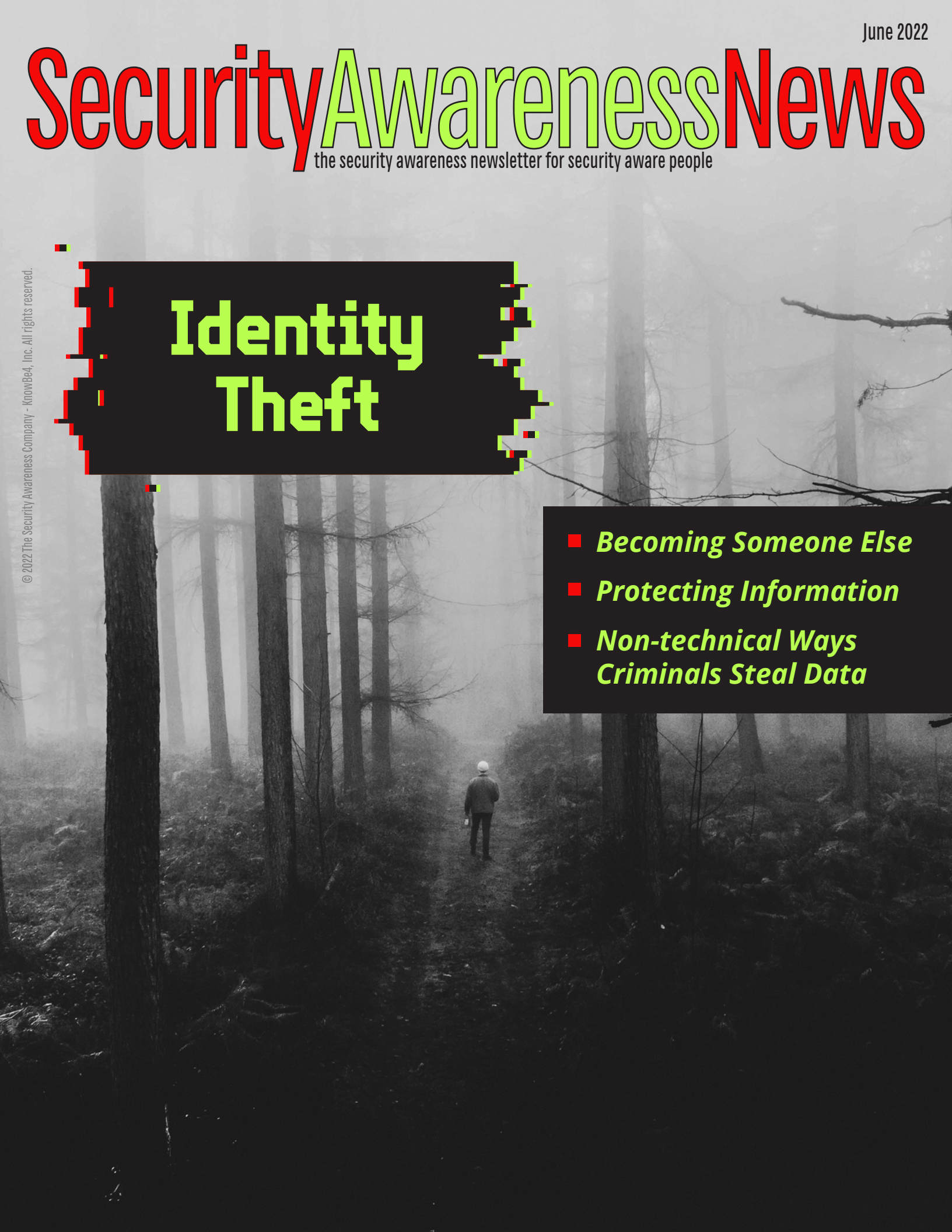
June 2022

SecurityAwarenessNews

the security awareness newsletter for security aware people



Identity Theft

- *Becoming Someone Else*
- *Protecting Information*
- *Non-technical Ways Criminals Steal Data*

▶▶▶ Becoming Someone Else

Have you ever wanted to be someone else for a day or two? Cybercriminals have. In fact, they're actively searching for ways to become someone else all the time via a scam called identity theft.

Identity theft typically involves the use of stolen or leaked personal information to commit fraud. The most common type is financial identity theft, where the thief opens new credit card accounts or applies for bank loans in the victim's name. Let's walk through a few other examples.

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.

Medical Identity Theft

- If an identity thief seeks medical care under the stolen identity of another person, the thief's medical history may be added to the victim's medical records. This information is difficult to correct and may affect future insurability.

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.

In all cases, identity theft is costly, emotionally distressful, and often requires a long recovery period for victims. Don't let it happen to you or anyone associated with our organization! Take extra precautions when handling confidential information to ensure it never ends up in the wrong hands.

Protecting Information

Identity theft is made possible when personal information ends up in the wrong hands. When combined, full names, home addresses, phone numbers, national identification numbers, and other forms of data give criminals what they need to commit fraud.

As such, protecting that information is paramount to ensuring identities remain secure—a responsibility we all share. Here's how you can help prevent identity theft:

Did you know?

