Vice presidents for student affairs (VPSAs) and other senior-level student affairs leaders have high-level access to their institution’s information systems, which contain confidential information about students, faculty, and staff. This information could include, but is not limited to, personally identifiable information, personal health information, educational records, and financial information. Data breaches through unintended disclosures, inadvertent mistakes, or through phishing can lead to financial, personal, and reputation damages not only to student affairs leaders but to their institutions as well. The financial cost of mitigating data breaches may include notification of affected individuals, investigation, remediation, credit monitoring, and legal expenses, depending on the severity and scope of the breach. The following tips can help VPSAs minimize their vulnerabilities to two of the most common reasons for data breaches: phishing and travel.

Fighting Phishing

Cybercriminals use phishing—a type of social engineering—to manipulate people into doing what cybercriminals want. Social engineering is at the heart of all phishing attacks, especially those conducted via e-mail. Technology makes phishing easy. Setting up and operating a phishing attack is fast, inexpensive, and low risk: Any cybercriminal with an e-mail address can launch one.

The education sector has seen a rise in social engineering–based attacks. Students, staff, and faculty at various institutions all have suffered losses when personal data and research were disclosed to unauthorized parties. Phishing played a part in more than 40 percent of these breaches. To avoid being phished:

• Limit what you share online.
• Protect your credentials.
• Beware of attachments. E-mail attachments are the most common vector for malicious software.
• Confirm identities. Phishing messages can look official.
• Trust your instincts. If you get a suspicious message manually locate the organization online and contact them via the website, e-mail, or telephone number that you researched.
• Check the sender and the sender's e-mail address.
• Take your time. If a message states that you must act immediately or lose access, do not comply.
• Don’t click links in suspicious messages.

Travel Tips

Traveling today is so much easier with technology. Whether it’s a trip to the coffee shop around the corner or to a café in Paris, you can stay productive, entertained, and in touch. Unfortunately, traveling with devices can mean increased cyber risks for keeping your personal and institutional information private and greater potential for device theft.

Before you travel, take the following steps:
• Travel only with the data and devices that you use regularly.
• If you are traveling on university business, check with your IT support staff about the possibility of getting a clean, encrypted laptop.
• Encrypt all devices and data that you take with you.
• Keep prying eyes out. Password protect all devices.
• Back up your data before you go.
• Set up multifactor authentication.
• Update your operating system and apps/software, including antivirus protection.
• Turn on “Find My [Device Name]” tracking and/or remote wiping options.
• Log out of browsers and apps, remove any saved login credentials, and clear your browser history.
• Clear your devices of any content that may be considered illegal or questionable in other countries.
• Don’t overlook low-tech precautions.
• Stay informed of Transportation Security Administration regulations.
• Avoid posting on social media about your travel plans.

When in transit:
• Power off your devices before you arrive at the border.
• Do not put devices into checked baggage.
• Always keep your devices with you.
• Be careful when using public wireless networks or Wi-Fi hotspots.
• Use a virtual private network.

While you are at your destination:
• Connect to the Internet securely.
• Physically protect yourself, your devices, and any identification documents.
• Do not plug in untrusted accessories.
• Never log into anything when using public computers.
• Disable Wi-Fi and Bluetooth when not in use. Wait to post about your trip on social media until you return home.
When you return home:
• Change all passwords you may have used abroad.
• Run full antivirus scans on your devices.
• Check your statements.
• Delete unneeded apps.
• If you had a loaner device, do not connect it to the network when you get home.

Stay Cyber Safe

The responsibility to protect institutional and personal data is not limited to IT staff but rather the responsibility of the entire campus, especially the administration and cabinet-level staff. Work closely with your divisional or university IT unit as well as other relevant units to develop a comprehensive cybersecurity program which includes technical, administrative, and end-user security awareness programs.

For more information on phishing, please visit: security.ucsb.edu/news/ucsb-cyber-security-tip-don’t-let-phishing-scam-rell-you

For more steps you can take to help secure your devices and your privacy, please visit: security.ucsb.edu/news/ucsb-cyber-security-tip-cyber-smart-traveling

Joe Sabado is associate chief information officer for student affairs at University of California, Santa Barbara. He is also chair of the NASPA Technology Knowledge Community.

Kip Bates is associate director of cyber security in administrative services for the University of California, Santa Barbara.