IDShield℠

Investigator Tips

Gen Z Goes to College

The Gen Z kids heading to college today are “digital natives.” Born in or after 1995, when the term “smartphone” was coined, they’ve never known life without mobile devices, and they are rarely without one in their hand. A mobile device is how they communicate, shop, research, and get directions; for most, it has also replaced the television as the primary screen to watch video content. So of course, they can’t (and won’t) go to college without their smart phone in hand. While this “always on” mentality helps parents and friends stay in touch and enables students to get help in an emergency, if students aren’t smart about using and securing them, they can quickly lose their “lifeline” or become a victim of a scam or identity theft.

Before you pack the car full of dorm supplies, sit down with your prospective college student and make sure they have secured their smart phone by:

- Creating a lock on their phone that requires a PIN or fingerprint scan in order to use the device.
- Enabling “Find My Phone (or Device)” to help locate it in the event it is lost or stolen.
- Ensuring the software is up to date.
- Doing a backup so that if the phone is lost or stolen, the data can be retrieved.
- Knowing how to erase the device if it ends up in the wrong hands.
- Setting strong, unique passwords for each online account.

In addition to securing the device itself, students have become targets for “phishing” scams, which are getting harder to recognize, as the hackers get better at making them look legitimate. When viewed on a small screen, it can be even more difficult to recognize a fake email; however, as fewer people are opening emails (and those that do are becoming more cautious about clicking on links) hackers are turning to text messages. “Smishing” attempts rely on the immediacy of text messages, hoping the intended victim clicks on a link without stopping to think.

The Freshman 15

Smart phones aren't the only thing putting college students at risk for identity theft. The Identity Theft Resource Center reports there were 98 educational facility data breaches in 2016, including more than 50 colleges and universities. Students can't prevent these data breaches, but they should be aware of five common scams that target students, as well as 10 tips to keep their information safe.

Watch for these five scams:

Card cracking. Students are always looking for ways to make money, and they spend a lot of time on social media. Scammers take advantage of both of these in a scheme called card cracking, getting a student's attention via social media with offers to make some fast cash. They get the student to provide access to their checking account with a debit card, PIN or online login information; the scammer deposits a large check, immediately withdraws money from an ATM, and then gives the student a kickback. The student is told to report a lost or stolen card or credentials so the bank will return the withdrawn funds to the account. They may have their money back, but now the student is complicit in the crime.

Employment scams. Earlier this year, the FBI issued a warning about an employment scam that lures students with an offer of easy money. Unfortunately, this is not a legitimate job offer; instead of providing the student with income, they may be out money.

Roommate/rental scams. Not every rental listing is legitimate; the property may not exist, or it may be listed by an unauthorized party. Students can avoid rental scams by never paying a deposit without first visiting a property and meeting the landlord in person. Students should also be wary of prospective roommates they don't know, particularly if the new roomie sends a check in advance for more than their share of the deposit or rent, asking that the difference be wired back to them.

Social media scams. There are a number of social media scams, all designed to access personal information, money, or even cause harm. Some claim the student has won a prize, some involve romance, and others may come in the form of an email that asks the student to confirm or update personal information. Some even appear to come from a student's contacts, as scammers clone profiles to look as if a "sounds too good to be true" offer is coming from a friend.

Tuition scams. A student gets a call from the school administration office, saying they still owe tuition. The reason varies: a check bounced or a scholarship or loan fell through, for example. They say not to worry, just wire the money to their account by the end of the day. If a student gets such a call, they should contact the bursar's office.

10 ways to protect your information:

- Don't carry more personal information than you need.
- Keep personal information in a safe place.
- Lock your doors.
- Lock your laptop and smart phone.
- Keep software and virus protection up-to-date.
- Back up files and devices.
- Be careful when using free Wi-Fi.
- Don't share your passwords with roommates or friends.
- Only download software and apps from trusted sources such as Apple's App Store and Google Play.
- Be cautious about who you connect with, and what you share, on social media.

Knowing what to watch for and how to prevent it can help students avoid adding the weight of identity theft to their college experience. As for all that late night pizza, they're on their own!

Kroll