SecurityAwarenessNews

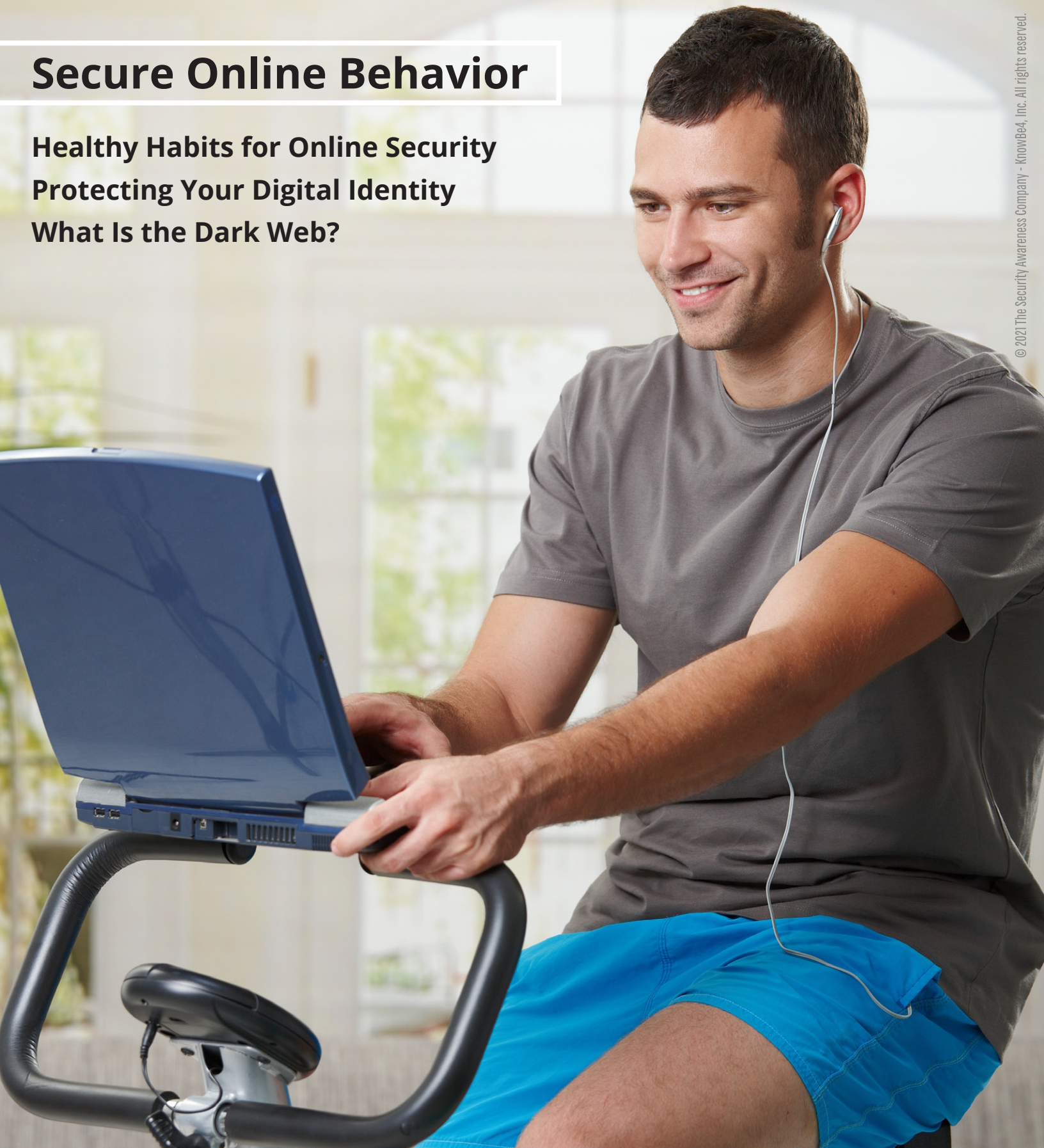
the security awareness newsletter for security aware people

Secure Online Behavior

Healthy Habits for Online Security

Protecting Your Digital Identity

What Is the Dark Web?



Healthy Habits for Online Security

The way we conduct ourselves on the internet carries real consequences. If someone uses their Twitter account to badmouth their organization, that person could face termination or lose out on promotions. If someone carelessly shares personal information on public forums, they could have their identity stolen.

