CAMPUS TECHNOLOGY

by Phineas Dowling

Securing Your Network: The Greatest Vulnerability is the Human Factor

When we picture "hacking" we might have an image from movies of an individual, sitting in a dark room in front of several monitors, furiously typing. The movie *Hackers* (1995) features many such scenes; the first introduces the protagonist, Dade, who hacks into and takes over a television network. He is interrupted by another hacker; the two battle it out digitally with furious typing until the mysterious hacker terminates Dade's connection. Worth noting here is that Dade had gained access to the TV station's system initially by tricking a security guard into giving him information. Despite the absurdist overtones of the scene, one element is based on a truth: the human element makes the system most vulnerable.

Reducing Vulnerability

Network security is about reducing vulnerability through a variety of policies and practices to control and monitor access to a computer network. While this includes network and software solutions, such as anti-virus software, passwords, and firewalls, network security also depends on policies and training designed at keeping the human element of a network just as secure as the digital elements. Although private institutions are not subject to the same FERPA restrictions as public schools, network breaches can come with a number of financial, legal, and reputational liabilities.

A security hacker is anyone who exploits vulnerabilities in network security. The most common goal is to access data or to lock out access to legitimate users for profit. The most common target is personally identifiable information (PII). This is information relating to an identifiable person including names, birthdates, social security numbers, locations, email addresses, phone numbers, credit card numbers, etc.

PII is generally sold in digital black markets and used to commit identity fraud. According to Javelin Strategy & Research's annual identity fraud report, in 2017, 16.7 Million U.S. consumers were victims of identity fraud for a total of $16.8 Billion stolen. Javelin's 2019 report shows a general decline in victims but a marked "resurgence of higher-impact

fraud types such as new account fraud, account takeover, and misuse of non-card accounts."

More victims are being targeted directly and forced to pay out of pocket in response to security breaches and ransomware attacks, where a hacker takes over an account or device and charges a "ransom" for returned access. PII data theft can be a lucrative business for hackers and devastating to individuals and the organizations targeted in these breaches.

Viruses Exploit Vulnerabilities, in People and Digital Networks

There is no such thing as an "unhackable" network, but universities can reduce possible exploits in the system and minimize the risk of a data breach. Your institution is likely doing a great deal on the technology side—using a variety of software and services designed for network security, such as anti-virus software and firewalls.

A major risk for most higher education institutions is that faculty and students most often access the network from personal devices and often from outside of the network. Every personal device and each login from off campus represents a possible vulnerability.

Students and researchers still need to be able to access the network from off campus, however. To manage this risk, most universities license a Virtual Private Network (VPN). These VPNs allow users access data from a public network as if they were directly connected to the private network.

Amidst this experience with COVID-19, though some universities are better prepared than others, all campus leaders must develop a clear and immediate plan to fully address students' needs to access the campus network remotely, whatever the reason might be.

To reduce potential vulnerability when users access the network, your institution should use two-factor or multi-factor authentication. Two-factor authentication (2FA) requires a user to present two (or more) pieces of evidence to authenticate who they are before access is granted. Typically, this means logging in on one device and confirming the login on a separate device, such as a cell phone.

Security Hygiene

Software and technological measures only go so far, as the greatest vulnerability remains the users of a network. Truly reducing risk and maintaining the integrity of your network security at your institution requires comprehensive training for users on network security policies and practices.

Most of these practices fall under "security hygiene." Just as we are all reminded daily now of the importance of washing our hands thoroughly, these practices and routines are about making sure your network and devices are clean and healthy. Good security hygiene requires maintenance and vigilance.

Software and operating systems, for example, should be updated regularly. Updates are vital in reducing possible exploits for hackers. Likewise, setting up and maintaining a strong password to access the network. Strong passwords are hard to crack. It is also important to update passwords at least every three months, which can limit continuous or return access if there is a breach.

The importance of updates and passwords is pretty clear to most, but there are some aspects of security hygiene you might not have considered before. It is important to change your devices' default settings. The California Institute of Technology's Information Management Systems and Services warns that

Amidst this experience with COVID-19, though some universities are better prepared than others, all campus leaders must develop a clear and immediate plan to fully address students' needs to access the campus network remotely, whatever the reason might be.

many devices, printers, and other equipment arrive pre-configured with default administration credentials that are well-known and routinely tried by hackers.

Like in the scene from *Hackers*, however, the greatest vulnerability is the users themselves. In the movie, the hacker used "social engineering" to deceive the security guard into giving him the information needed to access the network. Social engineering Social engineering occurs when someone lies or uses manipulation to convince people to divulge information or perform actions.

Phishing is a similar deception in which someone tries to obtain sensitive information such as usernames, passwords and financial details by pretending to be someone trustworthy, usually through email. Links and email addresses can be spoofed to look legitimate, so it is important that users have the proper training to know what to watch out for.

