BANK OF AMERICA

Keeping higher ed students safe from cyber attacks

When colleges and universities educate and empower students to defend against cyber crime, they help protect both the academic population and the institution.

With today's college students facing more frequent, varied and sophisticated cyber threats, young people are increasingly likely to fall victim to cyber scams. In fact, the increase in cyber crime complaints from victims aged 20 and younger between 2018 and 2021 was greater than the increase in victims aged 60 and older — 63% versus 49%.[1] Gen Z digital natives have a level of trust and ease with technology that older generations don't, which can make them more careless, and for criminals, the payload for scamming a student can be access to a target-rich university environment.

Higher education IT and security leaders are realizing that colleges and universities are increasingly attractive targets. As they put technology and processes in place to protect their organizations from cyber attacks, they're finding that it's not just the institutions themselves, but also the student population that's being bombarded with everything from ransomware to financial aid fraud. Higher ed institutions have the additional responsibility to keep the student body secure as well as educate their students about the dangers that come with technology use — and empower them to be part of the solution.

> Cyber crime against 20-year-olds and younger increased 63% between 2018 and 2021 — versus just 49% for ages 60 and up.[2]

Key takeaways

- Colleges and universities are trusted sources of information and are uniquely positioned to educate their students about cyber crime. There are five best practices for that curriculum:
- Collaborate: Build alliances with students. Make it a "one team" approach.
- Communicate: Speak with students on their terms and at their level.
- Motivate: Incentivize students with rewards and gamify cyber security training.
- Empower: Include students in cyber crime detection and planning processes.
- Listen: Stop lecturing and remember students can teach as well. Hear their concerns.

[1] FBI Internet Crime Complaint Center, "2018 Internet Crime Report" and "2021 Internet Crime Report."

[2] Ibid.

Recognizing the scams

As digital natives, college students are so comfortable with technology that it's easy for them to overlook the risks. This is compounded by the fact that many are new to living independently and managing their own finances and technology for the first time. To help protect students from becoming victims, it's critical to keep them informed about the different types of threats targeting them. Most scams involve social engineering tactics like phishing (and voice and text variants, vishing and smishing) but use different lures to draw students in. Here are some of the more common scams:

Student loan debt relief scams

With several student loan forgiveness programs available from the U.S. Department of Education,[3] fraudulent websites, emails, texts and phone calls from companies purporting to help students reduce or eliminate their student loans are proliferating. These scams may try to steal personally identifiable information (PII) or trick victims into making unnecessary payments. The FBI issued a warning in October 2022 against federal student loan forgiveness fraud schemes.[4]

Fake real estate and housing listings

Targeting students looking for off-campus housing or roommates to share rental costs, fake real estate and housing scams take advantage of young students who are often first-time renters, trying to find housing from a distance (overseas or out of state), or scrambling to find a rental on short notice before the start of the school term. Some scammers impersonate landlords and fraudulently take security deposits on properties they don't own (and that aren't available). Other times, they may pose as potential subletters and use a common overpayment scam where they appear to send a payment for more than the deposit or rent is and ask the student to transfer the difference back to them. Scams offering moving services or even discounted textbooks may use similar overpayment tactics.

Fake employment offers

With many students looking for part-time jobs, scammers can lure them into applying for non-existent positions by offering enticing "work from home" scenarios or flexible hours. Like housing scams, these often use false fees or overpayments to defraud students. Overpayment scams are the result of falling prey to social engineering and can involve various methods of payment — be it peer-to-peer payment services, credit cards or checks.

Social media scams

As students enter new social circles, the risk of falling victim to social media fraud can increase. Scammers may set up fake profiles or business accounts and attempt to collect PII or trick them into downloading malware, use fake social media ads to steal payments or donations, or find ways to hack into and take over email or social accounts and use them to target others.

Fraudulent financial aid offers or credit card scams

Appealing offers of scholarships, grants or other forms of financial aid, as well as fake credit card or bank account applications, can trick new students into paying fraudulent upfront fees or be used to collect personal information. Similarly, students may receive fake unpaid tuition warnings that appear to come from the university, and demand immediate payment and threaten loss of enrollment.

