

Security Awareness News

the security awareness newsletter for security aware people

Security Awareness and Culture

The True Meaning of Security Awareness

How You Can Help Build a Healthy Security Culture

Becoming a Security Champion





The True Meaning of Security Awareness

The concept of awareness refers to someone's perception and knowledge of any given situation. Awareness serves many different purposes and is often applied to multiple use cases.

For example, it's common for various entities to raise public awareness, usually involving personal safety. The goal of public awareness campaigns is to educate large groups of people about issues that could directly impact them.

Brand awareness is similar but often serves a profit-driven agenda. Companies and organizations need to ensure their products or services are recognizable by the public at large. Brand awareness achieves that and is a vital part of marketing that helps one product or service stand out from another.

Then there's security awareness. In most work environments, security awareness involves employees who are knowledgeable about the various threats to data, systems, and people. When you inspect an email for warning signs of a phishing attack — such as poor grammar, threatening or urgent language, and suspicious links or attachments — you are using security awareness.

While these examples offer ideal definitions of awareness, there's one key concept that deserves closer attention: Someone being aware of something doesn't mean they care about that thing.

Thus, true security awareness means that individuals are not only knowledgeable of various threats, but also recognize the importance of preventing those threats from causing harm. It can further be packaged into a few general ideas:

It's an attitude: The thoughts and beliefs about general security issues and how they impact you and your organization.

It's a mindset: The ongoing perception of threats and the approach you take to handling daily routines with a security-first viewpoint.

It's a culture: The shared values, customs, and behaviors that determine the strength of an organization's resistance to cybercrime.

In fact, culture is the foundation upon which an organization's success is built. Every individual, through their awareness and their actions, influences the health of that culture in various ways. You can do your part by staying alert, caring enough to understand what's at stake, and being prepared to address any threats you might encounter.



How You Can Help Build a Healthy Security Culture



Every member of an organization plays an important role in shaping culture, which includes a commitment to maintaining security and privacy. Here's how you can help strengthen the security culture you're a part of:



Take Security Personally

While most security awareness programs focus on the security of an organization, the lessons you learn can and should be applied to your personal life. Cybercriminals are always trying to scam people in multiple ways, both in professional environments and in personal scenarios. Stay alert and make security awareness part of your life.



Always Follow Policy

Policies eliminate unnecessary risks and empower organizations to maintain the privacy of employees, clients, and business associates. Ensuring that security policies are never circumvented for any reason is a form of leading by example and directly impacts an organization's overall security posture.



Be a Culture Carrier

Culture carriers are the individuals who have an intimate knowledge of an organization's core values. They use that knowledge to positively influence those around them through problem solving and communication. You can become a culture carrier by gaining a firm understanding of security awareness and promoting the key messages of awareness programs.



Avoid Making Assumptions

Scammers know that the easiest way to steal information or money is by making themselves seem trustworthy. They deliberately 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 vital to avoid assuming someone is who they claim to be and always remain skeptical.



Report Security Incidents Immediately

Preventing security incidents is a shared responsibility across an organization's culture. Unfortunately, incidents can arise. When they do, it's vital to report them immediately. Timely reporting helps organizations review what happened and spread awareness to others, which can mitigate potential damages and reduce the chances of an incident happening again.



Becoming a Security Champion

An organization's culture is only as healthy as the people who form it. Like a houseplant, culture needs some care and attention to maintain its strength and continue to grow. Security champions play a key role in that vital process. Let's explore this concept by answering a few common questions.



What is a security champion?

Security champions (also known as ambassadors) are people who are thoroughly familiar with the values of an organization and help others uphold those values. They are culture carriers who stoke positive reinforcement of all things related to security awareness and nourish culture through their actions.



Do you need to be a security expert?

No expertise is necessary. Instead, champions have a general understanding of security and a willingness to learn more and grow beyond their daily responsibilities. In the process, they can earn the respect and trust of co-workers while also enhancing security culture.



Can anyone become a security champion?

The short answer is yes, but becoming a champion does not happen automatically. Many organizations have a system in place to determine who's best suited for the role. Some champions are chosen by leadership; others are nominated by their peers.



What qualifications are necessary?

Qualifications vary by industry, but security champions generally:

- *Demonstrate a fundamental understanding of security*
- *Stay informed about modern threats*
- *Offer support and help others when needed*
- *Possess strong communication skills*
- *Lead by example*



Are you a security champion?

If this concept resonates with you, then perhaps you have what it takes to be a security champion! Of course, it's not a role that's desirable for everyone (and some organizations don't recognize the role). Regardless, everyone can benefit — professionally and personally — by making an effort to meet the qualifications of becoming a security champion.

As always, be sure to follow your organization's policies and report security incidents immediately.