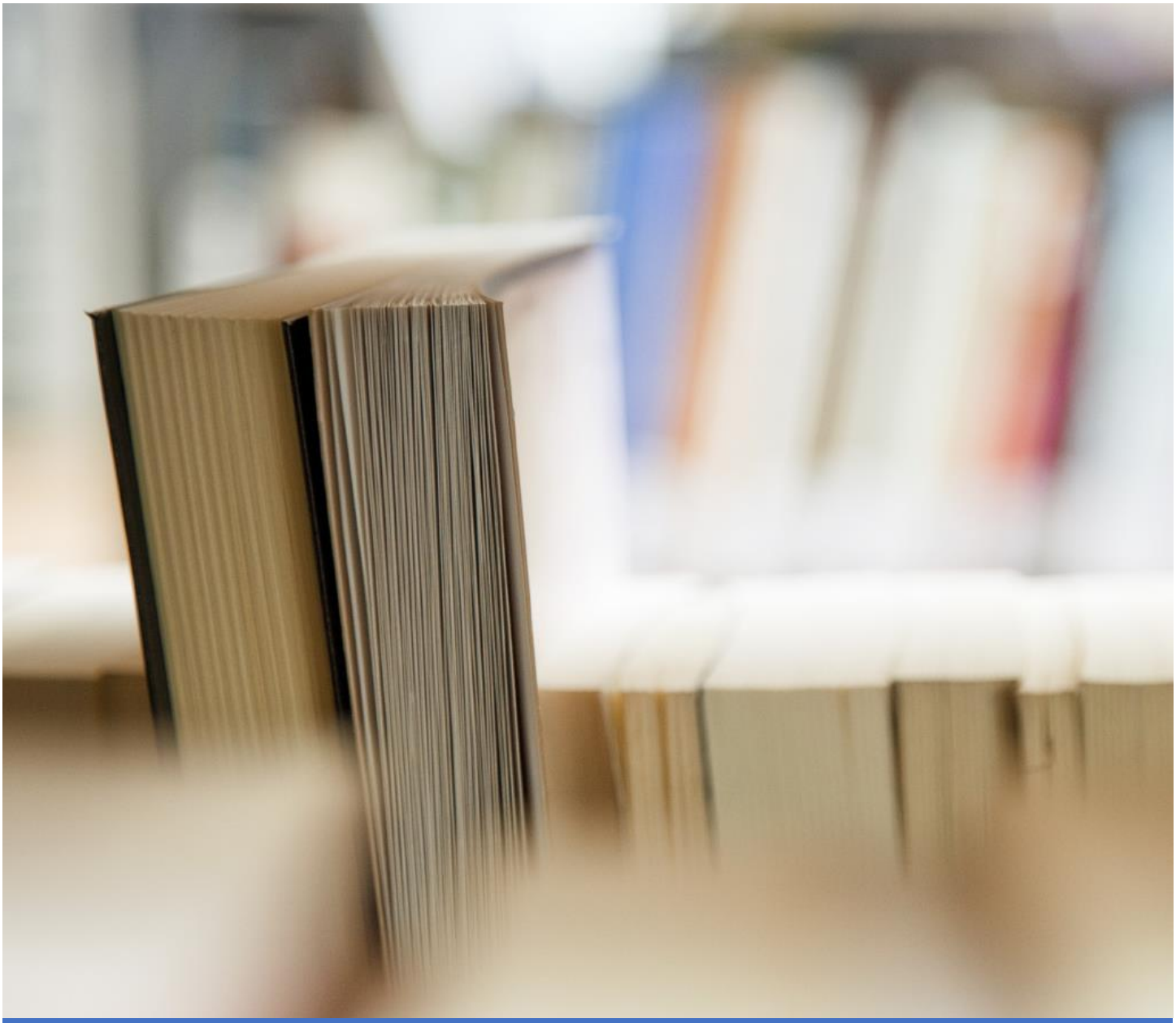

Cyber Safety for College Students

Essential Tips for Staying Protected Online

By Eric N. Peterson

For Dae

Table of Contents

Cyber Safety for College Students: Essential Tips for Staying Protected Online

College students face various cyber threats due to their frequent online activities, combined with the open nature of many university networks. This short eBook will describe why college students are:

- A target.
- The most common attack types.
- Real-world use cases.
- Best practice solutions.

Why College Students are a Target

College is where independence, technology, and sharing knowledge all come together. College is a big change in the lives of many young people. It's a time when they become more independent and immerse themselves in technology. There's also a culture of being open and sharing information. Even though these things are good for personal growth and building relationships, they also make college students easy targets for hackers.

