Student

Protect your accounts, recognize phishing, and report fast when something looks wrong.

Before — prepare

- Turn on multi-factor authentication (MFA) for your campus account, email, and any system holding your records.
- Use a password manager and a unique password for your campus identity. Never reuse it on other sites.
- Keep your laptop, phone, and browser updated. Install updates within 7 days of release.
- Back up your coursework to campus cloud storage (and a second copy where allowed). Don’t rely on a single drive.
- Save the IT help desk and security team contact info in your phone before you need it.
- Complete any phishing or security training the campus offers — even short modules build real skill.
- Review your account recovery options (backup email, phone) so an attacker can’t reset your password.

During — respond

- If a message, login page, or pop-up looks suspicious, stop. Do not click, do not enter credentials.
- If you already clicked or entered a password, change that password from a different device and report it now.
- If your device is acting strange (files renamed, ransom note, unexpected encryption), disconnect it from Wi-Fi and any cables, leave it powered on, and contact IT.
- Forward suspicious emails using the campus ‘Report Phishing’ button or as an attachment to the security team.
- Don’t try to ‘fix’ a suspected infection yourself. Don’t pay a ransom on a personal device — call IT.
- Follow official guidance from the campus emergency channel. Ignore unverified rumors on social media.

After — recover & learn

- Change passwords for any account that may have been exposed and review login history.
- Re-enable backups and confirm your important files are still recoverable.

- Tell classmates and roommates what you saw — phishing campaigns usually target many students at once.
- Attend any post-incident briefings; they teach you the exact lure that worked so you can avoid the next one.

Self-audit checklist

- ■ MFA is on for my campus email and student portal.
- ■ I use a password manager (or at least a unique password for school accounts).
- ■ My laptop and phone install updates automatically.
- ■ I have at least one backup of my coursework outside the device I use daily.
- ■ I know how to report a phishing email on my campus.
- ■ The IT help desk number is saved in my phone.
- ■ I've reviewed my account recovery email and phone in the last 6 months.

Created by Joshua Gerstenfeld and Scott Jacques with support from the CrimRxiv Consortium. Code MIT-licensed; content licensed CC BY 4.0. Sources: NIST SP 800-61r3, NIST IR 8374, CISA #StopRansomware, EDUCAUSE. See: https://github.com/crimconsortium/campus-ransomware-playbook