Expert explains the alarming creativity of today's cyberattacks, and five unlikely places you're vulnerable

January 30 2024, by Maggie Haslam

The increased sophistication of cyberattacks through social media platforms, computer hardware, smart devices and popular websites demands more care in how we engage the internet, says Associate Research Professor Charlie Harry. "At the end of the day, we should all expect the worst and have an action plan for recovery." Credit: Valerie Morgan/University of Maryland

Associate Research Professor Charles Harry likes to strike up

conversations with his new students by asking about their pets: Their favorite memories, the name of their first pet, even if they chose the collar based on their favorite color. Most don't hesitate—after all, he's their professor.

But what if the question comes by email or social media post—and despite all appearances it's not really Harry asking? What many students don't realize is that they've just surrendered two potential password challenge questions.

Being mindful about the information you share, from your birthplace in a social post to professional qualifications on LinkedIn, is critical as cyberattacks become more nuanced, said Harry; and we should all expect the worst. A former National Security Agency cyberwarfare expert and director of the University of Maryland's Center for Governance of Technology and Systems, Harry has made it his mission to educate not just students, but CEOs, government leaders and other novices in understanding and identifying their risk to a cyberattack.

Harry's "Cybersecurity for Everyone" is the most popular UMD massive open online course (MOOC) on the continuing education website Coursera, with more than 500 enrollments per day globally. Harry's most recent endeavor with colleagues and students from the College of Information Studies and School of Public Policy developed "attack surface maps" for state government leaders: tools that for the first time reveal county government vulnerabilities in every municipality nationwide, arming them with the intel to preempt cyberattacks, rather than just react to them.

"My goal is to get people seeing cybersecurity in a very interconnected way," he said. "All this stuff—laptops, phones, cloud systems—is widely dispersed geographically but it all works together. And so, you have to understand the big-picture view of this problem, and how a vulnerability

in just one device can cascade into something widespread."

Cyberattacks have gotten much more sophisticated and complex over the past 15 years, he said, with "black hat" hackers specializing in writing malware or gaining access working together across criminal enterprises. According to Harry, cyberthreats shouldn't just be keeping Gov. Wes Moore or a Fortune 500 executive up at night—anyone who connects to a commercial, government or institutional website is a point of entry to a potential payout.

"You may not have access to the most sensitive information, but what you do have is access to the network," he said. "You're a conduit to what they want to get."

Faculty and staff are required to sit through UMD's security awareness training, "Defend Your Shell," by the March 1 deadline—but your inbox isn't the only place where potential threats lurk, said Harry. Below, he shares a few unlikely places vulnerable to a cyberattack:

- Popular websites. Think twice before you click that ad on the margin of your favorite website. "Malvertising," or nefarious ads on trustworthy websites that redirect readers to malicious websites or install malware on their devices, is an increasingly popular tactic with cybercriminals. "It's pretty sophisticated," said Harry. "You didn't click on a suspicious email; you just went to a website."
- LinkedIn. Self-promoting on this platform can be key to finding your dream job—but depending on where you currently work, it could also make you the perfect candidate for a social engineering attack, said Harry. That recruiter link to upload your resume might actually be a tactic for installing malware on your computer, accessing your login credentials and gaining access to your company's network. "It's not necessarily about your

position, although hackers do look at that too; they are big on researching who does what," he said. "But ultimately it's about access. If you touch the network, you could potentially be a way in."

- Your boss. Deepfake and generative AI have revolutionized the practice of extorting information and money, said Harry. Criminals can effectively capture and mimic people's voices—such as your boss, or even your kids or grandkids—convincing people to share sensitive information like social security numbers or passwords. "I'm not saying to always be questioning these things, but you have to be a critical thinker. This is quickly becoming run-of-the-mill criminal activity."
- Flash drives. While it's become less of a problem, that free flash drive you pick up at a convention can still be a distributor for malware. "You should consider anything given to you might be problematic" when it comes to computing hardware or software, he said.
- Your printer. The constant software updates pinging your devices are a drag, but serve an important purpose. "These companies push them out when there's a security vulnerability," said Harry, who recommends not clicking "remind me later" on updates to computers or other smart devices; if it's connected to the internet, it's a way in.

Provided by University of Maryland

Citation: Expert explains the alarming creativity of today's cyberattacks, and five unlikely places you're vulnerable (2024, January 30) retrieved 12 May 2024 from https://techxplore.com/news/2024-01-expert-alarming-creativity-today-cyberattacks.html