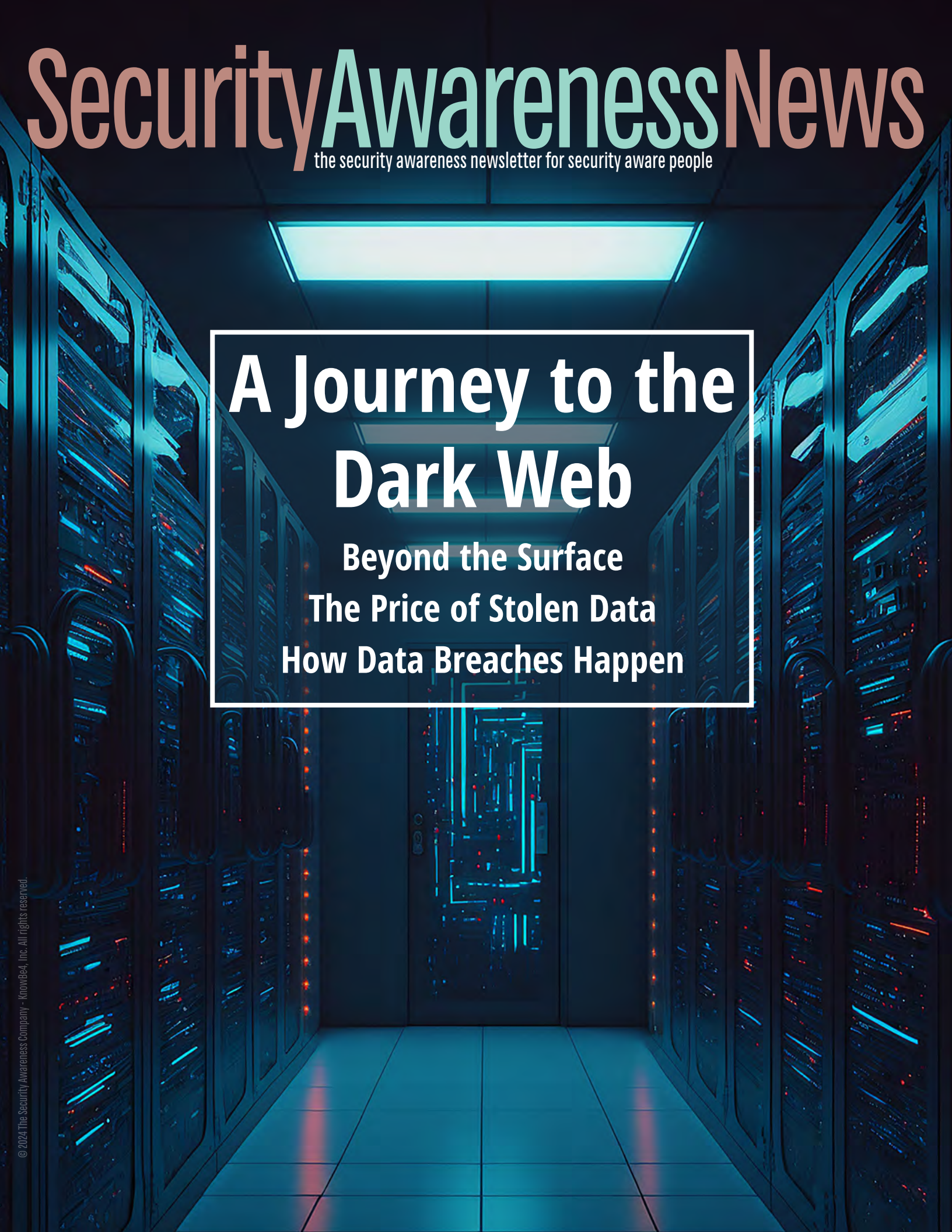
SecurityAwarenessNews

the security awareness newsletter for security aware people

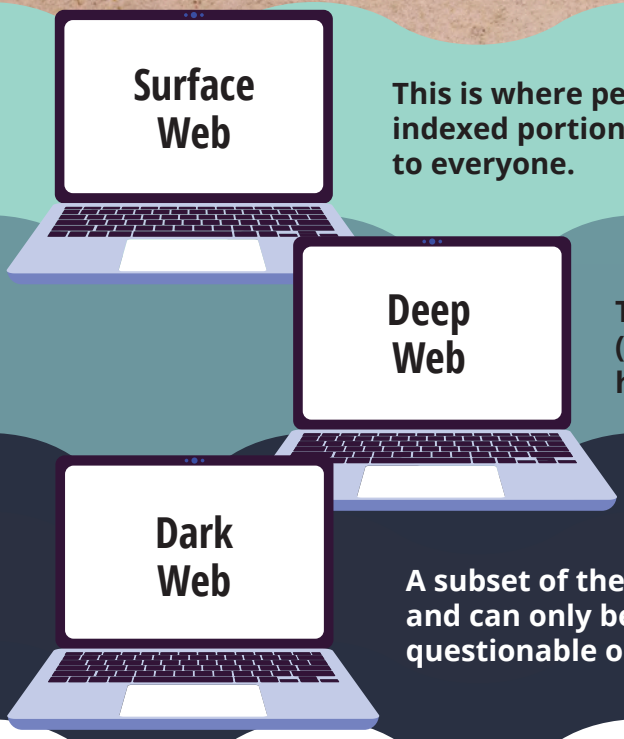


A Journey to the Dark Web

Beyond the Surface
The Price of Stolen Data
How Data Breaches Happen

Beyond the Surface

Have you ever wondered how many websites there are? While it's difficult to measure the exact number, researchers estimate over a billion. But those sites represent only a small fraction of the World Wide Web, which is made up of three parts:



This is where people spend most of their time when using the internet. It's the indexed portion, meaning it appears in search engine results and is accessible to everyone.

