FIVE THINGS WE CAN

CYBERSECURITY involves more than thinking up complicated usernames and passwords. With many turning to apps and websites for everything from managing their finances to monitoring their health, the risks and consequences of compromised security in the digital realm have never been greater or potentially more devastating.

How secure are you online? Professor Yan Chen suggests five behaviors that can help make you more cybersecure.

1

PRACTICE EMAIL AWARENESS

If you've ever managed an email account, you already know about the inevitable stream of scams that can arrive in your inbox. While messages from desperate "foreign dignitaries" may seem easy to recognize and disregard as phony, many users still fail to practice sound judgment.

Advanced fee scams that ask unsuspecting users for immediate financial payment online in exchange for future riches exist only to enrich the fraudsters who perpetrate them. The ubiquitous "Nigerian prince" email scam duped people out of $12.7 billion in 2013 alone, according to research group Ultrascan AGI.

"Social engineering attacks like email scams remain one of the most common forms of cyber attacks," Chen explains. "People continue to fall victim to emails that appear superficially attractive but are really just asking for your credit card number or acting as a delivery mechanism for installing a malicious email attachment."

To avoid becoming the next victim of an advanced fee scam, Chen recommends against sharing any confidential information by email. With banks, online stores, and other reputable institutions implementing heavily secure online portal systems to conduct customer activity, you're fairly safe in assuming that any email message asking for financial information—no matter how intriguing its reasoning—does so with an ulterior motive.

2

GET EDUCATED

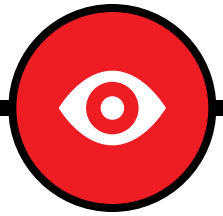
For many users, education is the best defense against cybersecurity risks. Chen notes that increasingly, elementary and high school curricula include cybersecurity lessons for students. That's no surprise. A 2013 study from independent watchdog group Common Sense Media found that nearly three-quarters of children under age eight had regular access to a smartphone or tablet.

Universities have also begun to bolster their course offerings similarly. Northwestern Engineering's Department of Electrical Engineering and Computer Science recently launched its Digital Forensics and Incident Response course, which uses case studies inspired by real cyber attacks to teach students how to recognize and address data breaches.

For those who don't have access to formal cybersecurity education, Chen says that media coverage of cybersecurity news offers an effective crash course. "When news media cover major cybersecurity attacks, they inevitably follow up with security experts who offer recommendations for becoming more cybersecure," Chen notes. "At the very least, you learn how to avoid making the same mistakes as the victims in the news."

DO TO BE CYBERSECURE

3



WATCH YOUR APPS

Consumer research giant Nielsen reports that in 2014, US smartphone users spent an average of 14 hours more per month using apps than they did just two years earlier. As mobile app interactions increase, exposure to pop-up and latent advertising found in many apps poses a growing cybersecurity risk: when clicked, these ads can transport users out of the app and onto the web, where viruses and other malicious content may lie in wait.

Chen recommends practicing caution before clicking on ads within an app—especially ads that ask you to download a program. No app is resistant to linking to potentially malicious content.

To mitigate this risk, Chen and his research team have developed a dynamic detection system for Android phones that pinpoints dangerous ads and reports how they reached the user. While he emphasizes security throughout the app development process, Chen thinks the new technology can help developers address the risk inherent in such advertising.

"Security often lags when there is a rush to get an app or product to market," he says. "Unless developers have witnessed or experienced an attack first-hand, they may remain passive when it comes to incorporating the necessary security measures."

4

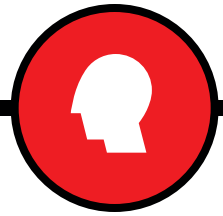
GUARD INFORMATION SYSTEMS

As an individual, you can do little to protect your confidential information from a cyber attack on a retailer that has your data stored in its system. But you can certainly guard your confidential information on a personal level. For starters, Chen recommends maintaining comprehensive virus and malware protection software across all devices, from laptops to smartphones and tablets.

"No protection system is perfect, but many are equipped to recognize and thwart most viruses and attacks," Chen says. "The right software can do a lot of the work for you."

Another way to protect your devices is to exercise diligence when downloading software updates. While it may be tempting to close pop-up windows that notify you about new updates for your operating system or app, Chen says those updates often have as much to do with improving security capabilities as they do with offering new software features.

5



ADOPT A PROACTIVE MINDSET

Beyond developing better personal cybersecurity habits, Chen advocates supporting larger societal efforts to improve the cybersecurity standards at an industry and governmental level. "The challenge of improving cybersecurity isn't a technical one," he says. "There are still advanced attacks targeting large-scale institutions, but they represent a minority compared with overall cybercrime. The majority of attacks target known vulnerabilities for which patches exist. People just don't use them."

Reactively addressing security threats once a product reaches market jeopardizes customers. Instead, companies should emphasize the importance of recognizing vulnerabilities at the outset of development.

Government also has a role to play. In addition to fully enforcing existing cybersecurity protection laws, it can enact new legislation to set even more stringent standards for hospitals, universities, and other major institutions to ensure they have appropriate safeguards in place to protect their very sensitive data.

"It will take time before we can educate everyone about cybersecurity," Chen says. "A new mindset, coupled with improved legislation and better enforcement, can speed up our progress."

Written by Alex Gerage