The Data Privacy & Security Checklist for College Students

Physical Precautions

- ❏ Have sensitive physical documents (bank, legal, personal, FAFSA, applications, etc.) sent to a permanent address (e.g., parents' home)
- ❏ Leave your Social Security card, passport and other documents in a permanent, off-campus location (e.g., parents' home in a fireproof and waterproof box or a bank safe deposit box)
- ❏ Shred any important financial documents that come in the mail and never leave sensitive mail lying out
- ❏ Always lock your dorm room door and don't leave devices unlocked or unattended in a gym locker, the library or in a classroom
- ❏ Check for unusual devices added to the ATM that might be skimming your card info
- ❏ Always cover the keypad with your hand when entering your PIN, whether at an ATM or a retail store

Secure Laptops & Mobile Devices

- ❏ Do not leave your laptop in an unattended car or in a public place (e.g., library, dining room, classroom)
- ❏ Register your laptop with campus security if possible
- ❏ Install laptop tracking software (e.g., Find My iPhone, Lojak)
- ❏ Enable "Find my iPhone" (iPhones) or "Find My Device" (Android) in case your phone is lost or stolen
- ❏ Encrypt your laptop (Apple: FileVault, Windows: BitLocker) and smartphone (by using a strong password)
- ❏ Spend time locking down the privacy and security settings on your smartphone — you won't believe what you're giving away for free and how damaging it can be
- ❏ Don't store personal information (SSN, passwords, etc.) in unencrypted files or insecurely in the cloud
- ❏ Securely back up your files on a remote hard drive or a trusted cloud provider (iDrive, iCloud, Carbonite) in case your data is lost or frozen by ransomware
- ❏ Lock your phone screen with at least a 6-digit passcode — the longer, the safer
- ❏ Don't insert strange storage devices (i.e., USB drives) and only insert such devices from friends or administration after scanning them for viruses
- ❏ Be suspicious of communal workstations in dorms, libraries, etc. Never log in to websites with usernames and passwords unless you're certain the computer is secure and won't save your information
- ❏ Turn on automatic computer operating systems, software and mobile app updates
- ❏ Be mindful of malware and ransomware "updates" from untrusted sources
- ❏ Do not take or store sensitive or embarrassing photos on your devices as they are commonly exposed by hackers, "friends" or former boyfriends or girlfriends
- ❏ Invest in strong security software with anti-virus, spyware and ransomware protection, even if you own an Apple
- ❏ Don't discard or sell old devices without professionally wiping them of all data and removing or erasing all SIM cards

SILEO

Defend Wi-Fi Usage

- ❑ Do not use public Wi-Fi to shop online, access financial accounts, or visit sensitive sites. Never enter your login names or passwords while on a free Wi-Fi hotspot
- ❑ Consider using a Virtual Private Network (VPN) to encrypt your data
- ❑ Only visit websites with “https” at the beginning of the URL, not “http”
- ❑ Disable the automatic Wi-Fi connectivity feature on your phone under Settings
- ❑ Monitor your Bluetooth connection in public areas and make sure a password is needed to connect
- ❑ Get an unlimited data plan and stop using public Wi-Fi — it is far safer, as it is always encrypted

Protect Online Accounts

- ❑ Enable pop-up blocking, private browsing mode and “Do Not Follow” in your browser preferences
- ❑ Disable third-party cookies and location tracking in your browser preferences
- ❑ Create a unique, highly secure password to access each online account (see below for details)
- ❑ Opt out of all information sharing as found in the website’s privacy or data use policy
- ❑ Minimize storage of your payment information online (e.g., credit card and bank account numbers) as these are often breached by cyber criminals
- ❑ Set up automatic account alerts to inform you of all activity, including purchases, transfers, account changes, etc.
- ❑ Don’t use Torrent websites to download free movies, songs or textbooks — many of these sites install malicious software as part of the download
- ❑ Sign up for electronic statements whenever possible to minimize physical mail and document storage
- ❑ Log out of all online accounts when finished if using someone else’s computer
- ❑ Check your credit report three times a year at AnnualCreditReport.com
- ❑ Opt out of junk mail at OptOutPreScreen.com
- ❑ Never loan anyone your credit or debit card