The deep web represents the largest percentage of the internet (roughly 90%). It hosts a vast amount of information that is hidden from the public for privacy and security reasons.

A subset of the deep web, this layer of the internet is intentionally hidden and can only be accessed by specialized web browsers. It's where a variety of questionable or illegal activities sometimes occur.

You've spent most of your time browsing the surface web, and some of your time on the deep web (such as when you log into a bank account). But most people never enter the dark web. For good reason.

As you might know, the dark web is notorious for criminal activity. If you've ever wondered what happens to leaked or stolen data, it often ends up here where people can buy or sell it, along with various other illegal items and services.

Unlike typical websites, those on the dark web usually require you to know a specific address to find them. This process allows criminals to achieve their objectives and quickly vanish as needed.

Note, however, that the dark web itself is not illegal and does offer legitimate benefits. For example, it can provide a safe refuge for journalists who are at risk of political retaliation or censorship. In fact, the dark web provides the most privacy of the three because it is built for the purpose of anonymity. Unfortunately, that purpose also creates a shelter for criminals, which explains the dark web's questionable reputation.

What does all of this mean for security? Simple: When you handle confidential data, it's your job to ensure it won't end up on the dark web — or any layer of the web where it doesn't belong. The internet is a big place. So stay alert for scams, use situational awareness, and always follow organizational policy.

The Price of Stolen Data

One of the key goals of security is preventing data breaches, which occur when confidential information gets leaked or stolen. That information often ends up for sale on the dark web, where cybercriminals operate underground marketplaces. Here are a few examples of the value of stolen information compared to common items:

Credit card numbers = a meal for two at a chain restaurant

Online banking login credentials = a plush bathrobe

Hacked email account = a monthly cable subscription

Hacked social media account = a pair of movie tickets

Of course, like any marketplace, the cost of items vary by supply and demand. There is, however, one cost that stays the same: the price of privacy. Data breaches often result in making someone's private information public — a costly scenario that can lead to one or all of the following consequences:

Personalized Phishing Attacks

When an attacker gains access to enough personal information, they will use it to create personalized phishing messages. This tactic adds a layer of trust, causing the target to lower their guard, increasing the likelihood of falling for the attack.

Identity Theft

Identity theft is one of the most common and harmful side effects of data breaches. It happens when a scammer uses stolen personal information to open fraudulent accounts, file insurance claims, and apply for credit applications in the victim's name.

Account Takeover

Stolen usernames and passwords allow attackers to completely take over online accounts. While this often leads to financial losses for the victim, imagine if a malicious person gained control of someone's social media profile. They could irreparably harm their reputation with a few offensive posts.

All three of those scenarios highlight the hefty price tag of stolen data and how important it is to prevent breaches. You can do your part by prioritizing security awareness at work, home, and everywhere in between.

How Data Breaches Happen

One of the best ways to prevent data breaches is by gaining an understanding of how they happen in the first place. Let's explore five common reasons breaches occur and how you can avoid them.

Social Engineering Attacks

Social engineers use manipulation to mislead people into doing something they shouldn't. For example, they might impersonate someone from the IT department and ask an employee to confirm their username and password.

- **Avoid it: Stay alert for common warning signs of scams, such as threatening language and urgent requests, and never assume someone is who they claim to be.**

Malware Infections

Malware refers to malicious code or software that can steal data and spy on people. It can also lock up systems or data until the victim agrees to pay a specified ransom. This is known as ransomware.

- **Avoid it: Use extreme caution before opening links or attachments. Never plug in random USB devices, such as flash drives and charging cables, which cybercriminals use to spread malware.**

Outdated Software

There's a reason why developers regularly issue software and firmware updates. Sometimes, it's to improve functionality or fix something. Updates are also a vital part of patching security vulnerabilities.

- **Avoid it: Always keep your personal devices and apps up to date. At work, follow policies for when to run updates and never install any software without approval from your organization.**

Weak Passwords

Nothing makes a cybercriminal's job easier than when people use weak, easy-to-crack passwords for online accounts.

- **Avoid it: Ensure every account and device gets a long, unique password. Consider using a passphrase — a combination of words that are easy for you to remember but hard for others to guess.**

Human Error

Here's an unfortunate fact: Human error is one of the leading causes of breaches. From circumventing policy to opening malicious links or attachments, mistakes add up and can be quite costly.

- **Avoid it: Many mistakes occur because someone is rushing through a task or not paying attention. By simply slowing down and using situational awareness, you can avoid accidentally causing security incidents.**