February 2019

Security Awareness News

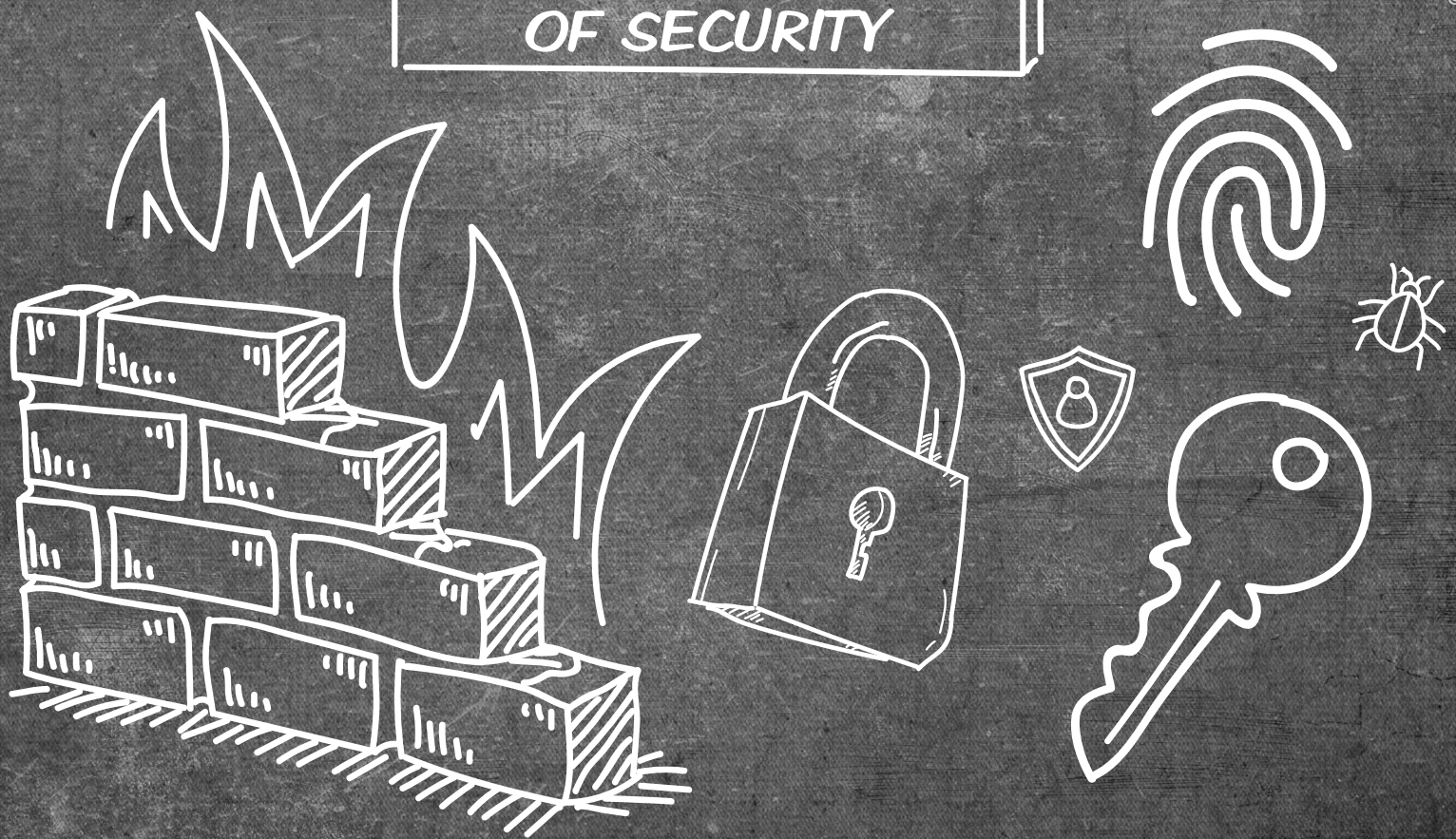
the security awareness newsletter for security aware people

THE SIMPLE SIDE OF SECURITY

KEEPING IT SIMPLE

[SEPARATING PROFESSIONAL FROM PERSONAL]

THE TANGIBLE SIDE OF SECURITY



© The Security Awareness Company, LLC

KEEPING IT SIMPLE

The simplest security actions, ranked!