Prevention and Recovery

Good network security is not just about prevention but is also about how you recover after a data breach. MIT also has a Data Incident Response Team (DIRT), which is on hand to assess and assist with recovery from information security breaches. Such teams help shore up the breach, reduce liability from the breach, and help prevent future breaches.

Network security is ever-evolving as new threats and new solutions emerge. In the near future, many businesses and institutions will likely adopt AI-powered network detection and response (NDR) solutions, which continuously scan a network for harmful data.

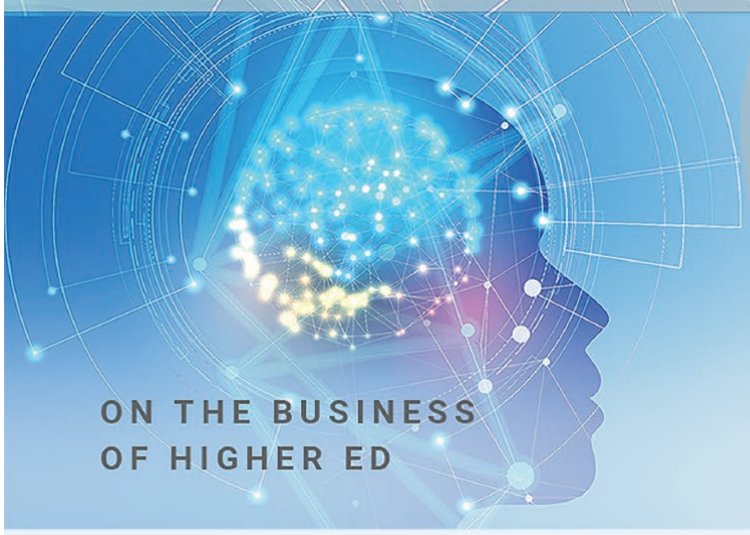
Another solution that institutions will likely deploy soon is "zero-trust security." A zero-trust model of network security, according to Microsoft, "assumes breach and verifies each request as though it originates from an open network." Essentially, such a model is based on continuous authentication at multiple levels every time a device or user accesses a resource.

Although there are new procedures and policies developing every year to confront new challenges as they emerge, the best defense will always come down to how you prepare your people. Thorough systems and practices, a robust suite of technological solutions, a risk-mitigating data classification plan, and comprehensive training will help limit vulnerabilities and protect your institution and your students.

ABOUT THE AUTHOR: Phineas Dowling is a PhD candidate in literature at Auburn University where he teaches literature and composition. His dissertation is on Scottish identity and British literature of the long eighteenth century. In addition to his scholarship, Phineas has a strong interest in pedagogy and university administration.

FOCUS

touchnet
A Global Payments Company



ON THE BUSINESS
OF HIGHER ED

BOB MASK
COLORADO SCHOOL OF MINES

Get More Out of Your Campus ID

Enjoy this summary of a recent FOCUS podcast in which Bob Mask shares his creative methods for getting even more out of the campus ID system at Colorado School of Mines.

Bob Mask, director of campus card services at the Colorado School of Mines, explains how his campus uses credential cards for more than just identification. He outlines how individual electronic cards are used throughout the summer for many on-campus events and camps with a variety of attendees and visitors. Mask highlights the convenient functions of the cards from building access to mealtime checkout and the variety of benefits.

In partnership with Student Conference Services, Mask and his card services team are tasked with running logistics for 30 summer events or camps that bring in over 2,500 visitors each year. Each campus visitor uses housing and/or dining services. To grant building entry access to each visitor, proximity cards are programmed to the correct buildings that each visitor needs access to. The card also allows access on a floor-by-floor bases. The cards run on a number system, so when a staff member looks at a proximity card, they know exactly which buildings and floors the card is attached to. Having this information encoded through a number system is an additional layer of security if the proximity cards are lost or stolen.

In an effort to streamline the dining process, Colorado School of Mines created a "summer conference meal plan" that is attached to each of the proximity cards. By utilizing the TouchNet meal system, they have been able to create a block plan that allows for a single swipe for each meal for each day for each card. It helps control how often the card is used and is trackable when the card is used. The block plan is still flexible enough for groups to work with food service for specific needs. This method makes it very easy to estimate accurate billing and costs for each group based on their time spent on campus. The inspiration for this process came from the dining process at Disney resorts. It is all centered around the convenience needs of short-term summer visitors and campers.

By combining building access and dining plans on a single proximity card, Colorado School of Mines is able to streamline security and meal billing. Mask and his team have saved both time and resources, as well as cut down on human error and turnaround time between summer groups, by implementing this new card process.