Staff and department personnel

Daily habits, vendor risks, and clear escalation paths protect the systems your departments rely on.

Before — prepare

- Enable MFA on every work account, especially email, finance, HR, student information, and vendor portals.
- Verify wire transfers, banking changes, and vendor payment updates by phone using a number you already have on file — never one in the email.
- Lock your screen whenever you step away. Use a privacy filter for shared spaces.
- Keep approved software only. Ask IT before installing anything that touches campus data.
- Know where your data lives. List the systems your job depends on and confirm they are backed up.
- Maintain printed and offline copies of critical contact lists in case email is unavailable.
- Train new hires and student workers on phishing reporting from day one.

During — respond

- If a tool stops working, files are renamed, or a ransom note appears, disconnect from the network and call IT — do not email about it from the affected device.
- Stop sending or approving payments until IT confirms the environment is safe; this is a common attack window.
- Do not destroy artifacts — keep the screenshot, the email, the file, the URL.
- Use approved out-of-band channels (phone, signed-in-app messaging) to coordinate with your team.
- Refer external inquiries to the official communications lead. Don’t speculate on cause or attribution.

After — recover & learn

- Reconcile financial activity for the impacted period; verify against bank statements directly, not internal reports that may be tampered with.
- Review vendor access; revoke anything no longer needed and re-credential what stays.
- Update standard operating procedures based on what worked and what didn’t.
- Re-train staff on the specific lure that triggered the incident.

Self-audit checklist

- MFA is on for all work accounts including finance and HR systems.
- I have a callback procedure for verifying wire-transfer and vendor banking changes.
- I know which systems my unit depends on and which would hurt most if unavailable.
- Critical contact information is available offline (printed list or phone-stored).
- My screen locks automatically and I lock it when I step away.
- I have completed my campus phishing/security training in the last 12 months.
- Student workers and new hires have been onboarded to phishing reporting.

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