Clearly, there is no buffer between online behavior and real-life results. With that as the focus, here are a few healthy habits that improve online security and keep you out of harm's way:

Remember, the internet never forgets

There are far too many stories of a social media post going viral and it coming back to hurt the person who created it. What you post online stays online forever, even if you delete it. Always consider the ramifications of anything you share.

Manage privacy settings

Modern web browsers offer various levels of privacy settings, such as blocking location access. Maximizing these settings improves your overall security. Occasionally review them to ensure nothing has changed.

Limit permissions

Many websites prompt users to allow notifications and other permissions. Limit these as much as possible to control third-party access to personal information. Do the same for all mobile applications.

Verify the source

Before submitting any personal details, confirm that the website you're visiting is legitimate. Double-check the URL and look for "HTTPS" (instead of HTTP), an internet protocol that indicates an encrypted connection.

Think before you click

Whether it's a suspicious link or a random pop-up, slow down and think before you click to avoid data-stealing malware. And remember that mobile devices are also susceptible to malicious infections.

Here at work, always follow organizational policies, which exist to encourage secure online behavior.

Need more information? Just ask!

Protecting Your Digital Identity

Identity theft is made possible when personal data, such as someone's full name, national ID number, and birth date, ends up in the hands of cybercriminals. They can use that data to commit fraud that directly harms specific individuals, such as applying for credit cards or filing fake insurance claims.

The decisions you make here at work play a huge role in preventing identity theft from happening to someone else. It's one of the reasons we put so much effort into security awareness.

The decisions you make in your personal life play a similar role in protecting your own digital identity. Let's review a few simple actions that will help you stay safe.

Share with care

Cybercriminals often search social media profiles in hopes of finding sensitive data. Don't share any information that could potentially be used against you (or our organization).

Think like a scammer

Before revealing personal data or sending someone money, think like a scammer. Go through all of the possibilities and try to uncover the likelihood that you're being conned in any scenario.

Monitor your money

Get into the habit of routinely logging in to financial accounts and reviewing purchases. Unauthorized transactions are easier to resolve when they're promptly discovered and reported.

Consider a credit freeze

Depending on where you live, you might have an option to freeze your credit. This prevents anyone from running a credit check and opening new accounts. You can lift the freeze as necessary.

Sign up for credit alerts

There are a variety of services that will monitor your credit and send you alerts when something changes. Do some research and find a solution that works for you.

Utilize strong passwords

Secure your accounts with passwords that are at least 16 characters long, never used more than once, and are hard to guess yet easy to remember.

Remember to report all security incidents immediately. Timely reporting could help prevent identity theft from happening to our co-workers, clients, and business associates.

What Is the Dark Web?

To get a true understanding of the dark web (or darknet), it's beneficial to first review the World Wide Web's three layers:

Layer 1: The Surface Web

The internet you know and use every day. It's the indexed portion, meaning it shows up in search engine results and is available to everyone.

Layer 2: The Deep Web

The deep web is hidden and represents the largest percentage of the internet (roughly 95%). It hosts all sorts of private information. When you log in to a bank account, you are visiting the deep web.

Layer 3: The Dark Web

Technically part of the deep web, this is where a variety of questionable or illegal activities sometimes occur. If you've ever wondered what happens to stolen or breached data, it often ends up for sale here.

You've spent most of your time at Layer 1, and some of your time at Layer 2. But what about Layer 3?

As you might know, the dark web is notorious for criminal activity. It's where people can buy or sell illegal goods and services, like stolen credit cards, breached login credentials, illegal drugs, and so on. Unlike typical websites, those on the dark web often require you to know a specific address (and use a special web browser) to find them. This process allows criminals to set up shop and quickly vanish as needed. But it also offers legitimate benefits, such as providing 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 layers, because it was built for the purpose of anonymity. Unfortunately, that purpose also creates a shelter for criminals, which explains the dark web's questionable reputation.

The security implications here are obvious. When you handle confidential data, it's your job to ensure it doesn't end up on the dark web—or any layer of the web where it doesn't belong. You accomplish that task by staying alert for phishing attacks, never plugging in random USB devices, creating strong passwords, and following organizational policy.

From a personal standpoint, note that the dark web is not illegal to visit (there's even a version of Facebook down there!). However, secure online behavior suggests avoiding it unless absolutely necessary.