# What To Do When Your Data Is Breached

You've been notified that your sensitive information has been stolen in a data breach. Don't give in to breach fatigue – there are important steps you should take now to make sure the damage is mitigated.

Because so much of our sensitive data is stored digitally, sometimes your information can be stolen even though you weren't personally targeted, and you maintain good cybersecurity behaviors. Healthcare organizations, businesses, and even governments leak data in what we call data breaches. Generally, these systems are protected by multiple layers of digital defenses, but sometimes a cascade of human error can leave the door open for bad actors.

In the short term, though, why it happened doesn't matter. When you find out your data might have been compromised in a breach, act fast to protect yourself.

## Keep Informed

As soon as you become aware of a data breach impacting a company, organization, or agency you engage with or are employed by, watch for their communications about what happened. New federal regulations require more companies to disclose data breaches. Read statements released by the impacted organization. Look up stories from high-repute news organizations and info from trusted cybersecurity outlets. This will help you understand the scope and nature of the data breach, including the type of data compromised and the potential risks associated with the exposed information. Between reports from the impacted organization and information from third-party groups like journalists and cybersecurity researchers, you can also get a sense of what actions to take.

## Change Your Password

The first step you should take is to change your password for the affected account. Follow our rules for a strong password — it should be at least 12 characters long and use a variety of characters, including upper case letters, lower case letters, numbers, and symbols (like ? and +). It is best if the password is a random string of characters, not a recognizable word or phrase. Use a password manager to generate super strong passwords and as a digital vault to securely store all your passwords. Very importantly, each account should be protected by its own unique password.

## Stop Reusing Passwords

Along with changing the password of the impacted account, if you reused that password for any other account, quickly change those passwords, too. This is why each account should have a special password, because if one platform is breached, the hackers don't obtain a skeleton key that can unlock all your other accounts. This is an opportunity to generate a unique password for everything you do online. Store them all in a trusted password manager.

## Enable Multi-factor Authentication

If the account with the breached platform permits the use of multi-factor authentication (MFA), turn it on. Wherever you can, you should enable multi-factor authentication, which is sometimes called two-factor authentication (2FA). 2FA adds an extra layer of security beyond your password. MFA will require another verification step, such as replying to a text message, a facial scan, or verifying your identity through a secure, standalone app on another device. This additional security measure can significantly reduce the risk of unauthorized access to your accounts, even if hackers are able to get ahold of your password.

## Keep an Eye On Your Financial Accounts

Especially after your personal information was exposed in a data breach, regularly monitor your finances, including checking your bank accounts, credit cards, and online payment platforms (like PayPal or Venmo). Be on the lookout for any suspicious activity, unauthorized transactions, or unfamiliar charges. If you notice anything unusual, contact the financial institution immediately and report the incident. Use credit cards whenever possible, because you won't be liable for fraudulent charges.

## Look Over Your Credit Reports

You can obtain your credit report for free online, and many banks will grant you access to your credit report. Regularly review these reports for any suspicious activities or accounts opened in your name without your consent. This step is very important if your Social Security number was lost in a breach. By checking your credit report, you can identify potential cases of identity theft. If you discover any discrepancies, promptly report them to the respective credit bureau and follow their instructions for resolution.

## Don't Take the Phishing Bait

Cybercriminals attempt to exploit big data breach situations by sending phishing emails, texts, or DMs designed to trick you into sharing additional sensitive data or clicking on malicious links. Exercise caution while perusing your inbox and verify the legitimacy of any communication before providing any sensitive information. Even a few seconds of skepticism can make a difference. Remember, legitimate organizations will not ask for sensitive information, like your login info or bank account number, through email or text messages.

## Consider Credit Monitoring

If the data breach involves very sensitive personal or financial information, like your Social Security number or credit card information, you probably should enroll in a credit monitoring service. These services alert you to any changes in your credit reports, providing an extra layer of protection and immediate notifications if any suspicious activity occurs. Oftentimes, the impacted organization will offer free credit monitoring to affected customers, but you will have to sign up for it. You might want to also consider freezing your credit, which limits access to your credit report. You can easily unfreeze your credit later if needed, like if you're applying for a new credit card or mortgage.

Having your information swept up in a data breach is undeniably aggravating. Some people think the loss of personal information online was unavoidable. While we can't stop cybercriminals from trying to hack us, we can do more to protect ourselves. All of us, individuals, technology providers, and our governments have actions we can adopt. We can work together to reduce their frequency and severity.

You can start by practicing good cybersecurity habits, like using a unique password for each account, and enabling MFA on all of your accounts, especially important financial services accounts, email, and social media accounts. If it's not offered, ask the provider when they plan to offer it or consider switching to a provider that offers MFA. That way, most of your digital realm will remain vigorously defended even if a random platform is breached.

---


The information provided in the MS-ISAC Monthly Cybersecurity Tips Newsletter is intended to increase the security awareness of an organization's end users and to help them behave in a more secure manner within their work environment. While some of the tips may relate to maintaining a home computer, the increased awareness is intended to help improve the organization's overall cyber security posture. This is especially critical if employees access their work network from their home computer. Organizations have permission and are encouraged to brand and redistribute this newsletter in whole for educational, non-commercial purposes.