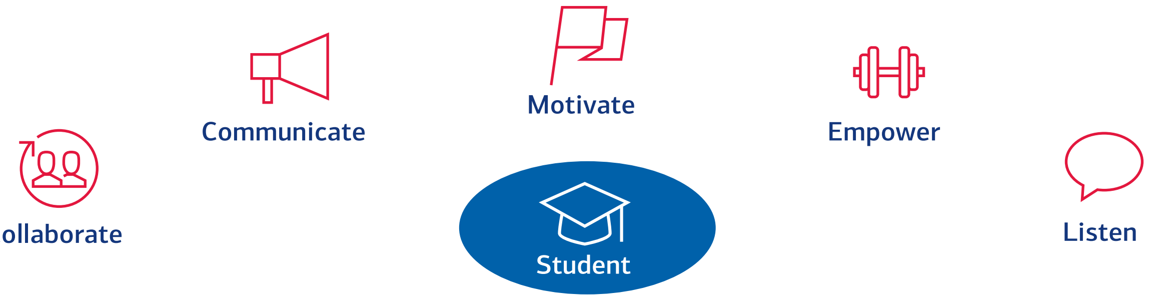
> By marshaling all the populations of a university — administrators, faculty, students, etc. — you can create a large and diverse cyber security team.

[3] U.S. Department of Education Federal Student Aid, "Student Loan Forgiveness."

[4] FBI, "Potential Fraud Schemes Targeting Individuals Seeking Federal Student Loan Forgiveness," October 2022.

Best practices for keeping students safe

As trusted sources of information, colleges and universities are well positioned to educate their students about the ways in which they and their schools are targeted by cyber criminals. With established student outreach organizations and a wide variety of communication channels available, sending your student body messaging about cyber security isn't likely a problem. But getting their attention and engaging them as part of your cyber security defense could be more difficult. These best practices can help to keep your students' attention on cyber defense:



1. **Collaborate: Build alliances with your students.** Rather than treating your students as cyber security liabilities by sending constant warnings and unilateral mandates, setting the right tone and building alliances with your students can help keep them engaged as a key part of your cyber security defense. By marshaling all the populations of a university — administrators, faculty, students, etc. — you can create a large and diverse cyber security team.

2. **Communicate: Connect with students on their terms.** Don't rely on a single method of communication to connect with your students. According to one study, 18- to 24-year-olds have a 1.3-second active attention span.[5] Gen Z students respond better to concise, visual communications. Use a multipronged approach incorporating social media and newer platforms for communication and take advantage of existing student portals and apps that they already use to search for information.

3. **Motivate: Provide incentives to students.** Reach out to students when they are most engaged with the institution (e.g., orientations, sporting events and other campus-wide activities) and consider using informational but fun and competitive games as ways to engage students in cyber training, such as phishing tests. By offering rewards (think visual badges or even school spirit gear) rather than setting strict training requirements, you can engage students more effectively. Additionally, offering paths for student recruitment to cyber security career opportunities can help educate and provide motives for their participation.

4. **Empower: Include students in your detection and planning processes.** Students can be the first line of defense against existing cyber crime techniques as well as the first to recognize the latest scams that arise. Provide students with the tools they need to be a part of your security framework by making sure they know where to report security threats (such as phishing attempts, for example) and be sure they receive feedback when they do so. Partnering with and engaging them in your ongoing efforts to detect new threats and protect the university's digital ecosystem can not only help educate students on how to best defend themselves, but it can also keep them engaged in helping you build a culture of cyber security awareness.

5. **Listen: Stop lecturing and remember to learn from your students.** Encouraging students to report their experiences, including successful and attempted scams, isn't just about empowering them. They can provide critical information to help you stay on top of new threats. Their understanding of the latest social media trends can help you stay more current than traditional research organizations can. Students are often also the first to hear about new methods of social engineering, so their input can be invaluable for educating the rest of the university population.

Continued diligence and partnership across the institution are the keys to a cyber-secure campus environment. With better awareness of the risks across campus, and a proactive dialogue with your students, the risk of cyber crime is minimized — a worthwhile goal for all.

[5] OMD Worldwide, "OMG and Yahoo: When Consumers Pay Attention to Ads, When They Don't," August 2022.

"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**	**Are Not Bank Guaranteed**	**May Lose Value**