Improving information security by giving employees options

March 27 2018, by Eric Hollenbeck

Credit: CC0 Public Domain

Computer users — at home and at work — often engage in behaviors that create security risks and privacy threats, despite having a variety of security options available.

Clicking on unfamiliar links, choosing weak passwords and sharing personal information can leave a user's computer or employer open to having information stolen.

For businesses, this is especially concerning because employees who engage in risky behaviors at home may carry those habits into the workplace, putting the company, fellow employees and customers at risk. According to IBM and the Ponemon Institute, the average cost of a data breach for companies in 2017 was more than $3.5 million.

Give employees a reason to care

A recent study published in the *Journal of Management Information Systems* suggests information security managers and supervisors could have greater success in motivating employees to act more securely by avoiding cold, authoritative commands, and instead create security messages that are relatable and provide options for how employees can better protect information and respond to threats.

According to Washington State University researcher and co-author Rob Crossler, Carson College of Business assistant professor of information systems, employees may fail to realize they are putting company data at risk or have less of an interest in taking steps to ensure security because it's not their personal data.

"If you want people inside an organization to truly change their security behaviors, you have to give them a reason to care," said Crossler. "You have to get them motivated in order to be effective at changing behaviors."

Choices not mandates

According to Crossler, when employees feel they have a choice in their response in what works best for them, they tend to take actions that are more secure.

He recommends information systems managers avoid messaging that is too rigid in its instruction, and instead focuses on different strategies for protecting information and responding to threats. For example:

Your passwords are the keys to your digital life, and your online accounts are a proverbial gold mine for someone looking to steal your identity. Hackers often accomplish identity theft by figuring out online passwords. Regardless of how confident you are in your computer skills, you can learn how to create strong passwords and manage them using a password manager. A password manager is software that aids in keeping track of multiple passwords. We recommend using Dashlane, 1Password, KeePass or LastPass. Each of these is an adequate solution, so feel free to choose the software you like the best as your password manager.

The goal is "changing the conversation to be about a partnership," Crossler said. "The focus should be 'We are in this together, and you have options on what you can do to help,' as opposed to 'You have to do this or that.'"

Better security not perfection

"When it comes to securing what you are doing, we are all going to fail. We are not going to be perfect. Phishing attacks are getting so good that even the most alert individual is going to make a mistake," he said. "If they fail in their actions, employees should be encouraged to immediately report it and do the right thing without fear of being reprimanded."

Organizations can work to safeguard against security threats and encourage their employees to make better decisions by providing information and security training on a more frequent, year-round basis, said Crossler. Managers and supervisors also can find the latest information on security issues and threats, as well as access up-to-date education and training resources, on the United States Computer Emergency Readiness Team website (http://www.us-cert.gov).

More information: Philip Menard et al, User Motivations in Protecting Information Security: Protection Motivation Theory Versus Self-Determination Theory, *Journal of Management Information Systems* (2018). DOI: 10.1080/07421222.2017.1394083

Provided by Washington State University