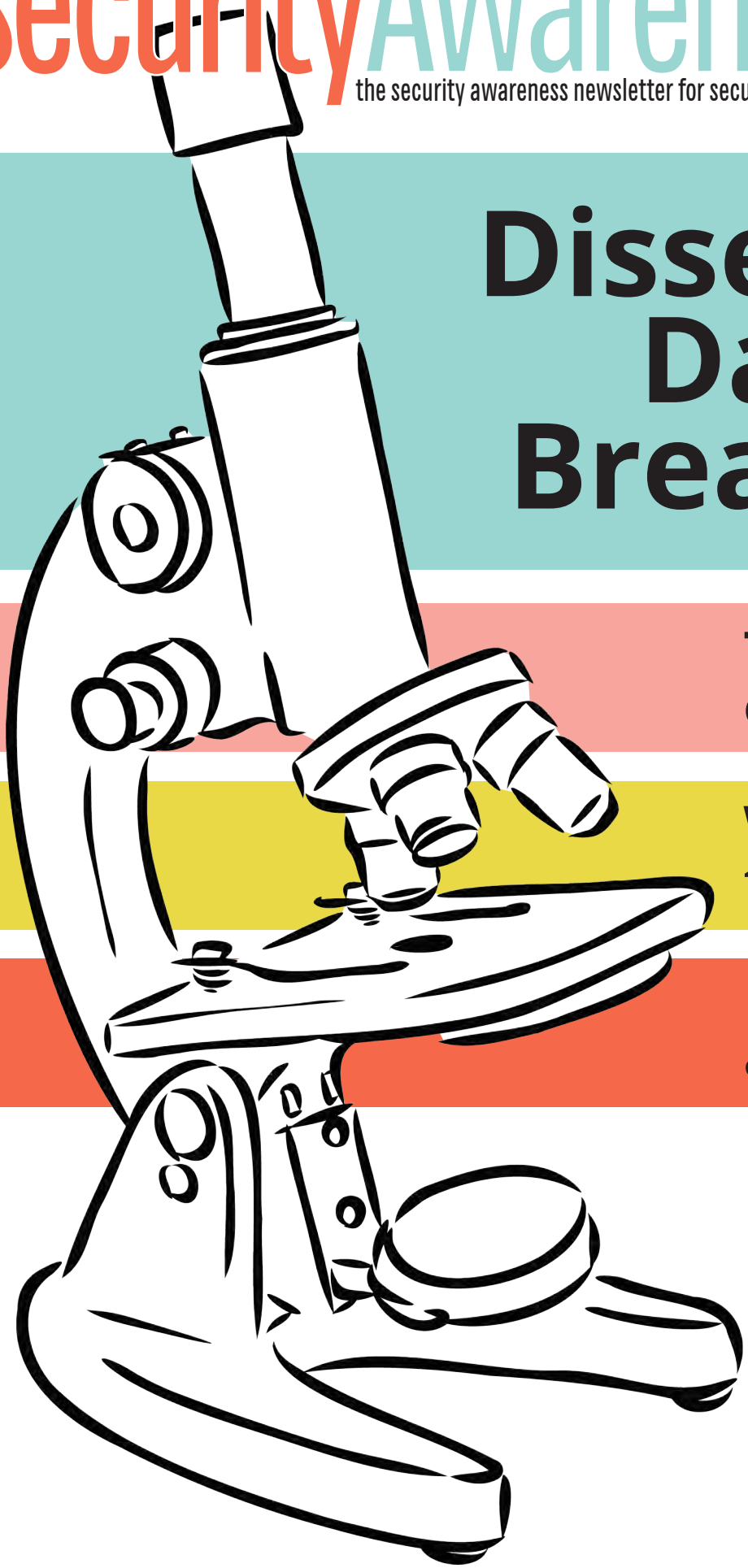
May 2022

Security Awareness News

the security awareness newsletter for security aware people



Dissecting Data Breaches

The Main Cause of Data Breaches

What Happens to Stolen Data?

Data Breaches and You

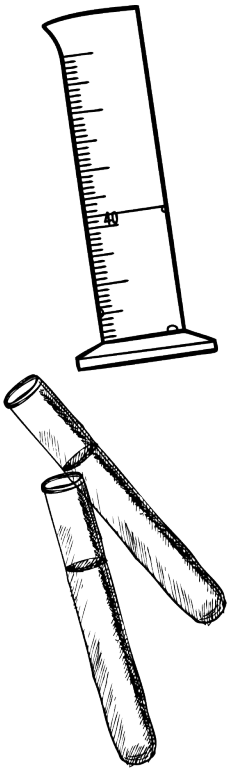
THE MAIN CAUSE OF DATA BREACHES

A typical data breach fits this description:
any event that allows unauthorized access to confidential information.

EXAMPLE ONE: a criminal hacker uses a phishing attack to steal customer credit card numbers.

EXAMPLE TWO: an employee sends confidential information to the wrong person.

While both examples transpired for different reasons, they have one thing in common: human error. Obviously, the second example involved someone making a crucial mistake. The first example involved malicious intentions, but someone still made the mistake of falling for a phishing scam, likely by clicking on a malicious link.



