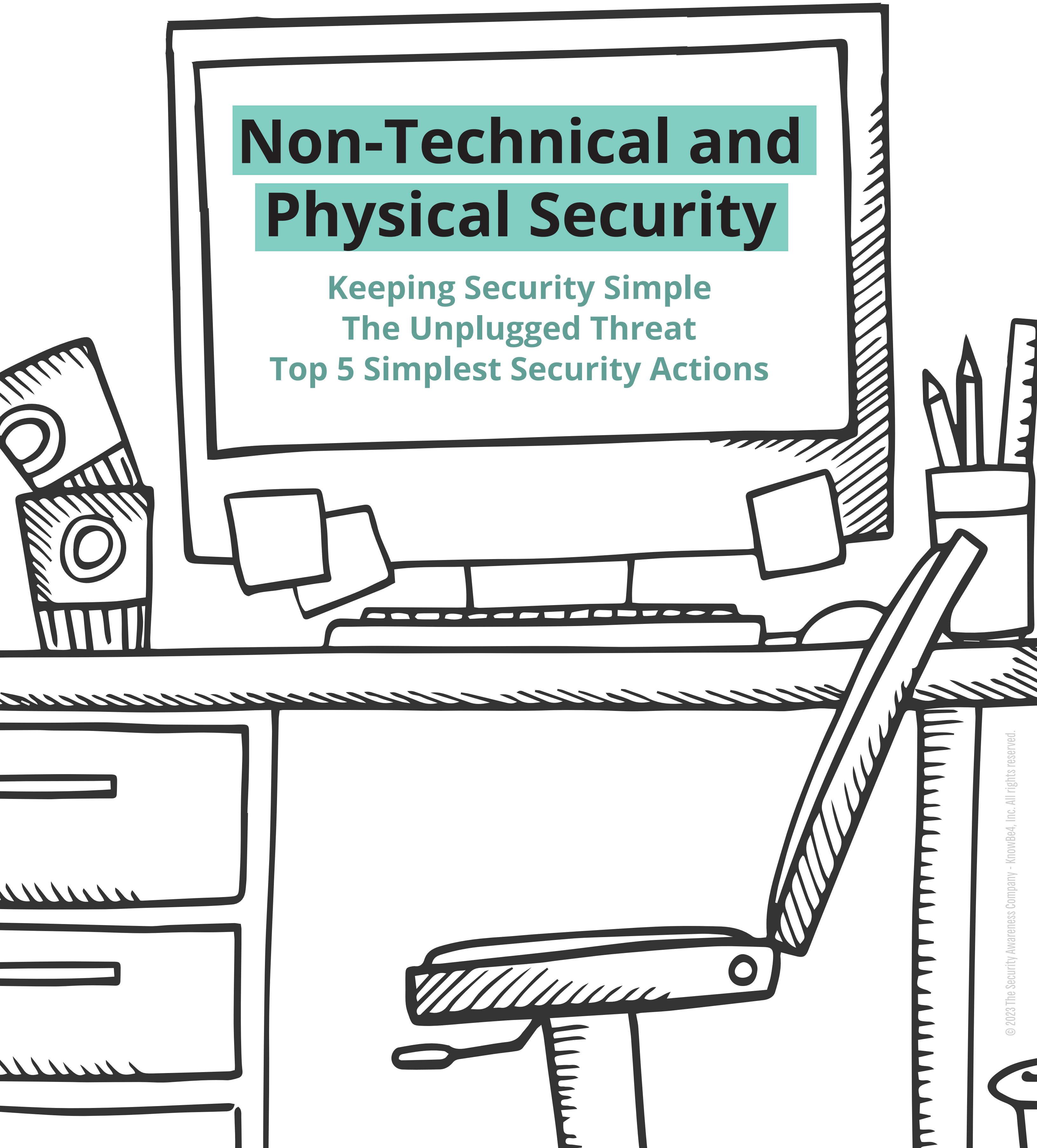
July 2023

SecurityAwarenessNews

the security awareness newsletter for security aware people



Non-Technical and Physical Security

Keeping Security Simple
The Unplugged Threat
Top 5 Simplest Security Actions

Keeping Security Simple

What if you were told that phishing scams — attempts to steal information or infect devices with malicious software — were actually easy to launch? Not that they should be oversimplified, but all anyone needs is an internet connection and someone's email address. That's about it.

