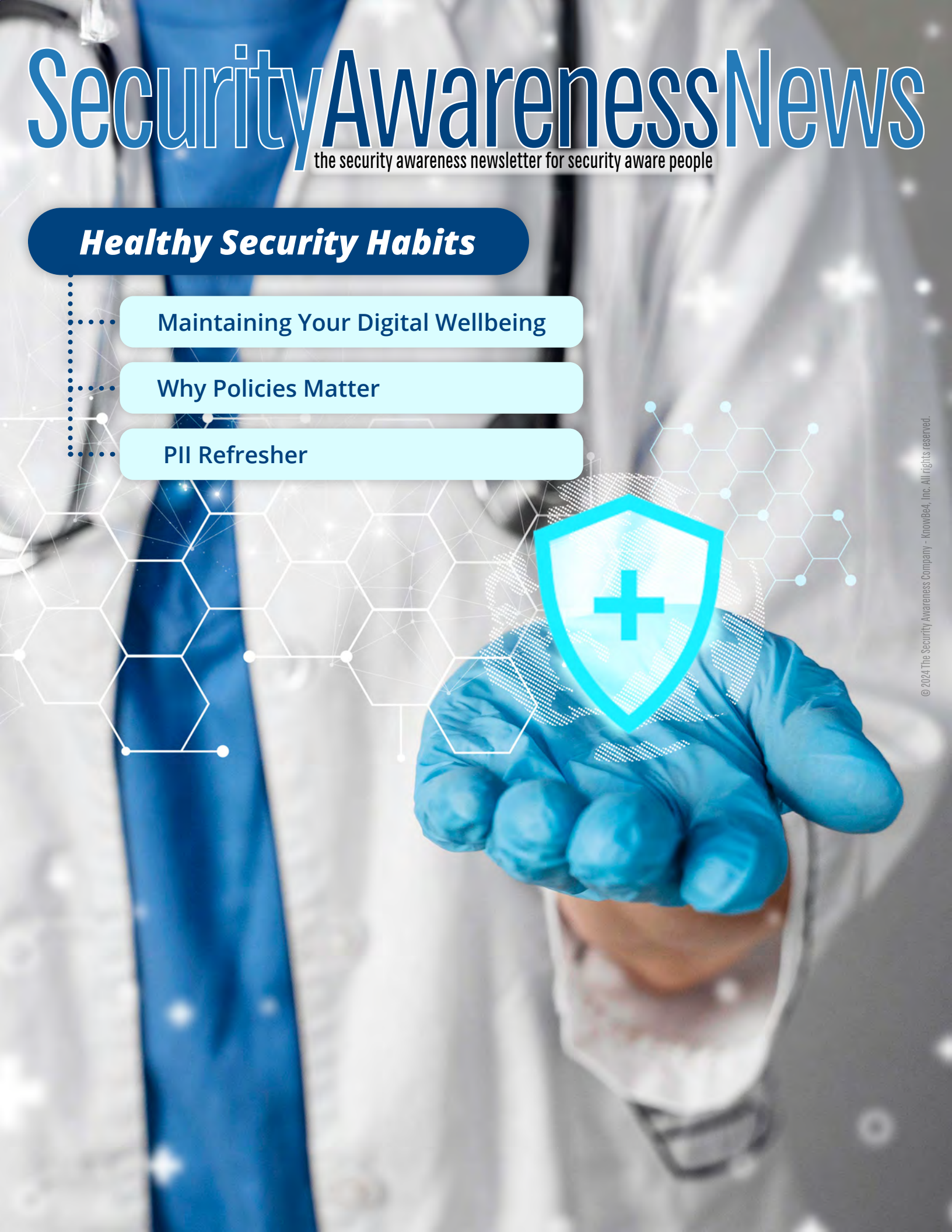
SecurityAwarenessNews

the security awareness newsletter for security aware people

Healthy Security Habits

- Maintaining Your Digital Wellbeing
- Why Policies Matter
- PII Refresher



Maintaining Your Digital Wellbeing

Developing good habits in life is the key to strong physical and mental health. Research shows that people who regularly eat healthy foods and exercise are generally happier. A commitment to those habits (and many others) can be challenging, but it's a fundamental part of living a fulfilling life.

Similarly, you can take actions that contribute to the health of your digital well-being. By making a commitment to the following security habits, you can avoid the many scams and downsides of living in a connected world.

