SecurityAwarenessNews
the security awareness newsletter for security aware people

Security Awareness Culture

7 Dimensions of Security Culture
How You Can Strengthen Security Culture
Security Culture at Home

7 Dimensions of Security Culture

In the fourth annual Security Culture Report, CLTRe (a KnowBe4 company) surveyed over 320,000 employees and 1,800 organizations around the world in an effort to measure the impact of security culture. The report defines security culture as "the ideas, customs, and social behaviors of an organization that influence their security" and evaluates individuals across seven dimensions:

Attitudes
The feelings and beliefs that employees have toward the security protocols and issues.

Behaviors
The actions and activities that have an impact on the organization's security.

Cognition
The understanding, knowledge, and awareness of security issues.

Communication
The quality of communication channels to discuss security topics and provide support and a sense of belonging.

Compliance
The knowledge of written security policies and the extent to which they are followed.

Norms
The knowledge of and adherence to unwritten rules of conduct within an organization.

Responsibilities
How individuals perceive their role in the strength of an organization's security.

These concepts provide clear insight into the significance of an individual's mindset. In fact, 94% of security leaders reported that culture is the most important element in their security strategy, which makes sense. A healthy culture empowers people with a sense of belonging and provides visible, safe paths for communication.

The challenge is that culture can't be artificially manufactured or enforced with rules and guidelines. Instead, it must grow organically as an extension of strong leadership. What does this mean for you?

As a valued employee, you play an important role in the strength of our culture and our shared goal of maintaining security and privacy. Your attitude, your behavior, and the decisions you make all combine to determine whether we accomplish that goal.

At the end of the day, security isn't just about computers and data. It's about people (like you!) who lead by example, follow policy, and ask questions when they need help.

How You Can Strengthen Security Culture

A healthy security culture features individuals who understand their responsibilities, can readily identify cyberthreats and other risks, and know what to do should a security incident arise. Here's how you can help strengthen the culture you're a part of:

Take Training Seriously

We get it. Training can sometimes feel like a distraction that impedes productivity. It's also a vital element of developing a healthy culture that avoids security incidents. Furthermore, the lessons you learn from awareness training can be applied to your personal life, which will help you avoid scams and keep your personal information safe.

Lead by Example

Even if you're not in a management or leadership position, setting a good example matters. Remember, your attitude influences others and, by extension, the health of our organization's culture. When you address security awareness with optimism and sincerity, your teammates will take notice and feel inclined to reciprocate that behavior.

Think Like a Scammer

Whenever you're faced with a scenario that could threaten security (such as a potential phishing email), put your scammer hat on. Ask yourself, "How likely is it that I'm being scammed right now? What's the worst that can happen if I click that link or divulge that information?" This proactive mindset helps people identify and eliminate threats.

Never Make Assumptions

Imagine you're in charge of wiring funds to third-party vendors. You receive an email from your boss with a random request to send money to a new vendor. Do you process the request without a thought? If yes, then you've made the assumption that the email is actually from your boss and not an imposter. Assumptions lead to costly mistakes. Ask questions instead!

Always Follow Policy

We mentioned earlier that culture cannot be manufactured through rules and guidelines. But that doesn't reduce the importance of following organizational policies. In fact, ensuring that security policies are never circumvented for any reason is a form of leading by example and directly impacts our overall security posture.

Security Culture at Home

We believe that building a strong culture extends beyond the borders of work. That's why we encourage you to take the information we provide through awareness training and create a security culture in your household. Here are a few tips for how to do that:

Develop Password Policies

Most organizations have requirements for how passwords are created and stored. Individuals would be wise to follow suit and protect their personal accounts with strong passwords. As a reminder, a strong password is:

1. **long (a minimum of 12 characters)**
2. **never used twice**
3. **hard to guess but easy to remember**

Keep Devices Updated

Developers often push security updates to devices and software. Ignoring them opens the door for cybercriminals who can exploit vulnerabilities that compromise your security. Ideally, enable automatic updating wherever it's available.

Get the Right Tools

Here's a quick list of security tools that are inexpensive and easy to use:

- ***Virtual private network (VPN): encrypts your internet connection to prevent data theft.***
- ***Password manager: creates, stores, and syncs login credentials across multiple devices.***
- ***Antivirus/anti-malware: defends your devices against viruses and malware.***
- ***Data backup: ensures you won't lose data in the event of a computer failure or malware infection.***

Limit What You Share

Scammers use social media and other public forums to collect personal information. Never share anything confidential, and consider setting accounts to private. Only accept friend requests or connect with people after you've verified their legitimacy.

Have the Talk

For those of you with kids, it's vital that you empower them to stay safe on the internet. They must understand the dangers of cyberbullying, sharing inappropriate content, and divulging personal information. These lessons should be taught before kids are allowed to go online.

Stay Informed

Knowledge is power. Stay informed of current cyberthreats, and research all software products before installing. Don't assume cybercriminals only attack organizations. Learn to identify phishing attacks and other scams that attempt to steal data or money.