1

ALWAYS FOLLOWING POLICY.

Our organization's policies were developed to protect sensitive data and prevent security breaches. Circumventing those policies for any reason puts us all at risk.

2

KEEPING A CLEAN DESK.

A messy workspace can inadvertently lead to security blunders. It's a lot easier to lose sensitive documents or ID badges if your desk is a mess!

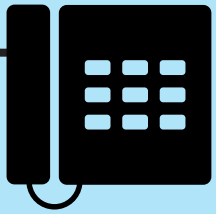
3

PROTECTING PRIVILEGED ACCESS.

Whether it's your usernames and passwords for devices and accounts, or a key that unlocks a secured area, never allowing someone else to use your credentials is one of the easiest actions of security awareness.

The past 15 or so years have ushered in advancements in technology that amaze even the savviest of tech-heads. Many of us would never have thought that controlling lights and thermostats from thousands of miles away could be possible. Or that we would one day be able to use facial recognition to unlock smart devices and fingerprint scanners to unlock physical safes. And that's practically old tech now. On the horizon is a world of connected things (the internet of things, or IoT) that will change the way we interact with nearly every aspect of our lives, both personally and professionally.

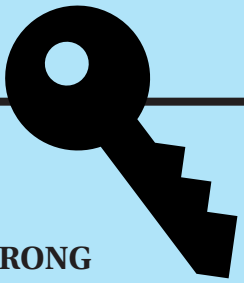
How does it all work? Thankfully, we don't need to understand the complex technical details of gadgets in order to use them and protect them. At home, at work, and on-the-go, developers have created a world of devices and services that make our lives easier. All we have to do is use common sense and situational awareness to avoid causing data leaks or physical security breaches. That's what security awareness is about, after all. It's not a highly technical process that requires you to be well-versed in writing code or setting up networks. **Instead, awareness simply requires you to stay alert, think before you click, and report anything unusual!**



4

REPORTING SECURITY INCIDENTS.

We can't mitigate or prevent future incidents if they go unreported. As always, if you see something or hear something, say something!



5

USING STRONG PASSWORDS.

Passwords are one of the few things standing between sensitive data and cybercriminals. That's why it's vital that we create strong, unique passwords for every account.

© The Security Awareness Company, LLC

A Lesson from Jasper the Disaster

Why should we isolate work data from personal data? Consider the following example:

While traveling, Jasper decides to install a cloud service on his work-issued smartphone, so he can access his music collection. The problem? ***That cloud service backs up everything and syncs it to all of the devices he owns.*** Now, sensitive data from his organization is freely flowing to his personal devices, potentially creating a data leak. Conversely, Jasper's sensitive, personal information like photos or private documents, which should **remain** personal and private, is also flowing freely to that smartphone which is completely monitored and managed by his employer.

You can see how slippery this slope gets. It's an issue that negatively impacts both Jasper and his organization and is a great example of how important it is to isolate your work life from your personal life. ***If you have any concerns or questions about the best ways to separate your professional and personal lives, ask!***

Access Control and the Principle of Least Privilege

Controlling access is a cornerstone of information security. Put simply, access control refers to the management of who has access to what. Some individuals within our organization have been granted a high-level of access. Others have more restricted access. In all cases, every individual has been granted the minimum amount of access needed to perform their job functions. This is known as the principle of least privilege, the purpose of which is to reduce risk to systems and data by limiting access to both.

What's your role in all of this? Obviously, you likely don't have the rights to create or elevate access controls. But you do have the responsibility to protect the access you've been granted. Never allow someone else to use your credentials for any reason. And if you believe you've been granted more access than necessary, please let us know!

BYOD?

BYOD, or bring your own device, presents a challenging scenario for organizations of all shapes and sizes. On one hand, it's valuable to allow end users to access work-related information on their personal devices (laptops, smartphones, and tablets). Doing so provides added efficiency and makes remote work possible.