Remain dedicated to strong passwords.

Protecting your online accounts is one of the most important aspects of personal security. As you can probably guess, strong passwords represent the first step to keeping those accounts safe. Reminder: A strong password is long, hard for others to guess but easy for you to remember, and never used twice.

Think before you click.

Phishing is any attempt to lure people into making a bad decision — like clicking on a malicious link or paying a fraudulent invoice — and it is one of the top concerns. Stay alert for common warning signs of those scams, such as threatening messages, unexpected attachments, and urgent requests.

Avoid oversharing on social media.

Scammers often search social media profiles in hopes of finding valuable information. They will then use that information to launch phishing attacks designed to steal money or even more confidential information. Avoid it by setting your social profiles to private and being selective about what you post.

Stay updated.

Outdated devices and software are easy targets for cybercriminals and place confidential information at risk. That's why developers often release updates, especially for operating systems of computers and smartphones. Enable automatic updates wherever they're available so you never miss a crucial patch.

Practice good mobile hygiene.

Smartphones have access to an abundance of personal data and are top targets for cybercriminals. As such, it's crucial to maintain proper mobile hygiene. That means only installing apps from trusted sources, limiting the permissions of those apps (such as access to contacts and location), and removing apps you no longer need.

Why Policies Matter

If work-related security concepts were given a slogan, it would probably be "always follow policy." In fact, you've probably encountered that statement many times, and for good reason. Policies are created to keep data, systems, and people safe.

Without clearly defined policies, organizations would struggle to maintain security. They would also struggle to adhere to compliance regulations — the laws that establish requirements for data privacy. Organizational policies often align with those requirements to ensure rights are not violated.

With that in mind, let's explore a few examples of common policies and why they exist.

POLICY:	WHY?
Passwords must meet specific requirements, such as how long they should be and when they should be updated.	Weak passwords lead to weak security and could allow unauthorized access to confidential information.
Only install approved applications or software.	It's vital for organizations to control the flow of data on devices and manage security vulnerabilities.
Report all security incidents immediately.	Timely reporting helps organizations investigate incidents and mitigate potential damages.
Never plug in random USB devices.	USB flash drives and cables are used by criminals to distribute malware (malicious software).
Always store work-issued devices in a secure manner.	Leaving a laptop or mobile device in plain sight (such as in a vehicle) could lead to theft.

Now imagine none of those example policies existed or if team members blatantly ignored them. Weak passwords, for example, place online accounts at risk of being hacked. It wouldn't take long for the organization to suffer a data breach that leaks sensitive information.

While it might be tempting to view policies as organizations telling people what to do, in reality, policies exist to protect everyone's privacy, including yours! As such, always following policy is a great habit that helps maintain both security and privacy.

PII Refresher

Personally identifiable information, or PII, is a common term associated with data privacy regulations. While "PII" is specific to the United States (other countries call it personal data or simply personal information), the concept of what PII is and why it's so important translates globally. Here's what you need to know:

PII includes many types of data.

It can broadly be defined as "any information that can be used to identify, contact, or locate a specific individual." Examples of PII include full names, home addresses, national ID numbers, and passport numbers. That's a short list, but the key takeaway is that PII refers to confidential information of specific people.

PII is highly sought after by cybercriminals.

PII carries a lot of value. When cybercriminals manage to steal it, they can then sell it to other criminals, use it to launch a variety of scams, or steal someone's identity. Identity theft is especially dangerous because it allows the scammer to open fraudulent accounts in the victim's name.

If you have access to PII, you're responsible for it.

Depending on your role, you might have access to someone's personal information. It's your obligation to ensure that information remains protected. Simple actions like locking workstations when not in use and never sharing your credentials are examples of common sense security that help prevent unauthorized access.

Protecting PII is about more than just protecting data.

While every organization wants to avoid any sort of breach of security, the central concept here is protecting people, not just data. That's because PII is a digital representation of an actual person. When it gets stolen or leaked, it could lead to a variety of harmful consequences that impact someone in real life.

Maintaining data security and privacy is not difficult.

You don't need to be a computer expert to protect PII. In fact, security (and privacy) are functions of using situational awareness and avoiding scams. You can spot scams by looking for common warning signs such as threatening language, urgent requests, and unexpected links or attachments.

Remember, you are the last line of defense when it comes to protecting PII! Stay alert, always follow policy, and think before you click.