Of course, there's a big difference between successful and unsuccessful phishing attempts. The attacker needs to craft a believable message that will convince the recipient to, as an example, divulge their username and password or other personal details. Still, when you think about the steps involved, phishing is not complicated and neither is security. We can keep it simple by answering three fundamental questions:

What do cybercriminals want?

While many cyberattacks are financially motivated, data theft is also a common goal. Confidential information like full names, addresses, national ID numbers, and other personal details carry a lot of value.

How do they get it?

Behind almost every scam is a simple objective: Gain someone's trust and use it against them. Attackers create scenarios designed to mislead people and shortcut rational thinking.

Why do they want it?

The money part is obvious. Stolen information also offers additional paths to paydays. For example, with enough personal data, a scammer could open fraudulent accounts in the victim's name.

Answering these questions helps summarize the simplicity behind many of the threats you might encounter. There are, of course, much more technical attacks used by advanced cybercriminals. In all cases, you can maintain security and privacy by using a combination of awareness, skepticism, and common sense.

Here's what that combination looks like in practice:

Awareness:

Stay alert and keep your guard up. Remember that scammers hope to catch people when they're busy or tired, making them more likely to arrive at quick decisions without much thought.

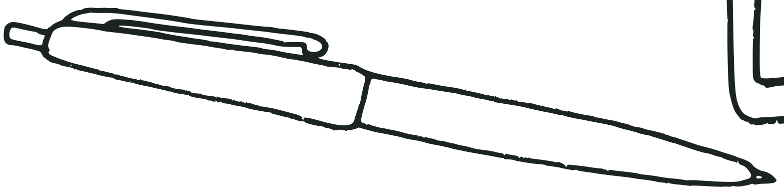
Skepticism:

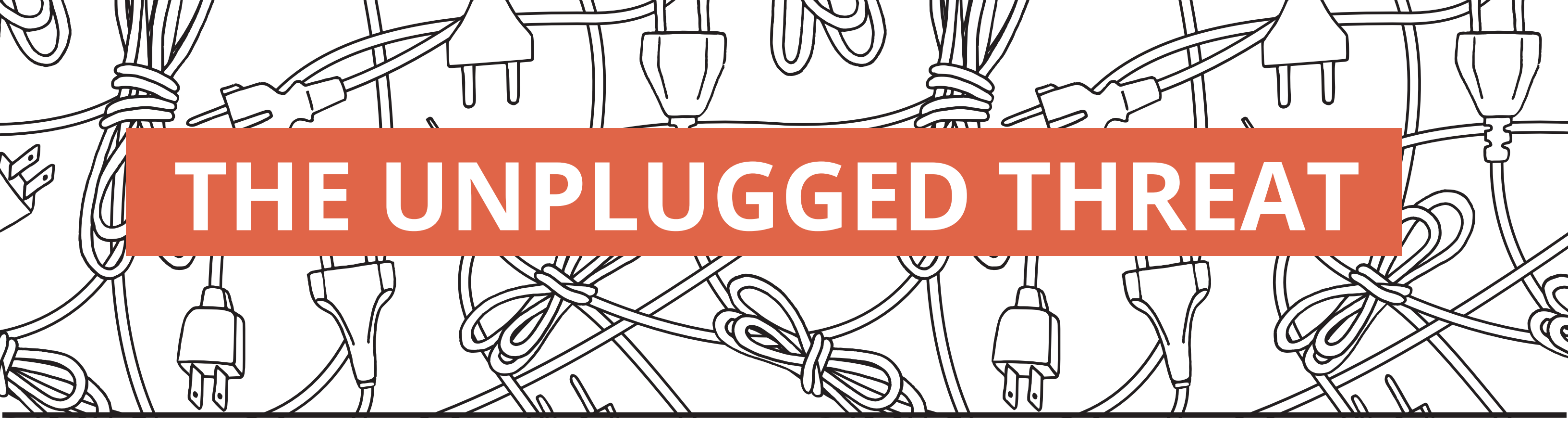
Any scenario that triggers emotions should also trigger your suspicions. Scammers leverage emotions by using threatening language, pushing a sense of urgency, and offering unrealistic promises.

Common sense:

Albeit a vague concept, common sense matters. Most people would never publicize their bank account information for obvious reasons. Apply that mindset when handling requests for sensitive data or money.

Here at work, remember to always follow organizational policies, and report security incidents immediately!