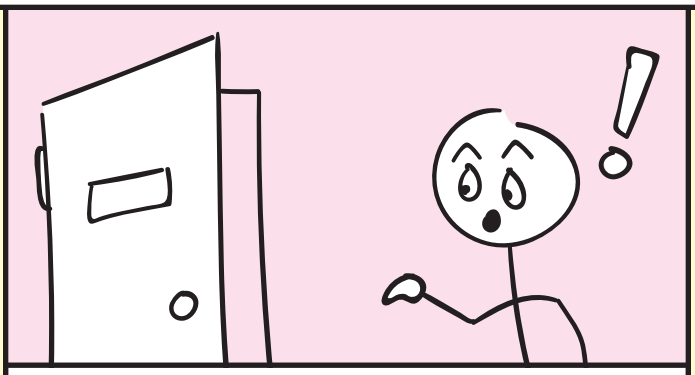
It also adds layers of security risks. ***Organizations have no control over their employees' personal devices, making it impossible to ensure said devices are up to date and properly secured.*** It also makes it difficult to monitor and manage the flow of sensitive data. As such, every organization must weigh the risk/reward for allowing employees to bring their own devices. ***To find out if you may BYOD, please ask! And no matter what, always follow our organization's BYOD policies.***

© The Security Awareness Company, LLC

The Tangible Side of Security

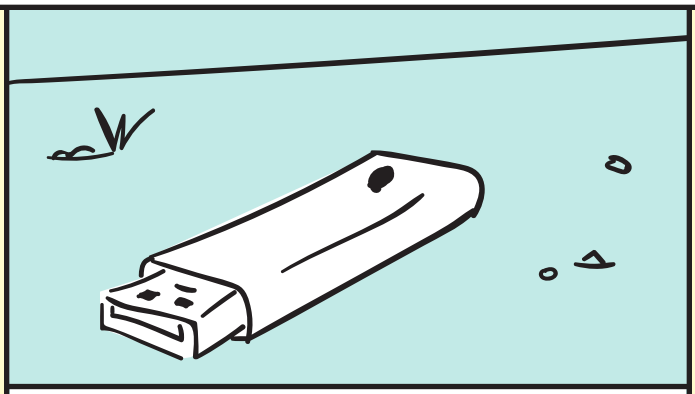
Security awareness isn't isolated to the internet and other cyber-related domains. It has a physical side that deserves just as much attention! Consider the following scenarios and how they might apply to your day-to-day life, both professionally and personally.

Is that door supposed to be open?



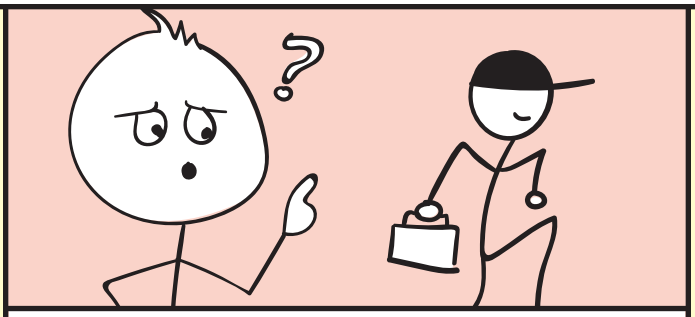
Leaving secured areas unlocked is no different than using a weak password to protect your bank account. **If you see a secured door left open, close it and report it!** If you have access to these areas, don't let anyone else in unless approved and, as you enter, ensure no one sneaks in behind you.

Oh, look, a USB flash drive!



If you randomly find a USB drive or any other form of media, don't plug it in to view the contents. Social engineers intentionally leave these items in areas where they'll be found and accessed. A simple USB drive could lead to a complicated data breach.

Do you know that person?



Maybe he's here to fix the vending machine. Or maybe he's a social engineer dressed up like a service repair guy hoping to gain unauthorized access to our organization. **Never assume an unfamiliar person has the right to be here.** If you see someone you don't know, confirm that they are who they claim to be, and double-check with management. As always, report any unusual events ASAP.

End user discretion is advised.

We discourage you from publicly discussing sensitive data unless you have privacy. But if you must discuss or access sensitive info in public, do so in a way that no one can overhear your conversation or look over your shoulder to see your screen. Keep your voice down and find an area that puts a wall behind you, if possible.

Dissuading dumpster divers.

Social engineers have no shame and will happily dig through dumpsters and recycling bins hoping to find valuable sensitive information. Therefore, **we must always fully destroy data that is no longer needed**, which can mean thoroughly shredding documents or restoring devices to factory defaults before discarding them, for example.

© The Security Awareness Company, LLC