

SecurityAwarenessNews

the security awareness newsletter for security aware people

Identity Theft and Data Breaches

The Compromised Account Cheat Sheet

Tax Season Identity Theft

How to Cause a Data Breach in 10 Easy Steps

The Compromised Account Cheat Sheet

One of the worst notifications to receive is the one that begins with, "We regret to inform you that we've suffered a data breach." Your personal data could now be in the hands of cybercriminals. What follows is a quick cheat sheet to help you navigate situations involving compromised accounts.



Change your passwords immediately. Data breaches serve as a great reminder of why it's so important to use unique passwords for every account. Duplicate passwords give attackers access to other accounts, making the security breach in question significantly worse.



Identify what kind of data was impacted. Most entities will inform customers of what type of data may have been compromised. This helps you identify where you're most vulnerable and what you need to do next.



Alert financial institutions. If the leak includes credit card or bank card data, alert your bank so they can update your card and account number. You may have to visit a local branch to get a temporary card until the new one arrives.



Notify credit reporting bureaus. One of the biggest concerns of a data breach is suffering identity theft, where criminals use your personal information to open accounts in your name. Contact credit bureaus, and consider placing a fraud alert or freeze on your credit reports to prevent this from happening.



Keep a close eye on your accounts. Routinely check bank accounts and credit card statements for unauthorized charges.



Take advantage of credit monitoring services. Most breached organizations will offer free credit monitoring services to impacted customers. Take advantage of it, and stay alert for any unusual activity on your credit reports.



Dealing with Data Breaches at Work

Here at work, take every precaution to ensure that our customers, clients, business associates, and fellow employees never have to use the above cheat sheet. Stay alert. Think before you click. And always follow policy.

Tax Season Identity Theft

The threat of identity theft exists all year long, but increases during tax season when scammers ramp up attacks. If successful, criminals can open accounts and file fraudulent tax returns in your name, putting you on a long, difficult path to recovery.

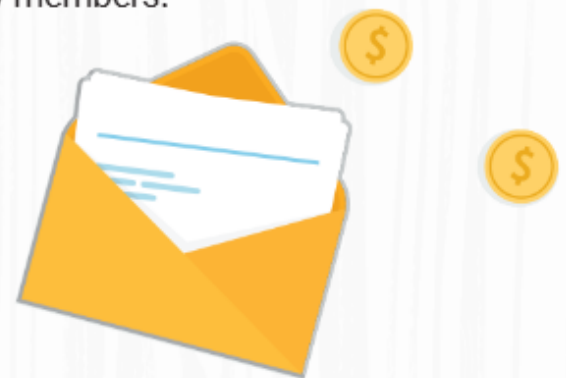


Avoiding ID theft begins by ensuring that your personal information remains private.

That means sharing less on social media and maximizing the security settings of social media accounts, staying alert for phishing attacks that attempt to bait you into clicking on malicious links, and using common sense (you know, like not broadcasting your national ID number on social media).

During tax season, remember that tax collectors won't call you, email you, or text you to ask for a credit card payment for overdue taxes. Scammers will do anything they can to convince their targets to reveal confidential information, including posing as government entities, co-workers, friends, and family members.

If possible, file your taxes early to get a jump on any criminals that might have obtained your personal information. To avoid ID theft all year long, consider placing a freeze on your credit reports, which will prevent anyone from opening accounts in your name.



Here at work, help protect the identities of our clients, customers, and business associates by following our organization's policies and considering the ramifications of what might happen if personally identifiable information ends up in the wrong hands.





How to Cause a Data Breach in 10 Easy Steps!

STEP 1: Make sure to click on every link, and download every attachment sent to you via email. On mobile, feel free to trust links sent to you in random text messages.

STEP 2: Disable antivirus and other security apps on every device, especially your work computer.

STEP 3: Ignore security policies. They're more like suggestions than hard guidelines anyway.

STEP 4: Plug in that random USB flash drive you found. It could have some good information on it!

STEP 5: Feel free to download sensitive information to a personal device without encryption.

STEP 6: Don't bother using a virtual private network when accessing public WiFi.

STEP 7: Trust anyone and everyone who calls you on the phone and asks for confidential information.

STEP 8: Install whatever apps you want without regard for who developed them.

STEP 9: Share your privileged access with whomever asks for it, and never lock your workstation.

STEP 10: Post a bunch of personally identifiable information on social media.

BONUS STEP: Use the same passwords for every account.

As you can see, causing a data breach takes little effort. Obviously, we want you to do the opposite of the above steps. Your dedication to maintaining data privacy is what makes you a valuable member of our organization. If you need more information about your role in preventing data breaches, please ask! And remember to report all security incidents immediately.