1. Independence and Inexperience:

As students leave the safety of their homes, many are taking care of their own things for the first time on themselves. Most of the time, this independence comes without the knowledge needed to spot possible cyber threats. This mix of financial independence and lack of experience makes people vulnerable to being taken advantage of, whether they are handling bank accounts, signing up for new services, or buying things online.

2. Ubiquitous Technology Use:

Tech-savvy people live and work on college campuses. Students use devices like laptops, smartphones, smartwatches, and tablets for school and home use. With so many devices, there are more chances for attacks, especially if the devices aren't protected or if students don't know how to keep their devices safe.

3. Open Network Environments:

Universities often have large, open network infrastructures to meet the different online needs of students, teachers, and administrative staff. Even though these networks make study and communication easier, they can also be easier to break into than corporate or home networks.

4. Culture of Sharing:

Today's college students have grown up in the digital age, where it's common to share personal moments, academic successes, or even random thoughts on platforms like Instagram, Twitter, or Facebook. Even though this culture encourages connection and speech, too much sharing can give cybercriminals personal information that can be used to scam, phish, or steal a student's identity.

5. Valuable Data:

Universities and their students deal with a lot of important information, from study and new ideas to personal information and financial data. Cybercriminals know how valuable the data could be, whether they want to sell it, use it for ransomware attacks, or use it in other bad ways.

6. General Trust & Experimental Mindset:

College settings often encourage trust, working together, and being open to trying new things. Even though these are good qualities, they can sometimes make it hard to know when to be careful. Students might download school materials from sources that can't be checked, join unsafe networks for group projects, or try out new software without thinking about the security risks.

In conclusion, college students live in a world full of opportunities and information. However, the fact that they are independent, use technology, and believe in sharing makes them more vulnerable online. It shows how important it is for schools to put cybersecurity education first, giving kids the knowledge and tools, they need to stay safe in a world that is becoming more and more digital.

Understanding the Threat Landscape

Common cyber threats for college students include: Phishing, malware, ransomware, and social engineering. Here are definitions as well as examples.

Phishing:

Definition: Phishing is a cyber-attack where perpetrators attempt to trick individuals into divulging sensitive information, such as login credentials or credit card numbers, by masquerading as trustworthy entities in electronic communication.

Example: An email that appears to come from a trusted bank asking users to "click on a link to verify their account details." Once the user clicks on the link, they are directed to a fraudulent website designed to look like the bank's authentic website, where they are prompted to enter account information, which is then stolen by the attackers.

Malware:

Definition: Malware is a general term for malicious software that is specifically designed to disrupt, damage, or gain unauthorized access to computer systems. It encompasses various types of harmful software such as viruses, worms, trojans, and spyware.

Example: A user might download a seemingly harmless software from the internet, only to find out that it covertly installs a trojan, which then allows attackers to access and control the user's computer remotely.

Ransomware:

Definition: Ransomware is a type of malware that encrypts a victim's files or locks users out of their systems. The attacker then demands a ransom from the victim, promising to restore access or decrypt the files upon payment, although there's no guarantee they will do so.

Example: A user receives an email with an attached document claiming to be an invoice. Upon opening the attachment, the user's files are encrypted, and a screen displays a message demanding payment (usually in cryptocurrencies like Bitcoin) in exchange for the decryption key.

Social Engineering:

Definition: Social engineering refers to manipulative tactics that trick individuals into divulging confidential information or performing actions that compromise security. Unlike other cyber-attacks, which exploit software vulnerabilities, social engineering exploits human vulnerabilities.

Example: An attacker calls an employee posing as IT support, claiming they need the employee's password to perform a critical system update. Trusting the caller's supposed identity, the employee shares their password, inadvertently granting the attacker access.

In all these scenarios, the common theme is deception. Cyber attackers are constantly evolving their tactics, relying on both sophisticated technology and human psychology to achieve their malicious goals. Awareness and education remain crucial in recognizing and preventing such threats.

Real-life stories

The cyber-attacks above can be found in real-life college stories from all over the country.

Phishing Attacks:

> Students often receive fraudulent emails posing as university services, asking them to click on links or download attachments, which can lead to data theft or malware infections.
>
> Example: In 2019, students of Oregon State University were targeted by a phishing scam that compromised 636 student records.

Ransomware:

> This is a type of malicious software that encrypts the victim's data, demanding payment to unlock it.
>
> Example: In 2020, the University of Utah faced a ransomware attack and paid a ransom to prevent student information from being released.

