

SecurityAwarenessNews

the security awareness newsletter for security aware people

Healthy Security Habits





Top Five Habits of Security-Aware People

Developing good habits is key to strong physical and mental health. Similarly, developing good security habits can keep you and your organization safe. You don't need to be a computer expert to do this. You just need to practice the right routines until they become automatic.

Here are the top five habits security-aware people include in their daily workflow.

Always Following Policy

Policies are designed to maintain the security of everyone associated with an organization. They're the guidelines that exist to help protect systems, data, and people. Always following those policies is one of the easiest habits any individual can practice.

Staying Alert For Warning Signs

Online scams are everywhere. The key to avoiding them is knowing which warning signs to stay alert for across all forms of communication. Here are a few common examples of signs that someone might be trying to scam you:

- They use threatening language
- They have an unexpected and urgent request for you to take action
- They include suspicious and unexpected links or attachments

Avoiding Assumptions

Scammers know that the easiest way to steal information or money is by making themselves seem trustworthy. They want to mislead people into thinking an email is safe or a phone call is legitimate, hoping the target will let their guard down. That's why it's best to avoid assuming someone is who they claim to be.

Using Multi-Factor Authentication

As always, passwords are a fundamental part of security. But passwords alone are not enough. You should also use multi-factor authentication (MFA). MFA is a security tool that requires at least two forms of authentication before allowing access to an account.

Reporting Incidents

If you ever encounter a scam or notice anything suspicious or unusual, get into the habit of reporting it immediately. Timely reporting helps organizations quickly review what happened and reduce potential harm.

Exercising Physical Security

Security is not just about what happens online or on devices. There's also a physical side to security involving simple actions that play a big role in keeping people, devices, and data safe. Let's review a few ways everyone can contribute to this important part of security.



Lock Your Devices

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 is an important yet simple part of security. Additionally, make sure all devices are protected with strong, unique passwords.



Practice Situational Awareness

Situational awareness is about being mindful of your surroundings. If you ever work in public, be careful about who's around you. Shoulder surfers can easily see your screen to view sensitive data. Also, avoid discussing confidential work details in public places, as you never know who might be listening.



Be Wary of USB Drives

Cybercriminals often install malicious software (malware) on USB drives and leave them in places where they'll be found. The attacker hopes that someone will plug the drive in, which could infect their device with data-stealing malware. Avoid this attack by using only the USB devices you own.



Store Documents Properly

Physical documents can be just as sensitive as digital files. Never leave documents containing confidential information out in the open where anyone could access them. Store them securely (such as in a locked drawer) and properly dispose of them when no longer needed.



Prevent Tailgating

Physical access to buildings and workplaces is important to some criminals. That's why they might attempt to sneak in behind someone after that person unlocks a door. This is an attack known as tailgating. As unlikely as that scenario sounds, it remains a possibility and is a firm reminder to ensure that entries to protected areas are always secured.

Digital Health Checkup

Maintaining your digital health is a lot like staying physically fit: It isn't a one-time event. Instead, it's about the small choices anyone can make to keep devices secure and avoid risks. And just as a yearly checkup with a doctor helps catch small health issues before they become big problems, a digital health checkup helps you spot risks before they turn into security incidents.

Use this guide to keep your digital life healthy and secure.

Stay Up to Date



Outdated devices and software are common targets for cybercriminals and can expose confidential information. That's why developers often release updates, especially for the operating systems of computers and smartphones. Enable automatic updates wherever they're available so you never miss an important security upgrade.

Don't Overshare on Socials



Some people tend to overshare personal details on social media, which scammers are happy to abuse. You can avoid those scammers by limiting what you share and being selective about who may access what you post. It's usually best to set your profiles to private and only connect with people you know and trust.

Review Your Apps



Occasionally, it's a good idea to review the apps on your phone and uninstall any you no longer use. This process not only frees up storage space but also removes any applications that might be collecting personal data.

Consider Getting a Password Manager



A password manager is software designed to create and store your passwords for various websites and services. It can automatically provide long, complex, and unique passwords for every account, so you don't have to memorize them. You only need to remember one strong main password to unlock the application.