Exploits & Vulnerabilities

Employee Security Training is Vital to Remote Success

Organisations were forced to adapt rapidly over the past months as lockdowns kept most workers at home. Employees are often described as the weakest link in corporate security chains, do they become an even greater liability when working from home?

By: Trend Micro
July 01, 2020
Read time: 2 min (564 words)

Authors

Trend Micro
Research, News, and Perspectives

Organisations have been forced to adapt rapidly over the past few months as government lockdowns kept most workers to their homes. For many, the changes they've made may even become permanent as more distributed working becomes the norm. This has major implications for cybersecurity. Employees are often described as the weakest link in the corporate security chain, so do they become an even greater liability when working from home?

Unfortunately, a major new study from Trend Micro finds that, although many have become more cyber-aware during lockdown, bad habits persist. CISOs looking to ramp up user awareness training may get a better return on investment if they try to personalize strategies according to specific user personas.

What we found

We polled 13,200 remote workers across 27 countries to compile the Head in the Clouds study. It reveals that 72% feel more conscious of their organisation's cybersecurity policies since lockdown began, 85% claim they take IT instructions seriously, and 81% agree that cybersecurity is partly their responsibility. Nearly two-thirds (64%) even admit that using non-work apps on a corporate device is a risk.

Yet in spite of these lockdown learnings, many employees are more preoccupied by productivity. Over half (56%) admit using a non-work app on a corporate device, and 66% have uploaded corporate data to it; 39% of respondents "often" or "always" access corporate data from a personal device; and 29% feel they can get away with using a non-work app, as IT-backed solutions are "nonsense."

This is a recipe for shadow IT and escalating levels of cyber-risk. It also illustrates that current approaches to user awareness training are falling short. In fact, many employees seem to be aware of what best practice looks like, they just choose not to follow it.

Four security personas

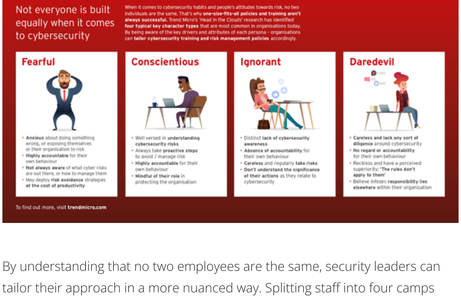
This is where the second part of the research comes in. Trend Micro commissioned Dr Linda Kaye, Cyberpsychology Academic at Edge Hill University, to profile four employee personas based on their cybersecurity behaviors: fearful, conscientious, ignorant and daredevil.

In this way: Fearful employees may benefit from training simulation tools like Trend Micro's Phish Insight, with real-time feedback from security controls and mentoring.

Conscientious staff require very little training but can be used as exemplars of good behavior, and to team up with "buddies" from the other groups.

Ignorant users need gamification techniques and simulation exercises to keep them engaged in training, and may also require additional interventions to truly understand the consequences of risky behavior.

Daredevil employees are perhaps the most challenging because their wrongdoing is the result not of ignorance but a perceived superiority to others. Organisations may need to use award schemes to promote compliance, and, in extreme circumstances, step up data loss prevention and security controls to mitigate their risky behavior.



By understanding that no two employees are the same, security leaders can tailor their approach in a more nuanced way. Splitting staff into four camps should ensure a more personalized approach than the one-size-fits-all training sessions most organisations run today.

Ultimately, remote working only works if there is a high degree of trust between managers and their teams. Once the pandemic recedes and staff are technically allowed back in the office, that trust will have to be re-earned if they are to continue benefiting from a Work From Home environment.

Tags

How To | Web | Exploits & Vulnerabilities | Mobile | Articles, News, Reports

Related Articles

New Ransomware Spotted: White Rabbit and Its Evasion Tactics

Earth Lusca Employs Sophisticated Infrastructure, Varied Tools and Techniques

This Week in Security News - January 14, 2022

See all articles ›

Recommended for you

Ransomware

Cybersecurity for Industrial Control Systems: Part 1

Learn more ›