What's your student cyber security strategy?

When institutions take on the responsibility of preparing students to protect themselves against cyber crime, everybody wins

In 2020, the Federal Trade Commission convinced a federal court to shut down several companies that had bilked thousands of college students and recent graduates out of a combined $23 million. Dangling promises of reduced debts, the companies had convinced the victims to let them take over as their loan servicers. But then the companies charged fees and kept all or most of the students' monthly payments. They kept the ruse going for months, and in some cases years, by obtaining the students' Department of Education login credentials and changing their contact information.

Most college and university leaders are aware that higher education is an increasingly attractive target for cyber criminals. But they may not realize that it's not just the institutions, but students too who are facing more frequent, varied and sophisticated threats. Untold numbers of criminals are out to steal students' money, identities, or both, and most students are not prepared. Their parents and previous teachers were, understandably, focused on threats like cyber bullying and online predators. Colleges and universities can help their students learn to avoid online fraud, just as they've long counseled them about street crime and shady landlords.

Today's college students have grown up online, it's second nature to them. That engenders a natural trust that can prevent them from understanding some of the risks. That's compounded by the fact that they're probably away from home for the first time and making more important decisions for themselves. These circumstances make them ripe targets for criminals.

Like the loan payment scam described above, the most common schemes targeting students are not technically sophisticated, but cunning in that they push just the right buttons. For example, a cyber thief will post photos and details about a

> **Today's college students have grown up online, it's second nature to them. That engenders a natural trust that can prevent them from understanding some of the risks.**

BANK OF AMERICA

well appointed, affordable apartment close to campus, available today only with a deposit (and perhaps a completed application that asks for Social Security number).

Most scams involve some form of social engineering, a broad term referring to any attempt to trick the target into believing they're dealing with a legitimate entity. Students are easy to find because they post about their school affiliations on social media. Other examples focused on students include:

- Offers of scholarships or other forms of financial aid, or credit cards. These will lead to requests for upfront fees and/or personal information. (Sometimes the fraudsters' only goal is to collect contact information — for future scam attempts.)
- Unpaid tuition or fees warning. This will appear to be coming from the student's school and will warn of losing enrollment status if payment is not made immediately. Parents sometimes receive these as well (they also share information on social media that's useful to cyber criminals).
- Discounted textbooks or moving services: These are similar to the apartment scheme described above.
- Part-time jobs. Students are invited to apply for positions (often "work from home" scenarios) with flexible hours and good pay. The pitch often asks for an upfront fee. In some cases the scam works by sending the student a check, for say $1,000, and telling the student to then send their own payment of $500 to some other party. But then the student learns that the $1,000 check is fraudulent, and they are now responsible for the $500 payment.

Anxious, distracted students fall for these all the time (just as older adults are taken in by scams masquerading as messages from utility companies, banks and the IRS). As trusted sources with established channels of communication, colleges and universities are uniquely positioned to educate their students about the new perils awaiting them online.

The good news is, institutions also benefit from this.

An entire digital ecosystem can be impacted by the actions of anyone attached to it, and in higher education that includes students. The more that institutions can educate students, the safer overall their ecosystems will be.

There is no one way to approach this challenge, but the key is communicating early and often. Here are some more tips.

Set the right tone

Fear, shaming and nagging are not an effective motivators. Don't think of students as cyber security liabilities, the weak links in your defense. Think of them rather as allies on the front lines, who, when armed with information, are better able to defend the institution as well as themselves.

Most people respond better to explanations than to orders, and students are no different. Also, you never want to give the impression that the situation is hopeless. The message should be that the challenge is great, but by working together the campus community can keep everyone safe.

> Don't think of students as cyber security liabilities, the weak links in your defense. Think of them rather as allies on the front lines

Engage with students on their terms

Generation Z is famously hard to reach via traditional methods. Most institutions have adapted their recruitment, retention and other messaging efforts accordingly, adding texting platforms and chat bots to supplement the social media posts, emails and static web pages. A multi-pronged approach will be most effective in building cyber security awareness too.

This also requires ongoing effort, to remind students of what they've already learned and to keep them updated on emerging threats.

Universities have a wide variety of communication channels at their disposal, and should use all of them. This includes print publications like students newspapers and alumni magazines (remember, recent grads are also targets); flyers or presentations at the student union, book stores or on-campus IT centers; and booths at information fairs.

Faculty should also be encouraged to remind students about the need for vigilance. The more cyber security becomes part of the campus culture, the more effective the messages will be.

Keep it clear

IT professionals should not be solely responsible for designing the curriculum. It's a "curse of knowledge" situation: experts often can't remember what it's like not to know as much as they do, and unwittingly talk over novices' heads. The messaging should not assume prior knowledge of terms like phishing and malware. But at the same time, it's important not to talk down to students. Every incoming class is more technologically intuitive and savvy than the last, and can adapt quickly to change.

