SecurityAwarenessNews

the security awareness newsletter for security aware people

Data Breach Basics

The Primary Cause of Data Breaches

Defending Data

Preventing Identity Theft

The Primary Cause of Data Breaches

Data breaches — incidents where confidential information is stolen, leaked, or disclosed — are a major concern for organizations around the world. These security incidents frequently make headlines, potentially impacting millions of people and causing significant damage to reputations.

How do they happen? Consider the following two scenarios:

One:

A scammer emails someone and tricks them into revealing confidential information.

Two:

An employee accidentally sends confidential information to the wrong person.

While both examples transpired for different reasons, they have one thing in common: human error. 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 scam.

Those scenarios are, of course, not the only way data gets stolen or leaked. Some breaches are made possible when cybercriminals find vulnerabilities in outdated software or firmware. Others involve attackers probing networks for security misconfigurations that leave digital backdoors open.

Once again, mistakes — failure to install updates and improperly configured security settings — are what made the breach possible.

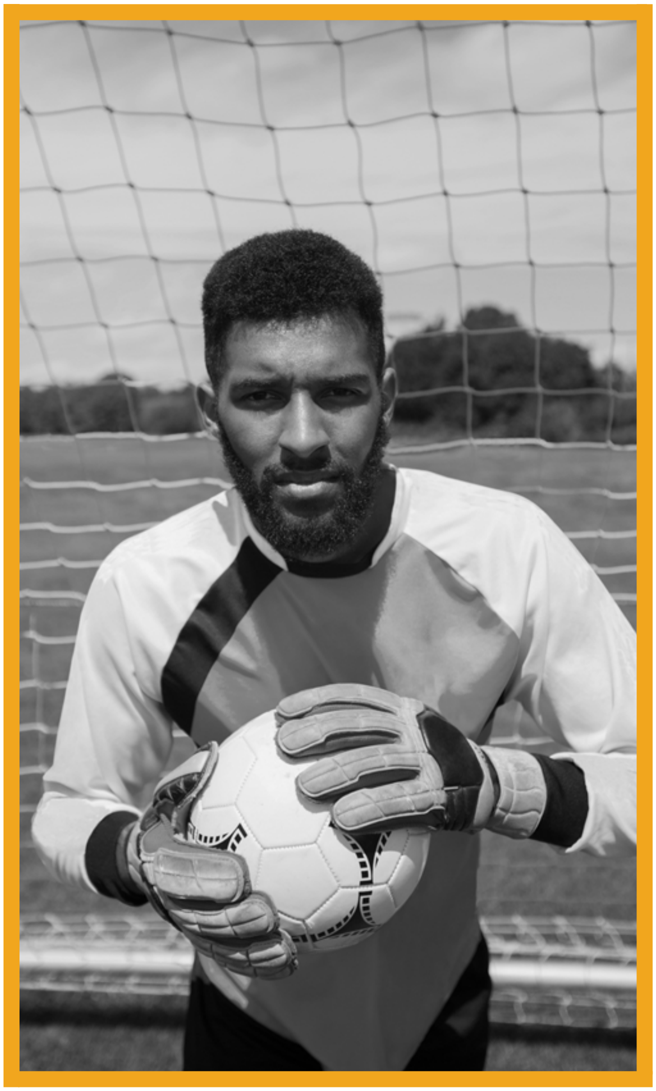
In other words, not every breach is caused by savvy criminal hackers with advanced skills. Many involve simple mistakes made by regular people. The purpose of highlighting that unfortunate reality isn't to cast blame. Instead, the goal is to raise awareness and remind you of one of the most vital security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

Your decisions and the actions you take ultimately determine the strength of your 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 confidential information.

Defending Data

Safeguarding information is a key part of maintaining security and privacy. Let's review a few ways to ensure the data you have access to remains protected.



Stay alert for phishing scams.

Phishing scams attempt to lure people into doing something they shouldn't, such as opening a malicious link or attachment. They are one of the top causes of data breaches and other security incidents. You can identify phishing scams by staying alert for warning signs such as threatening or urgent language and unexpected links or attachments.

Maintain good password hygiene.

Passwords are a fundamental part of protecting information. A strong password is long, hard to guess, and never used for more than one account. Additionally, always ensure your passwords adhere to organizational policy.

Prioritize physical security.

Here are a few examples of simple actions that help maintain physical security:

- Immediately locking devices and workstations when not in use
- Properly disposing of documents that contain confidential information
- Securely storing laptops and smart devices where they won't get stolen

Share with care.

Obviously, you should never post confidential information on social media. It's also wise to limit what you share in general. Scammers search social media and other public forums to gather intelligence and use it against their targets. Consider setting your profiles to fully private and only connect with people you trust.

Take it personally.

Data privacy impacts everyone. Think about what would happen if your confidential information were mistreated. Use that mindset whenever you handle sensitive data here at work.

Always follow policy.

Policies are designed to protect the privacy of employees, clients, and business associates. Ignoring policies for any reason puts everyone at risk and undermines security efforts.

Preventing Identity Theft

Imagine receiving an invoice for a service you didn't subscribe to or discovering inquiries on your credit report that you didn't authorize. Both scenarios could indicate that someone has used your personal information to commit a fraud, known as identity theft.

Here are just a few examples of what someone could do if they managed to steal your identity.

- Apply for a loan by using your credit score
- Open credit cards in your name
- Take over your online accounts

These scenarios are common worldwide and highlight a key point about this kind of cybercrime: It's personal and can have lasting effects. That's why it's important to understand the impacts of data breaches.

Full names, home addresses, national identification numbers and other forms of data, when combined, give criminals what they need to commit fraud. Ensuring that information is never leaked or stolen helps protect the well-being of real people.

You can do your part by staying alert for scams and using extreme caution when handling confidential information. Attackers sometimes attempt to impersonate people you know, like a manager or co-worker. So, never assume someone is who they claim to be and report anything suspicious immediately.

Other Types of Identity Theft

Synthetic Identity Theft

A synthetic identity is completely or partially fabricated. Commonly, a legitimate national identification number is used in combination with a fake name, address, phone number, and birthdate to create a fake person.

Child Identity Theft

This scam targets children by using their information to open a new account or line of credit. What makes child identity theft especially unfortunate is that it is often carried out by a family member, and most victims don't realize they've been scammed until they're much older.

Business Identity Theft

Also known as corporate or commercial identity theft, this scam occurs when someone poses as an owner, executive, or employee of an organization. The goal is to leverage that organization's credit or reputation for financial gain.