SecurityAwarenessNews

the security awareness newsletter for security aware people

Non-technical and Physical Security

Common Sense Security Awareness • 6 Simple Ways to Improve Security • Hacking Without Computers

Common Sense Security Awareness

How hard is it to hack an organization? Let's reverse engineer a cyber attack. Surely you must have a firm understanding of technology and computers, right? Maybe you develop or purchase sophisticated tools designed to infiltrate network firewalls and other cyber defenses. Once inside the organization, you need to navigate the network and eventually siphon the confidential information you're after—all without leaving a trace of your identity.

Sound complicated? In some cases, attacking organizations represents a challenging exercise. But it doesn't take a computer science degree to understand that, most often, **it's not computers that get hacked—it's humans.**

In other words, cybercriminals aren't always writing complicated code designed to break through our digital defenses and steal data. Instead, they're busy creating elaborate schemes that target you. They know the quickest and easiest way to pull off their scams is by tricking individuals into doing something risky like clicking on a malicious link or plugging in a random USB flash drive.

That's why we put so much weight on common sense security awareness. Yes, we need to implement technical processes to eliminate certain types of cyber attacks. **We also need to use common sense, and give physical security just as much attention as cybersecurity.**

Common sense security awareness requires that we consider the outcomes of our actions. What could happen if you discard a sensitive document without shredding it? What could happen if you use the same password for multiple accounts? What could happen if you download a random attachment? What could happen if you post sensitive information on Facebook? What could happen if you leave a smart device unattended in a vehicle or coffee shop?

Some aspects of information security involve highly technical processes. All aspects of information security involve human processes. So do your part. Don't assume it's only the IT department's responsibility to prevent data breaches and other security incidents. Instead, use common sense and stay alert. Always follow our organization's policies. And if you have questions or need more information, please ask!

6 Simple Ways to Improve Security

Sometimes "cybersecurity" gets associated with "technology" as if the two are inseparable. While they are correlated, security doesn't require that you have a strong technical background. It's often straightforward. Here are six examples that demonstrate the simplicity of improved security:

one:
Delete unused apps.

People tend to install a variety of applications on computers and smart devices, and then forget about those applications over time. Take a few minutes every month to perform a digital cleaning and delete software or disable accounts you no longer use.

two:
If you see something, say something.

Reporting security incidents represents one of the easiest and most vital components of information security. The longer an incident goes unreported, the more damage it could cause. From phishing emails to secured doors left open, there is no potential security incident too small to report.

three:
Enable multi-factor authentication (MFA).

Every superhero has a sidekick. Think of multi-factor authentication as your password's sidekick. It helps protect your account by requiring a second code to log in (often sent via text message or email, or through an authenticator app). That way, if someone manages to get ahold of your password, they will still need the second code to access your account.

four:
Stay up to date.

Out-of-date devices and apps leave doors open for cybercriminals. Developers often use updates to close those doors and patch security holes. You can easily improve security by implementing automatic updates on all devices and software, so you never miss an essential upgrade.

five:
Audit privacy settings.

When was the last time you reviewed who can see what on your social media feeds? Do you know which apps have elevated permissions and access to personal data? As tedious as auditing privacy settings may sound, think of it as a way of regaining control of your privacy.

six:
Get a password manager.

For most of us, memorizing every username and password for every account is nearly impossible. That explains the tendency to use the same password for multiple accounts—a mistake that increases vulnerability. Make your life easier (and more secure) by getting a password manager, which is software that can create, store, and sync all your login credentials across multiple devices.

Bonus: Always follow policy.

Policies eliminate unnecessary risks and ultimately empower our organization to maintain the privacy of employees, clients, and business associates. When you, as a human firewall, always follow our policies, you help prevent security breaches while improving our organization's culture.

Hacking Without Computers

Returning to the opening question of "how hard is it to hack an organization?", let's focus on a few examples of how attackers "hack" you without using computers.

Tailgating

Physical access to buildings and workplaces offers a lot of value to criminals. That's why they might attempt to slip in behind someone after that person unlocks a door—an attack known as tailgating. This is also why we must take great care of our badges or keycards and ensure that they never end up in the wrong hands.

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 our organization and claim that 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 usernames and passwords (pro tip: don't do that).

Shoulder Surfing

Imagine you're sitting at an airport café working on a document that contains sensitive information. Since you practice common sense security awareness, your back is to the wall and no one can see your screen. If not for that simple action, any stranger passing by could look over your shoulder and potentially snap a quick picture of your screen and steal confidential information. We recommend never accessing that type of data in public settings, but if you must, use discretion and make sure no one can see what you're working on.

Dumpster Diving

Consider the example from above. This time imagine that the document has been printed out because someone needed a physical copy for a meeting. Now that the meeting is over, the document is no longer needed. That person decides to crumple it up and throw it away. The problem? As unlikely as this may sound, a scammer could dig through the trash and recover that document along with all the sensitive details it contains. If you make physical copies, be sure to shred them to prevent data leaks.

Pretexting

At the core of almost every scam is a pretext—a fabricated scenario designed to gain and abuse your trust. Attackers use a pretext to convince their victims to release sensitive information or, as we noted under the piggybacking example, a pretext could involve persuading someone to hold a door open. In some cases, the attacker may call you and pretend to be IT personnel or a customer service agent from a bank. Never give away confidential information unless you know for a fact the recipient is trustworthy and authorized to receive the information. This applies to both your job here at work and to your personal life.