Create & Manage Strong Passwords

- ❑ Simplify and secure your passwords using a password manager like Dashlane, 1Password or LastPass
- ❑ If you don’t use a password manager, follow these rules:
    - ❑ Create alpha-numeric-symbol passwords that are 13 characters or longer, not easily guessable and unique for every account
    - ❑ Do not use birthdays, family names, pets, favorite destinations or dictionary words
    - ❑ Store your passwords securely. Never write a password down and stick it near your device (e.g., top drawer, back of the laptop, mobile case, etc.) or keep it in your wallet
    - ❑ Do not store your passwords in your email account, contact manager or in an unsecured cloud account
- ❑ Enable two-step authentication/two-factor authentication (2FA) for websites that store personal info. This is one of the single strongest steps you can take to minimize account hacking and takeover
- ❑ If your password has not been breached or compromised and is long and strong, only change it once a year

SILEO

- ❏ Never use the same password for multiple websites as a breach on one website can lead to a breach on others

Don't Take the Phishing Bait

- ❏ Phishing schemes are highly sophisticated — distrust *every piece of email* coming into your inbox until you have verified that it is legitimate
- ❏ Never reveal private information (e.g., passwords, credit card numbers, SSN, bank account numbers, addresses, etc.) in an email or text
- ❏ To see if an email link is legitimate, hover over it with your cursor to see if it goes to the URL you were expecting and that you know is trustworthy. Even better, type in the URL yourself and surf to the website directly
- ❏ Ignore phishers who play on your fears ("You owe the IRS …," "Your account is about to be terminated …," "We're going to alert your parents to this behavior") and greed ("You're eligible for a free gift, great credit card offer …"). Emotion-based messages are often socially engineering you to act without thinking
- ❏ If you're uncertain about online legitimacy, call the organization directly
- ❏ Never download and install suspicious software that you haven't verified as legitimate
- ❏ Search the internet to see if similar phishing scams have been reported — Snopes.com is a good resource
- ❏ Distrust unusual callers, especially those who use fear, flattery or a call for help
- ❏ Do not give personal and financial data (e.g., passwords, SSNs, tax information, credit or debit card numbers, etc.) over the phone
- ❏ Government agencies will not cold call you and the IRS will contact you via mail
- ❏ Caller IDs can be easily spoofed — Hang up and call the institution directly (e.g., IRS, Office of Admissions, bank, etc.)
- ❏ If a company calls and says your computer is having problems, do not allow them to remotely connect to your computer to fix it

Lock Down Social Media

- ❏ Implement all suggestions above in "Protect Your Online Accounts" for your social media profiles
- ❏ Limit the personal information you post or list in your profile (e.g., mobile number, home address, age, location, school)
- ❏ Spend at least one hour customizing the privacy and security settings in each one of your social media accounts — this is of the highest priority and needs to be repeated somewhat frequently due to frequent changes in policy
- ❏ Do not accept requests from random friends and students on social media
- ❏ Do not advertise when you're going to be away from your dorm or apartment
- ❏ Do not allow your device to be geotagged (e.g., check in at locations via GPS)
- ❏ Remember that everything on social media is, by definition, social and will be shared
- ❏ To avoid revenge porn, do not take or store embarrassing pictures on your devices, cloud accounts or social media apps

- ❏ Be careful of sexting, as everything digital is hackable and will almost certainly be seen or shared by others
- ❏ Distrust any appeals for money, information or compromising images you receive on social media until you've confirmed it is a legitimate request in person
- ❏ Watch out for fake online personas — do your research before you agree to meet someone you met online

And finally, ask for help from your university, parents or a trusted source when you need help. None of us can do all of this alone.

About Cybersecurity Expert & Keynote Speaker John Sileo

John Sileo is an award-winning author and keynote speaker on cybersecurity, identity theft and tech/life balance. He energizes conferences, corporate trainings and main-stage events by making security fun and engaging. His clients include the Pentagon, Schwab and organizations of all sizes. John got started in cybersecurity when he lost everything, including his $2 million business, to cybercrime. Since then, he has shared his experiences on 60 Minutes, Anderson Cooper, and even while cooking meatballs with Rachel Ray. Contact John directly to see how he can customize his presentations to your audience.

SILEO