Depending on your country of residence, you might have an option to freeze your credit. This prevents anyone from running credit checks for any reason. You can unfreeze it whenever necessary. Parents and guardians can also take advantage of this by freezing their children's credit to prevent child identity theft.

Always follow policy

Policies are designed with the intent to ensure confidential information remains confidential. Circumventing them for any reason undermines those intentions and could lead to data leaks.

Remain skeptical

Treat requests for sensitive data with a high degree of skepticism. Avoid assuming someone is who they claim to be and take extreme caution whenever you access or transfer personal information.

Stay alert for phishing attacks

Carefully scrutinize emails and learn to spot warning signs such as poor spelling, threatening language, a sense of urgency, and suspicious links or attachments. Think before you click!

Avoid removable media

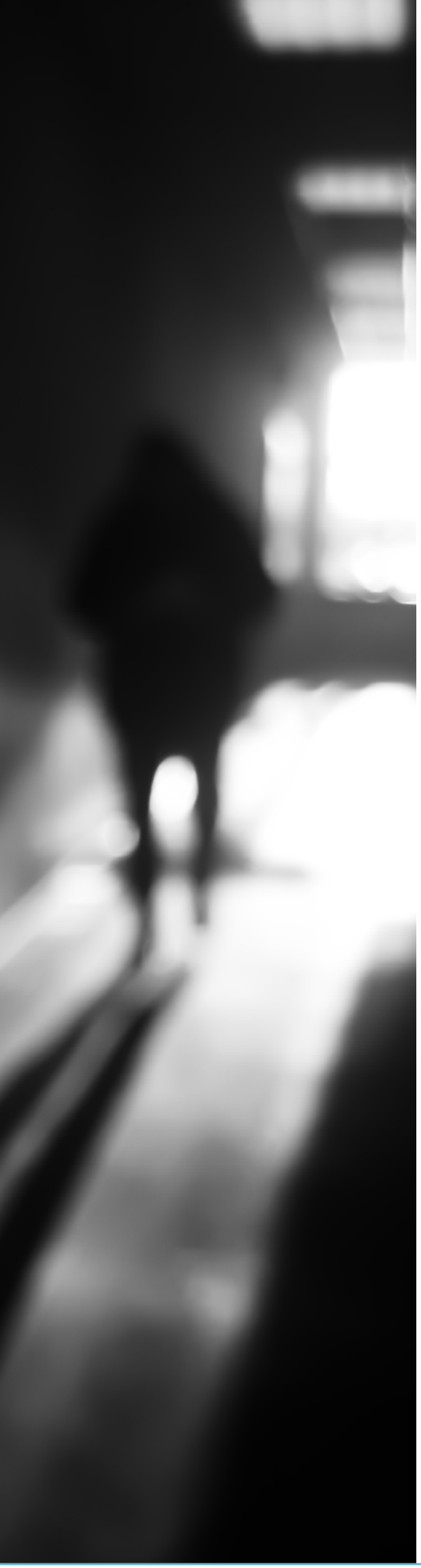
Not only are USB flash drives easy to lose, they are often used by cybercriminals to spread data-stealing malware. Never plug in a USB device that doesn't belong to you.

Utilize strong passwords

Protect every account with a strong, unique password. Consider implementing multi-factor authentication (MFA), a security feature that requires a second code before access is granted.

Report suspicious activity

While protecting information requires a proactive approach, we still need to be reactive when something seems off. Report all security incidents or suspicious situations immediately.



Non-technical Ways Criminals Steal Data

While many instances of data leaks involve some form of criminal hacking, that's not the only way data gets stolen. In a lot of cases, it's humans who get hacked, not computers. Let's explore the non-technical side of data theft.

Shoulder Surfing

Sometimes the easiest way to steal information is by simply looking over someone's shoulder as they browse on their laptop. You might be surprised what you can learn about someone by using this technique—a good reminder to use discretion when in public.

Piggybacking

There are several reasons why organizations require badges or keycards to enter certain areas. One of those reasons is to prevent unauthorized access that could allow an outsider to steal information. That's why it's important to follow the "one badge; one entry" philosophy and never hold a door open for someone who doesn't have clearance.

Tailgating

You've probably encountered tailgating in various works of fiction, which typically involves a character sneaking through a door behind someone who has legitimate access. You can easily prevent this by ensuring doors to secured areas stay closed and locked.

Dumpster Diving

We already mentioned that sensitive documents should be shredded when no longer needed. Be sure to take that advice home to protect sensitive information that, for example, exists in banking statements. Additionally, whenever you sell or recycle devices like smartphones, remember to restore to the factory defaults to erase all personal details.

Social Media Stalking

Scammers are always searching for pieces of the data puzzle. Social media often offers lots of opportunities to find those pieces. This is because many people tend to share too much and fail to set accounts to private. In the process, they give scammers a chance to stalk social media profiles and gather information.

Pretexting

A pretext is a made-up scenario designed to trick someone into divulging confidential information. A common example is a text message, phone call, or email that claims an account has been compromised and you need to confirm your login credentials immediately to avoid deactivation.