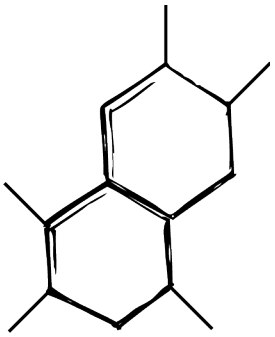
Of course, not every data breach features phishing attacks or accidental leaks of information. Some breaches are made possible when cybercriminals find vulnerabilities in unpatched software. Others involve attackers probing networks for security misconfigurations that leave digital backdoors open.

Once again, a human error—failure to update software, improperly configured security settings—is what made the breach possible.

In other words, most data breaches are caused not by savvy criminal hackers with advanced skills but by simple mistakes made by regular people. The purpose of highlighting that unfortunate reality isn't to cast blame. Instead, the goal is to raise awareness and remind you of one of the most vital security concepts: you are the last line of defense.

Your decisions and the actions you take ultimately determine the strength of our organization's security culture. That's why you might often encounter messages that remind you to always follow policy and think before you click. Those two simple actions require no technical skills and could be the difference between maintaining security and suffering a breach.

At the end of the day, we're all subject to data collection, and we all hope the people handling our data go out of their way to maintain our privacy. Keep that in mind when you're the one handling someone else's private information.

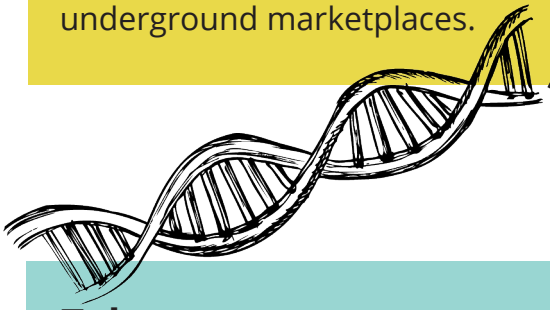


What Happens to Stolen Data?

Major data breaches often result in the personal information of thousands of people ending up in the hands of cybercriminals. What do the attackers do with all that data?

Sell it to other criminals

Information has monetary value. Full names, national identification numbers, home addresses, and so on all fetch a price on underground marketplaces.



Use it to launch phishing attacks

When a criminal knows your full name, where you work, your job title, or the names of your co-workers, they can personalize phishing messages to make them seem legitimate. This tactic adds a layer of trust, causing the victim to lower their guard, which increases their likelihood of clicking a malicious link or wiring money.

Take over accounts

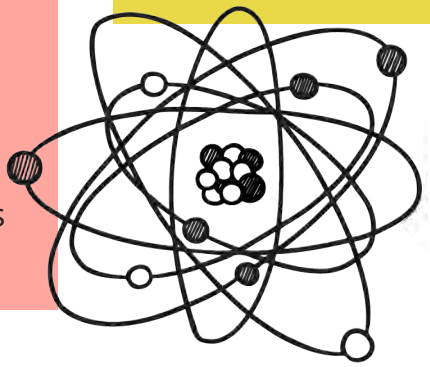
When login credentials get stolen, it allows attackers to completely take over accounts. Imagine if a malicious person gained control of a CEO's Twitter profile. They could irreparably harm the organization's reputation with a few offensive tweets, or even leverage the account to impact stock market prices.

Steal identities

Identity theft happens when a scammer uses stolen personal information to open fraudulent accounts, insurance claims, and credit applications. This crime is one of the most common side effects of personal data leaks. Also, it has one of the most difficult impacts on individuals.

Extortion

Cybercriminals will threaten to leak stolen data unless the organization pays a ransom. This is a common technique that accompanies ransomware (malicious software that encrypts data or locks up systems); extortion pressures organizations to pay the fee.



Data Breaches and You

Data collection is a part of life, but data breaches don't have to be. Let's review a few common threats to data and how to avoid them.

Threat: Phishing

Scammers send emails with malicious links or attachments, along with a convincing message designed to trick someone into clicking the link or downloading the attachment.

Prevention: Awareness

Learn to spot common warning signs such as a sense of urgency, threatening language, and poor grammar. Always hover over links to reveal the full URL.

Threat: Weak Passwords

Cybercriminals often use software that can guess inferior passwords in minutes, or even in seconds. If successful, they can take over accounts and gain unauthorized access to data.

Prevention: Password Hygiene

Ensure every account has a strong, unique password. Where available, implement MFA (multi-factor authentication), which requires a second code or PIN to be entered before access is granted.

Threat: Dumpster Diving

It's hard to imagine anyone blessing themselves with a trip to the dumpsters, but scammers have little dignity. They know that trash and recycle bins sometimes contain sensitive documents.

Prevention: Proper Disposal

If you need physical copies of confidential information, be sure to store them securely and shred them when no longer needed.

Threat: Social Media

People tend to overshare, especially on social media. Attackers leverage common sites to search for any information that might help them launch successful phishing campaigns.

Prevention: Privacy

Set your social media profiles to private and vet anyone who wants to connect with you. Never share information that could be used against you or our organization.

Remember to always follow policy and report security incidents immediately.
Need more information? Please ask!