust. These emails can even come from one of your contacts. They look like the real thing because they mimic the design of authentic emails, like those from your bank or email provider.

The goal of these hackers is to get you to unknowingly enter your password or download a document that can infect your computer. Most online services won't ask you to enter your login info directly from an email. If they do, you should instead go directly to their website to log in.

Think before you fill anything out. Does this email seem out of the blue? Does something seem off about it? Are you being asked to log in to an account to update something? Don't click, and don't enter your password anywhere. Open your browser, and type in the address of the company website instead.

Know the classic signs of a suspicious email.

- Displays grammar or spelling mistakes
- Send address looks unusual
- Promises something that seems too good to be true
- Asks you to log in from the email itself
- Asks you to open or download a file that you don't recognize

Be selective about who you give your email address to.

The more online accounts you create, the greater the risk that you'll be involved in a data breach. Many companies, services, apps, and websites ask for your email. But it's not always required. Here are some ways to avoid giving out your email address:

- Don't create an account if it's not required. For example, many online shopping portals allow you to check out as a guest.

- If a website requires an email address, use services like 10minutemail or Nada, which allow you to create a temporary one.
- Create a different email to sign up for promotions and newsletters. Don't include any personal info that could be used to identify you in that email address, like your name or birthday.

SECURITY TIP:

How to create strong passwords.

Include a combination of upper and lowercase letters, numbers, and characters. Combining a few unrelated words and changing the letters is a good method.

Read the guide

Use unique, strong passwords for every single account.

One of the best ways to protect yourself online is to use different passwords across all your online accounts. This way, hackers won't have the keys to your entire digital life if they get their hands on that one password you use everywhere.

Your passwords also need to be strong. Single words (like sunshine, monkey, or football) make for weak passwords. So do these 100 most-commonly used passwords, which include password and 123456. Avoid pop-culture references, sports teams, and personal info. Do not use your address, birthday, names of family members, or pets' names. The longer and more unique your passwords are, the harder they will be for hackers to crack.

SECURITY TIP:

Firefox recommends 1Password, LastPass, Dashlane, and Bitwarden for security and ease of use.

Remember all your passwords with a password manager.

Ever forgotten your password? It happens all the time. The average person has 90 online accounts. And we're being asked to create new ones all the time.

The good news is you don't have to recall all your passwords from memory. Password managers are secure, easy-to-use applications that do the remembering for you. They even fill your passwords into websites and apps when you need to log in. All you need to remember is a single password — the one you use to unlock your password manager. They can even generate hard-to-guess passwords to help make your accounts more secure. All your data is encrypted, making password managers pretty secure — even if they get hacked.

Learn how to avoid bad password habits that make a hacker's work easy.

5 myths about password managers

Password managers are the most recommended tool by security experts to protect your online credentials from hackers. But many people are still hesitant to use them. Here's why password managers are safe, secure, and your best defense against password-hungry cyber criminals.

What is a password manager?

Think of it like a safe for your passwords. When you need something inside the safe, you unlock it. Password managers work the same for your online credentials.

You create a single, super-strong password, which acts like a key. Install the password manager app on your phone, computer, browser, and other devices. Your passwords are securely stored inside it. Anytime you need to log in to an account, unlock your password manager and retrieve your login info.

Myth 1:
Password managers aren't safe or trustworthy.

With website vulnerabilities and security incidents on the rise, many people have grown to mistrust a tech tool to manage their passwords. What if the password manager gets hacked?

Reputable password managers take extra steps to lock down your info and keep it safe from cyber criminals.

A good password manager:

- Doesn't know your master password (so hackers can never steal it)
- Encrypts all your data
- Does not store any of your data on their servers
- Can generate strong, secure password

Myth 2:
Password managers aren't 100% secure, so I shouldn't use one.

No privacy tool can completely guarantee your online safety. Even the most elaborate lock can be broken into. Yet we still lock our doors to our houses and cars.

The alternative to using a password manager is to rely on your own memory to remember all your credentials. This inevitably leads to recycling passwords or using variations — a bad habit that hackers love.

Password managers can be such an effective security tool because they help us improve bad habits. With a password manager installed on your computer and phone, it's a lot easier to take your logins everywhere so you can use unique, strong passwords on every account.

Myth 3:
Storing all my passwords in one place makes them vulnerable to hackers.

Password managers don't store all your credentials together in one place. Any data you store in a password manager — passwords, logins, security questions, and other sensitive info — is securely encrypted. Even if the password manager gets hacked, cyber criminals would not be able to see your logins.

