SecurityAwarenessNews

the security awareness newsletter for security aware people

Identity Theft Foundations

What Everyone Should Know About ID Theft

How Identities Get Stolen

Top Data Protection Strategies

What Everyone Should Know About ID Theft

Identity theft is one of the most common scams worldwide that impacts millions of people every year. It occurs when a cybercriminal gains unauthorized access to someone's personal information and uses it for fraudulent purposes. Here's what everyone should know about this dangerous form of cybercrime:

It can lead to years of burden for victims.

With enough stolen data (such as national ID numbers, full names, home addresses, and more), scammers can commit a wide variety of fraud using the victim's identity. As examples, they could open accounts in the victim's name, file fake tax returns, and commit crimes under the victim's identity.

There are many different types of identity theft.

Here are a few examples:

- **Medical:** The attacker seeks medical care under the stolen identity of another person
- **Business:** The attacker poses as an owner or executive to leverage their organization's credit for financial gain
- **Child:** The attacker uses a minor's information to open a new account or line of credit
- **Synthetic:** The attacker creates a fake person using someone's legitimate national ID number

It's often made possible by data breaches.

A data breach is any scenario where highly confidential information gets leaked or stolen from an organization or other entity. Some of the biggest breaches in history have resulted in millions of people having their personal data leaked online and made available to cybercriminals.

The frequency of this crime has dramatically increased.

Identity theft is more prevalent than ever before due to the widespread collection of personal data. Additionally, modern services like E-commerce websites and mobile payment apps have provided criminal hackers with an abundance of options to steal data. This has led to a significant increase in fraud and theft.

You can help prevent it.

Personal data carries a lot of power and needs to be protected. You can help keep this data safe by always following policies, treating requests for information with skepticism, and staying alert for anything suspicious. These simple actions help protect the integrity of your organization and the privacy of individuals.

How Identities Get Stolen

Most identity theft scams are powered by a common source: stolen or leaked personal data. One of the best ways to learn how to avoid those scams is by gaining an understanding of how criminals gain access to that data in the first place. Let's review four of the most common ways that this happens.

Social Engineering

Social engineering is the use of deception to trick people into making a bad decision, often through emotional manipulation. For example, a social engineer will impersonate a bank representative and ask the target to confirm their account details over the phone.

Did you know? Almost every scam you might encounter, at work or at home, involves some form of social engineering.

Malware

Malware stands for malicious software, which refers to any sort of code or program that alters the functionality of devices. It's commonly used to steal data and transmit it back to the attacker. Some versions of malware can hide themselves and go undetected for months or even years.

Did you know? Mobile devices, such as smartphones and tablets, are just as vulnerable to infections as traditional computers.

Phishing

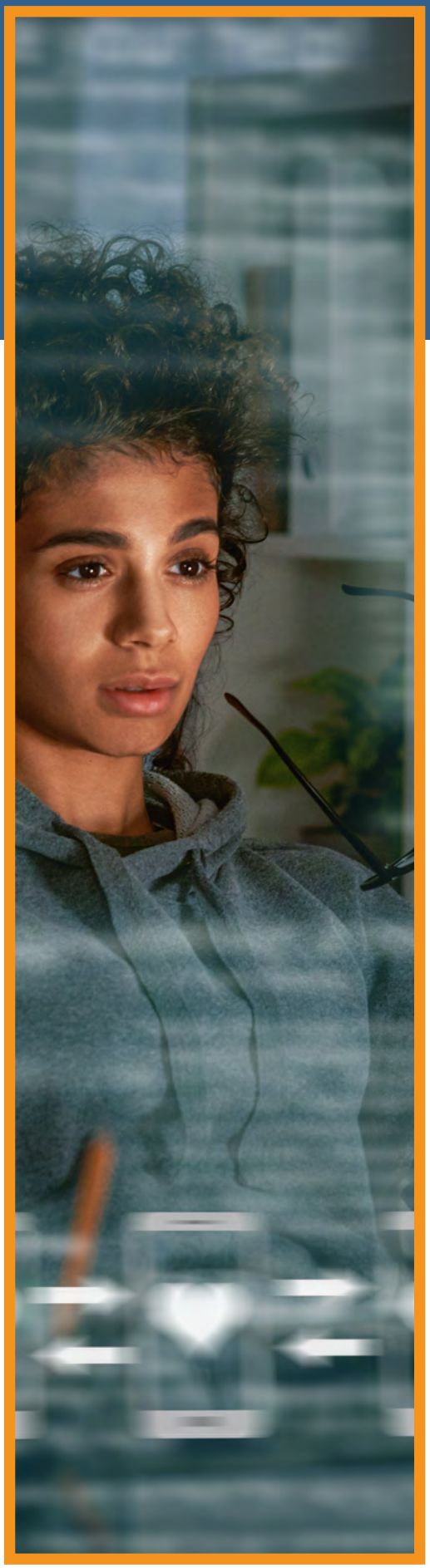
The top tool in the social engineering playbook, phishing attempts to lure you into making a bad decision. Many come via email and feature malicious links that can spread malware or direct you to a website that asks you to confirm personal details.

Did you know? While phishing is commonly associated with email, attackers also use text messages and phone calls to phish people.

Data Breaches

Many data breaches result in endless amounts of personal information finding a home on the dark web — a subset of the World Wide Web known for illegal activities. It's where cybercriminals can buy stolen data and use it to steal identities or commit other types of fraud.

Did you know? A lot of data breaches are caused by human error, such as someone clicking on a malicious link or failing to update software.



Top Data Protection Strategies

As identity theft scams continue to rise, it's important for everyone to refresh their knowledge of how to protect data, both at work and at home. Use the following strategies to keep data and people safe.

Learn the warning signs of scams

While the intentions of scammers might vary, many attacks feature warning signs that should raise your suspicions. Common examples include:

- Threatening language
- Urgent requests
- Unrealistic promises
- Random links or attachments

Keep personal info personal

Limit what you share on public forums like social media. Scammers often search those forums for any information that might help them build a profile on their targets. The more detailed profile they can build, the easier it is for them to scam someone.

Prioritize password security

Your online accounts, personal and professional, are home to vast amounts of data, most of it confidential. The main thing keeping attackers out of those accounts is your password. Therefore, it's vital to ensure every password is long, strong, and unique to each account.

Avoid making assumptions

Psychological manipulation is a powerful ingredient present in social engineering attacks. These scammers will create stories or scenarios designed to gain your trust, often by impersonating someone you might know. Don't fall for it. Never assume someone is who they claim to be.

Think before you click

Phishing attacks are the top way devices get infected with data-stealing malware. Carefully scrutinize messages before taking any action, such as clicking on a link or opening an attachment. If you're unsure a message is trustworthy, don't click on anything and don't respond.

Remember, identity theft can happen to anyone. So stay alert, always follow organizational policies, and report anything suspicious immediately.