Public Wi-Fi Eavesdropping:

> Unsecured or poorly secured campus Wi-Fi can be a hotbed for snooping, potentially allowing cybercriminals to intercept data.
>
> Example: Though specific stories for colleges may be less publicized, the threat remains well-documented across various public Wi-Fi networks.

Identity Theft:

> With the amount of personal data students share online, identity theft can occur, leading to fraudulent activities under the student's name.

Example: In 2018, the U.S. Department of Education warned about a malicious campaign targeting students' personal data.

Social Media Scams:

Fake profiles or deceptive links shared on platforms popular among students can lead to scams or malware.

Example: Scams, such as the "Secret Sister" gift exchange, have spread on social media, targeting younger users.

Adware and Spyware:

These can be unintentionally downloaded, tracking online activities, displaying intrusive ads, or gathering data without consent.

Example: While not limited to students, the risk is heightened with the number of software and tools often downloaded for academic purposes.

Tailgating or Unauthorized Access:

Unauthorized individuals may physically access restricted areas by following students closely.

Example: There have been instances across colleges where individuals gain access to labs or rooms to steal devices or data.

Doxing:

The act of researching and broadcasting private information about an individual without their consent, often as a form of revenge.

Example: While specific instances may not be widely reported for privacy reasons, the phenomenon is known to impact students involved in online debates or social media disputes.

It's important for students to stay informed about these threats and practice safe habits both online and offline. Being aware and taking preventive steps can significantly reduce the risks associated with these cyber threats.

Recommendations & Solutions

Phishing Attacks:

Solution: Always verify the sender's email address. Be wary of unsolicited communications, especially those urging immediate action or requesting personal details. Avoid clicking on links or downloading attachments from unknown sources. Being wary of "too good to be true" deals and offers targeting students. Universities usually have official channels to communicate critical information, so when in doubt, verify directly with the institution or organization.

Ransomware:

Solution: Regularly back up all important files to an external drive or cloud storage, keeping them separate from your main system. This ensures that you can restore your data without paying a ransom. Additionally, avoid downloading software or opening attachments from unverified sources. Additionally, apply regular software updates and recognize and avoid malicious apps.

Public Wi-Fi Eavesdropping:

Solution: Avoid accessing sensitive accounts or conducting financial transactions over public Wi-Fi. If necessary, use a Virtual Private Network (VPN) to encrypt your online activities, ensuring they remain private, even on open networks.

Identity Theft:

Solution: Use strong, unique passwords and enable 2FA/multifactor authentication for any accounts or applications that allow it. Utilize a password manager and never reuse passwords. Securely store any sensitive documents, especially those that contain personal information. Protect your student ID, key fob and any campus portals. Recognize secure e-commerce websites and monitor your bank statements and credit reports regularly for any suspicious activity. Be cautious about the personal information you share online, especially on social media.

Social Media Scams:

Solution: Be skeptical of too-good-to-be-true offers or sensational stories shared on social platforms. Verify the authenticity of any unexpected friend requests, as scammers sometimes impersonate acquaintances to spread malicious links or solicit information.

Adware and Spyware:

Solution: Install reputable antivirus and anti-malware software on your devices. Periodically run scans to detect and remove potential threats. Only download software or apps from verified, trusted sources.

Tailgating or Unauthorized Access:

Solution: Always lock rooms or labs when leaving, even if it's just for a short duration. Be cautious of strangers asking to be let into buildings or facilities. It's okay to ask for their ID or direct them to a main entrance where they can check-in. Utilize campus resources for cybersecurity awareness and training.

Doxing:

Solution: Be cautious about the amount and type of personal information you share online. Adjust privacy settings on social media platforms to limit what is visible to the public. Consider using pseudonyms or usernames that don't link directly to your real name on non-essential platforms.

In conclusion, fostering a general attitude of skepticism and caution online can go a long way. Cyber threats often rely on exploiting human error, so taking a moment to think before acting can make a significant difference. Encouraging peer discussions about online safety can also help spread awareness and best practices among the student community.

We encourage your continued learning in the ever-evolving field of cyber security and cyber safety and sharing where you can. Good luck!

About the Author

Eric Peterson is a cybersecurity expert based out of SLC, UT, working in cyber operations. He directs and manages teams helping to keep companies' data and enterprises safe. He has over 25 years of experience in IT and Cybersecurity, an M.S. and B.S. in IT Security and assurance, and over 20 industry-recognized certifications, including CISSP, CISM, CRISC, and CISA. For more information, connect with Eric on LinkedIn or visit https://www.cypertipsguide.com/ for more eBooks and helpful cyber tips and guides.