The only way to access your data is with a single master password that only you know. You use this password to unlock the manager on your computer, phone, or other devices. Once it's unlocked, a password manager can fill in your logins to websites and apps.

Myth 4:
Remembering all my passwords is safer than trusting technology to do it for me.

Our memories sometimes fail us. Ever clicked a "forgot password?" link? It's very common to use variations of the same password to make them easier to remember. With a password manager, you don't need to remember any of your credentials. It can be installed on all your devices and will auto-fill your passwords for you. Once you get in the habit of using one, you'll no longer have to worry about forgetting your credentials.

Myth 5:
It’s a huge pain to set up a password manager.

Sure, it takes time to log all your credentials in a password manager. But you don’t need to do it all at once. You can always start small and change just a few passwords at a time. Try installing a password manager and creating new, unique passwords for the websites you visit most frequently. Over time, as you log in to other sites, you can add others.

Find out how to mitigate the risks of identity theft to prevent financial loss.

Take further steps to protect your identity

When big data breaches happen, there’s immediately a lot of talk about credit reports. Security experts recommend you check your credit reports for suspicious activity. To protect your identity, they also recommend you freeze your credit. Here’s what that means and why it’s important.

What’s a credit report? Do I have one?

If you’ve ever rented an apartment, opened a bank account, or applied for a credit card or a loan, you likely have a credit report.

In fact, you have three credit reports. There are three credit-reporting bureaus in the United States: Experian, TransUnion, and Equifax. Each one holds a report on you that contains personal information about your credit history. Your credit reports contain:

- Personal identifying information, such as your name, past and current addresses, Social Security number, and date of birth.
- Current and past credit accounts, such as credit cards, mortgages, student loans, and auto loans.
- Inquiry information, which are instances in which you’ve applied for new loans or credit cards.
- Bankruptcies and collection information.
- Your credit report does not include your credit score.

Why you should check your credit reports once a year.

Having your information exposed in a data breach puts you at risk of identity theft. If someone steals your identity and tries to open new cards or loans in your name, it will appear on your credit reports. Each may have slightly different information, which is why it's important to check all three regularly.

By law, you are entitled to one free credit report a year from each of the three credit bureaus. You can request your credit reports at annualcreditreport.com. This is the only official and truly free website to obtain your reports. You can also call Experian, TransUnion, and Equifax directly or request your reports by mail.

Checking your own credit report will not affect your score.

You will never be penalized for checking your own report or your own credit score. And checking your report does not impact your score in any way. Experian, TransUnion, and Equifax may offer paid identity monitoring packages or charge for access to your credit score, but it's always free to check your report once a year.

Though the information on your credit report directly impacts your score, reports don't actually contain your score. There are many websites, services, and credit cards where you can check your score for free. So it's usually not necessary to pay the bureaus themselves to see your score.

What to look for to spot signs of identity theft.

When you receive your credit reports from Experian, TransUnion, and Equifax, review them carefully. These are long, dense documents that can be overwhelming, especially if you have a long credit history. Look for accounts or addresses you don't recognize or any information that is inaccurate. Make sure:

- All the accounts listed are ones you personally opened.
- All addresses listed and your employer are correct.
- Your balances and credit history are correct.
- All hard credit inquiries are from loans or credit cards you applied for. Soft inquiries may be listed, which are from pre-approved credit card offers. These do not affect your score.

Next step: Block unauthorized access to your credit report with a credit freeze.

Placing a freeze on your credit report is the most effective method to stop identity thieves in their tracks. It's completely free with all three bureaus and will not affect your credit cards, credit report, or credit score. You can continue using your cards as you were before.

Freezing your credit report means only you can apply for new cards or loans. No one else will be able to do this in your name. It's like putting a lock on your credit report, and only you have the key. You can unlock (or unfreeze) your credit report at any time. For example, you may want to open a new credit card. You can temporarily lift the freeze to do so, then refreeze your credit report again after.

Federal legislation requires credit-reporting agencies to offer free credit freezes and unfreezes. To freeze your credit report with Experian, TransUnion, and Equifax, call them directly or do it on their websites. You may be asked to create a PIN code or they may generate one for you. Keep this code safe, because it's the one you'll use if you need to unlock your credit. A password manager is a great place to save your PIN codes.

About Firefox Monitor Frequently Asked Questions Terms & Privacy