THE UNPLUGGED THREAT

How hard is it to hack into an organization? In theory, it should be quite difficult. Most organizations implement robust cybersecurity controls and policies — the barriers that are designed to protect confidential information and prevent criminal hackers from breaching systems and networks.

Hacking, however, doesn't always require a computer; so those barriers only represent one side of the defensive layer. There's also the non-technical side; the unplugged threat posed by people who use old-school techniques to physically gain unauthorized access. Let's explore what those threats entail and how you can prevent them.

TAILGATING

Physical access to buildings and workplaces offers a lot of value to criminals. That's why they might attempt to sneak in behind someone after that person unlocks a door — an attack known as tailgating. As unlikely as that scenario sounds, it remains a possibility and is a firm reminder to utilize situational awareness by ensuring entry points to protected areas are always secured.

DUMPSTER DIVING

Don't underestimate the willingness of data thieves, some of whom have no shame in digging through trash or recycle bins. Their hope is to find documents that contain confidential information or discarded smart devices where the data hasn't been properly erased. Be sure to properly dispose of any physical documents or assets that contain sensitive data.

PIGGYBACKING

It's polite to hold doors open for people, but it could also be a potential security incident. A scammer might dress up as if they're a member of an organization and claim they don't yet have a badge, so they need you to open the door for them. They "piggyback" off your access. It's not much different than giving someone else your username and password.

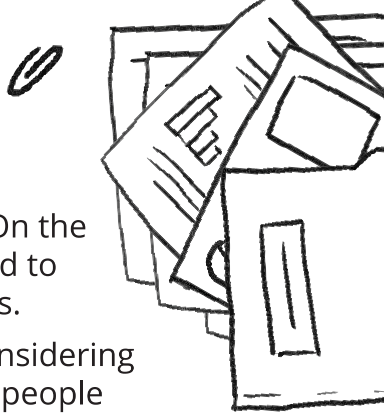
SHOULDER SURFING

Imagine someone on an airplane reviewing documents that contain sensitive information. How easy would it be for anyone sitting near that person to see details like full names, financial information, and email addresses? This unfortunately common scenario highlights the importance of discretion. When in public, it's best to avoid accessing or discussing anything confidential.

Some non-technical threats might seem unlikely, but don't ignore them! Protecting information, assets, and (most importantly) people requires a commitment to security awareness both online and in real life.

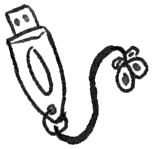
SAC the security awareness™ COMPANY
a KnowBe4 company

Top 5 Simplest Security Actions



Maintaining security and privacy requires a blend of technology and people. On the technology side, organizations often implement a variety of solutions designed to secure networks, filter out unwanted emails, and prevent unauthorized access.

Technology is, of course, imperfect. It can't prevent every threat, especially considering many external attacks are designed to circumvent technology. That's why the people element represents such a vital part of security. After all, people are the last line of defense. Here are five simple actions you can take to reinforce that line.



One: Following Policy

Policies are designed to maintain the security of everyone associated with an organization. They're the guidelines that exist to minimize costly mistakes and identify threats targeting systems, data, and people. Always following those policies represents one of the easiest actions any individual — from the CEO to the front desk — can take.

Three: Keeping a Clean Workspace

Don't overlook the importance of maintaining a clean, organized workspace. It might not seem like a security risk, but a messy desk could lead to mistakes such as misplacing ID badges or sensitive documents. Keep your workspace organized, and be sure to properly store anything that might contain confidential information.

Five: Reporting Incidents

An incident refers to anything suspicious or out of the ordinary. Finding a random USB drive, for example, is an incident that should be reported immediately. Why the urgency? The longer an incident goes unreported, the more harm it could cause. Timely reporting helps organizations quickly review what happened and mitigate potential damages.

Two: Locking Workstations

Regardless of your role or location, it's important to immediately lock workstations and devices when not in use. This simple step takes almost no time at all and helps protect the access entrusted to you. Additionally, ensure all devices are protected with strong, unique passwords, and never share those passwords with anyone.

Four: Avoiding USB Devices

Cybercriminals also prefer to keep things simple. That's why they install malicious software on USB drives and leave them in areas where they'll be found. They'll also mail those drives to organizations and hope somebody will plug one in, which could infect their computer. Avoid this attack by only using the USB devices that you own, including charging cables.