SOFTWARE

# What Universities Can Do to Limit the Cybersecurity Risk of Personal Devices on Campus

## As the number of personal devices increases, universities will have to protect against an incoming threat to network security.

by Elliott Levine

Elliott Levine is Director of Education for the Americas Region of HP, Inc. and the company's first Distinguished Technologist focused solely on edtech. A former K-12 district administrator and professor, Elliott is a past columnist for Electronic School and American School Boards Journal.

On any college campus today, there are likely at least three devices for every one student or faculty member. **Laptops, smartphones, tablets, printers, watches** — all are synonymous with the modern college experience.

As of 2018, 73 percent of adults in the U.S. own computers and **53 percent** have tablets, according to the Pew Research Center. Among Americans ages 18-29 years old, **94 percent** own a smartphone, and roughly 4 out of 10 people in this age group report they are online "almost constantly."

Devices are everywhere and people are always online, which makes security imperative. When "bring your own device" (BYOD) is the name of the game, however, cybersecurity is a profound challenge for university campuses.

## Doing More to Secure BYOD Environments

Institutions of higher learning should get ahead of potential cyber problems by educating everyone. Training alone may not solve the entire problem, but it is **still critical to provide people with general cybersecurity best practices**.
This includes not clicking on email links from unknown sources, which can lead to phishing attacks, and not connecting to unknown Wi-Fi accounts, which can allow nearby hackers to penetrate devices.

It is also the responsibility of university IT staffs to **enforce reasonable security policies**. For example, they can set limits on the types of operating systems, memory, storage and processing even while encouraging online access to network resources.
Another precaution institutions can take is requiring students and faculty to register every device on campus so any unit, whether it is a **laptop, smartphone or even a gaming console**, can be mapped back to its owner.

Students and faculty will bring their own devices to campus; this is a fact of campus life. Savvy universities will head off cyberthreats with a balanced program of training, security policies and technology security solutions.

## Common Reasons Hackers Target University Networks

Hackers target institutions of higher learning for three common reasons: identify theft, espionage and notoriety. Because of this, campus IT departments need to be **especially proactive about securing mobile and connected devices** against the variety of threats BYOD presents.

- **Identity Theft:** Many students are just getting their first credit cards, checking accounts and loans. Their inexperience makes them especially vulnerable. When creating or accessing accounts using unsecure, connected devices, students often expose sensitive financial data — such as Social Security numbers, ATM codes and computer passcodes — to the digital world. Because students do not have much of a transaction history, attacks can be more difficult to spot. College-aged students are three times more likely to lose money from fraud than older adults, according to a 2018 Federal Trade Commission report.
- **Espionage:** When imagining espionage scenarios, we do not often think of universities. The truth is, they are becoming prime hacking targets because of personal data and valuable research that are inadequately protected. While it is nearly impossible in most cases to clearly tie such incidents to devices students and faculty bring onto campus, it is highly likely they play at least some role.
- **Notoriety:** Money and information are prime draws for hackers, but one of the longest-standing drivers continues to be the thrill of undermining networks for sport. This reason has become more prevalent with so many tempting connected devices on campuses globally. Many hackers are willing to show off their skills in sanctioned places, such as sponsored hackathons or "white hat" hacking events, such as the annual DEF CON conference in Las Vegas. Still, about 11 percent of unauthorized attacks against universities are "just for fun," according to Verizon's "2018 Data Breach Investigations Report."

https://edtechmagazine.com/higher/article/2019/03/what-universities-can-do-limit-cybersecurity-risk-personal-devices-campus