Educate Employees to Practice Better Cybersecurity

HR Bartender | Sharlyn Lauby | March 12, 2024

Image captured by Sharlyn Lauby after the SHRM Annual Conference in Las Vegas, NV

As you may know, Mr. Bartender and I are fans of the Marvel Cinematic Universe (MCU). Lately, we've been getting caught up on older episodes of the show Jessica Jones. One of the episodes we watched recently showed private-investigator Jessica breaking into a morgue to gather information about someone and she needed to access the computer.

At first, she starts cursing that she can't get the information she needs because the computer is password-protected. Then she looks up to find – yep, you guessed it – the password was on a sticky note next to the computer screen.

Of course, we can laugh about it … this is superhero television (and who breaks into a morgue to hack a computer anyway). But how many places today still use the "password on a sticky note" approach to technology? Honestly, it's time for everyone to take cybersecurity seriously.

According to TechReport, 88% of security threats occur due to human error. I'm sure a lot of that human error is simply not knowing good cybersecurity practices. Cybercrime has a significant impact on organizations and the economy. It's predicted to reach $10.5 trillion dollars by next year (and that's not a typo – trillion).

One of the statistics that really stuck out for me in the article was that it can take up to 277 days to discover, identify, and contain a data breach. How many times do we click on a link and immediately think "Hmmm…should I have done that? Well, nothing appears to be wrong, so it must have been okay." The reality is … maybe not.

The reason I'm bringing this up is because the Society for Human Resource Management (SHRM) allowed me to preview a new program titled "Cyber Security: Self Defense in the Digital Age". It's a 30-minute session that outlines everyday steps that we can take to practice better cybersecurity.

The program is narrated by Jesse Goldhammer from the University of California's Berkeley School of Information and Center for Long-Term Cybersecurity. Goldhammer does a great job of conveying highly technical information in a casual manner. The session provides tips that serve as good reminders as well as new security information. The program also includes a quiz at the end for learning reinforcement.

I know a lot of companies make employees watch some sort of cybersecurity video if they click on a phishing email. But as I was watching this program it occurred to be that it might be better to take a proactive approach and have employees view something that shares best practices versus watching something after you have already made a mistake.

Given the organizational impact that cybersecurity threats can have, this is something human resources and learning professionals should educate themselves on. If an organization is experiencing a lot of turnover, it's possible that new employees don't know the organization's cybersecurity protocols. Honestly, it's not their fault.

Cybersecurity is also a topic that would be perfect for orientation or onboarding. Give employees the education they need to practice good cybersecurity from the start.

And if the organization already has a cybersecurity program in place, consider a regular schedule of refresher training that serves to heighten an employee's awareness. Whether we want to admit it or not, we've all found ourselves in a place where we're busy, frustrated, and the last thing we want to do is set up two-factor authentication for some software. But we also know that it's the right thing to do.

In the 2023, Voice of the Chief Information Security Officer (CISO) report, 68% of CISOs felt their organization was at risk of a material cyberattack (up from 48% the year prior). On the flip side, 61% felt unprepared to deal with a cyberattack (up from last year's 50%). Organizations cannot afford to sit back and say, "Oh, we're not a target for hackers. That happens to big, high-profile companies." These days, that's simply not true.

Because human error plays a role in cybersecurity, human resources departments should be a part of the conversation. That means educating ourselves so we can help the organization find good programs to educate employees.