> experts often can't remember what it's like not to know as much as they do, and unwittingly talk over novices' heads. The messaging should not assume prior knowledge

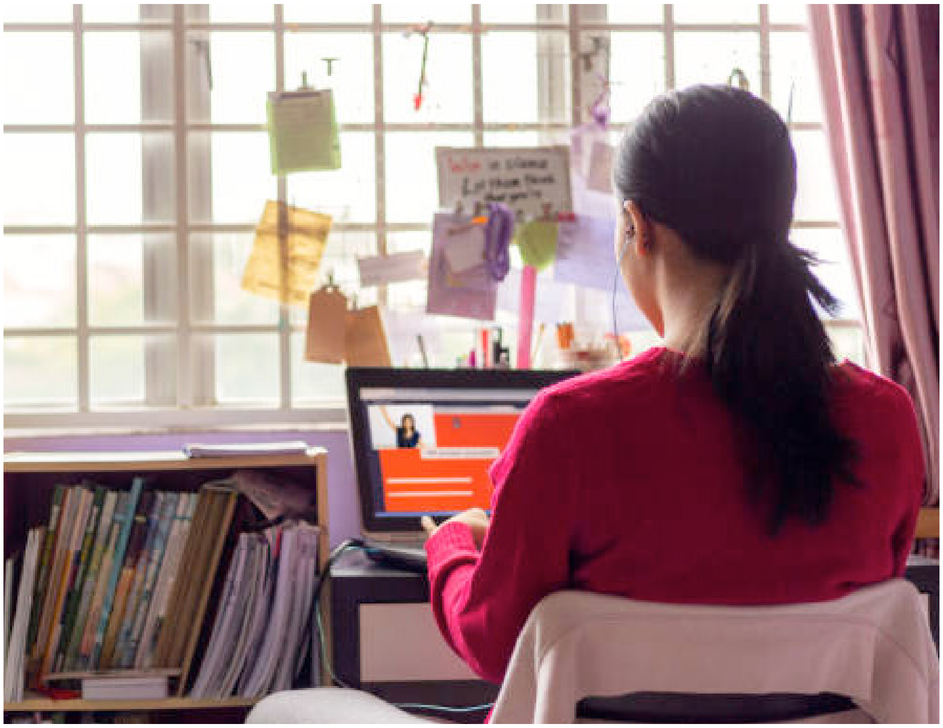
Student Affairs departments have a lot of experience communicating with students. Get that staff involved.

Don't forget to listen

Treating students as allies isn't just to flatter them — it's to learn from them. Encourage them to report successful and attempted scams — ideally to a designated office or web site — so that the information can be turned into an alert to the rest of the campus and made part of future messaging. (Every common scam was new at one time.) Don't use identifying information; the goal is not to embarrass, just to educate.

Again, the key is to communicate early and often with a clear message: Be cautious online. Pause before responding. If something sounds too good to be true, it probably is.

Students get caught up in their day-to-day lives, and will feel like the last thing they need is something else to worry about. But it's critical to reach them in these years, to prepare them for the immediate cyber security challenges and those of the workplaces they'll soon enter.



Neither Bank of America nor its affiliates provide information security or information technology (IT) consulting services. This material is provided "as is," with no guarantee of completeness, accuracy, timeliness or of the results obtained from the use of this material, and without warranty of any kind, express or implied, including, but not limited to warranties of performance, quality and fitness for a particular purpose. This material should be regarded as general information on information security and IT considerations and is not intended to provide specific information security or IT advice nor is it any substitute for your own independent investigations. If you have questions regarding your particular IT system or information security concerns, please contact your IT or information security advisor.

"Bank of America" and "BofA Securities" are the marketing names used by the Global Banking and Global Markets divisions of Bank of America Corporation. Lending, other commercial banking activities, and trading in certain financial instruments are performed globally by banking affiliates of Bank of America Corporation, including Bank of America, N.A., Member FDIC. Trading in securities and financial instruments, and strategic advisory, and other investment banking activities, are performed globally by investment banking affiliates of Bank of America Corporation ("Investment Banking Affiliates"), including, in the United States, BofA Securities, Inc. and Merrill Lynch Professional Clearing Corp., both of which are registered broker-dealers and Members of SIPC, and, in other jurisdictions, by locally registered entities. BofA Securities, Inc. and Merrill Lynch Professional Clearing Corp. are registered as futures commission merchants with the CFTC and are members of the NFA.

Investment products offered by Investment Banking Affiliates:
Are Not FDIC Insured • May Lose Value • Are Not Bank Guaranteed.