Workforce Security and Risk Training

Data Breach Notification? Don’t Panic — Take control

One Email Changed Everything

Justin had just finished dinner when he noticed an email from the car repair shop he recently visited to fix his car’s engine. The subject line of the email read:

“Important Security Notice About Your Account”

At first, he almost deleted it, assuming it was another scam. But curiosity got the better of him. The email explained that the company had suffered a data breach and that their customer information, including names, email addresses, home addresses, and phone numbers were exposed. The good news was that no credit card information had been compromised. Life was busy, and he decided it was not that big of a deal.

A few days passed. Then Justin started getting strange emails from the car repair company about numerous overdue bills requiring payment. The emails threatened he could go to jail if he did not pay them immediately. The emails looked legitimate, as they not only had the company logo, but they knew his name, phone number and home address. In a panic, Justin clicked on the link and paid the bill. It was several weeks later, while talking to a friend, that he realized the email and the bill were not legitimate — they were phishing emails that cyber criminals had created, using the information they had stolen from the hacked car repair company. By using Justin’s stolen information, the cyber criminals were able to create a more realistic attack. Unfortunately, Justin’s story is becoming increasingly common.

What is a Data Breach?

A data breach is a specific term for when personal data held by an organization has been either stolen by cyber attackers or accidentally exposed. In some cases, these organizations are required by law to notify any customers or partners whose data may have been lost or stolen as part of that data breach. The question becomes, what should you do if you are notified?

What Should You Do After a Data Breach?

The good news is that a breach does not automatically mean you will become a victim. What matters most is how you respond.

© SANS Institute 2026

1. **Change your password immediately**. If you have an online account at the impacted organization, change your password. More importantly, if you reused that same password for any other accounts, change those passwords too. Each of your accounts should have its own unique password. That way, if one account is breached, the stolen password cannot be used to access your other accounts. Cyber criminals know people often reuse passwords, and they will try stolen passwords against your other accounts. The easiest way to manage all of your unique passwords is with a password manager, which can create, store, and fill in strong passwords for you.
2. **Turn on multi-factor authentication**. Multi-factor authentication, often called MFA, adds an extra layer of protection for your accounts beyond just your password. Even if a cyber criminal steals your password, MFA can help stop them from logging in.
3. **Watch for follow-up scams**. After a data breach, criminals may send fake emails, texts, or phone calls pretending to be the affected company, your bank, or a support team. Using your stolen information, they can create far more realistic emails and text messages. Just because someone knows personal information about you, such as where you live, who you work for, or what type of car you drive does not mean they are legitimate. Do not click links or call numbers from these messages. Instead, go directly to the organization's official website or mobile app to confirm if these issues are real.
4. **Monitor your financial accounts**. Monitor your financial and credit card accounts for suspicious activity, such as unexpected purchases, cash withdrawals, password reset notices, or changes to your profile. Many banks and online services allow you to enable text or email alerts for any new transactions or account changes. These alerts can help you spot trouble quickly.

In some cases, organizations that have experienced a data breach will also offer you some type of identity fraud protection through a third-party service. While these services do little to protect your data, they can help you monitor your financial accounts, set up credit monitoring, and often provide insurance or other protections if you are a victim of identity theft as a result of the breach. Verify the authenticity of the identity monitoring firm, as you'll be giving them personal information in order to set up your account.

Unfortunately, there is little you can do to protect your data that other organizations collect, as in most cases you have no control over it. But by taking these simple steps, you can go a long way to ensuring you are much more secure when a data breach does happen.

Guest Editor

Brandi Narvaez is a Senior Cybersecurity Consultant with over 25 years of experience delivering information security and infrastructure projects. She specializes in protecting organizational users and assets, securing sensitive data, and aligning cybersecurity strategies with business objectives to enhance cyber resilience and align operational effectiveness.

Resources

How Cybercriminals Exploit Your Emotions: https://www.sans.org/newsletters/ouch/cybercriminals-exploit-your-emotions
The Power of the Passphrase: https://www.sans.org/newsletters/ouch/power-passphrase-why-longer-beats-smarter
Stop Password Pain: Use a Password Manager: https://www.sans.org/newsletters/ouch/stop-password-pain-reliable-password-manager
Protecting Yourself When True Privacy is Impossible: https://www.sans.org/newsletters/ouch/protecting-yourself-when-true-privacy-is-impossible

OUCH! Is published by SANS Security Awareness and distributed under the Creative Commons BY-NC-ND 4.0 license. You are free to share or distribute this newsletter as long as you do not sell or modify it. Editorial Board: Phil Hoffman, Leslie Ridout, Princess Young.

You can find more Ouch! On the following link: https://www.sans.org/newsletters/ouch