How mindfulness can help prevent hacks, and four more cybersecurity tips

August 29 2018, by Caroline Newman

Ryan Wright, the C. Coleman McGehee Professor of Commerce at UVA, specializes in cybersecurity and works with UVA's information security team to improve cybersecurity at the University. Credit: Dan Addison, University Communications

You probably have a phishing email in your inbox right now.

It might be an obvious scam, but it's more likely to be an insidiously friendly note that looks like it is from a colleague or friend, asking you to click this link or open that attachment. If you do, a hacker could access your username and password, potentially stealing troves of data and compromising your entire organization

"Phishing scams have changed substantially over the last three years," said Ryan Wright, the C. Coleman McGehee Professor of Commerce in the University of Virginia's McIntire School of Commerce. Hackers, he said, have moved from sending out millions of phony emails to ruthlessly targeting individual users, often using information from social media accounts to pose as colleagues, friends or family members.

Wright researches and teaches about cybersecurity and works with UVA's chief information security officer, Jason Belford, to improve cybersecurity at the University. He is also working with Vice President for Information Technology Ronald R. Hutchins to develop new anti-phishing training for all state employees.

Here are his tips for protecting yourself and your organization.

Understand how phishing scams really work

Email phishing scams are the most common technique hackers use to access individual usernames and passwords and thus infiltrate whole organizations.

Though we typically envision hackers as computer whizzes who build their own programs, Wright said that most simply buy phishing software off the dark web and use it to set up an email phishing scam.

If users click on a link or attachment in the phishing email, they are directed to a phony webpage, such as the Russian-backed sites

uncovered by Microsoft this week. Malware coded into the site steals their information, typically their username and password.

Hackers can then pose as a user to access information across an organization. Just one click, from one user, has triggered major hacks at organizations from Target to the U.S. government – despite their best efforts to secure their technical borders.

According to Wright, the average phishing webpage lasts about seven days, because response rates to any phishing email – just like a regular email – drop dramatically after 24 to 36 hours.

"Hackers know that they only need a site up for a few days," Wright said. "They set up millions of them. Identifying them is a bit like playing 'Whac-a-Mole' – you can't take them down fast enough."

Understand that you are the target, not your computer

"We tend to think of cybersecurity as a technical problem, but it is really a human problem," Wright said. "Ninety to 95 percent of attacks on organizations are attacks on individual people."

A recent study for Cybersecurity at Work, released this month, found that individual employees are the biggest risk factor for organizations. Nearly two in five surveyed admitted to clicking on a dubious link or attachment – about 40 percent of the workforce.

According to Wright, today's average phishing scam targets about nine people, using information from their LinkedIn, Facebook and other social media accounts to customize each message and pose as family members, friends or colleagues.

"These are very, very targeted campaigns," he said. "It's important to understand that you are the target, not just your computer."

Practice technology mindfulness

You probably think of mindfulness as something better suited to your yoga mat than your inbox, but Wright's research shows that mindfulness training is 38 percent more effective in preventing hacks than traditional anti-phishing training.

That number comes from field experiments Wright and his colleagues conducted at a large organization, sending their own phishing emails to one group trained in mindfulness techniques, one trained in traditional cue-based techniques (i.e. looking for suspicious subject lines, spelling and other cues) and one control group with no training.

"Cue-based training is certainly better than nothing, but the mindfulness training improved results by about 38 percent," Wright said. "When hackers are just looking for one click, that is a pretty significant number."

While cue-based training teaches users to look for a long and often-changing list of email characteristics, mindfulness training focuses on getting users to "stop, think and then act" before clicking something, trusting their instincts if something feels wrong.

"Even the briefest pause alerts your instincts, leading to a better decision the majority of the time," Wright said. "We often use technology fairly mindlessly; if you pause and are more mindful for just a second, then you have already won."

Rely on your co-workers

Wright calls it "the human firewall" – the web of human relationships and interactions that can make it that much harder for hackers to breach an organization. It consists not just of information technology personnel, but of coworkers who rely on each other to spot suspicious activity and communicate with the group.

"Our research has shown that people are far more likely to go to their coworkers with a security question before they go to IT," Wright said. IT departments should encourage that behavior rather than discourage it, he said, and help key influencers in different departments spread correct information.

"If you get a weird email and turn to someone in the next cubicle to ask about it, you've already won," Wright said. "That kind of awareness spreads positive security practices throughout the organization."

Read one cybersecurity news article every quarter

To increase your awareness of security risk, Wright suggests monitoring the popular press for cybersecurity news articles and reading at least one every quarter. Even that little bit of reading will help you stay aware and informed about the latest scams you are likely to see in your inbox, he said. And the higher your awareness, the lower your risk.

"The more security is front of mind, the better decisions people make," Wright said.

As a starting point, he recommends Krebs on Security, a website run by Washington Post reporter turned cybersecurity guru Brian Krebs.

Provided by University of Virginia