Cyber-Smart Parenting

A Guide to Protecting Your Student's Digital Life

As your student navigates college life, they're also managing an online world full of opportunity—and risk.

MONTCLAIR STATE UNIVERSITY | Information Security

Encourage Strong Password Habits

- Use long, unique passwords for each account.
- Enable a password manager to store them safely. (Many password managers have family plans!)
- Avoid sharing passwords—even with friends or roommates.

Promote Multi-Factor Authentication

- We ensure your student uses **Duo MFA** for school – encourage them to also use MFA for personal accounts.
- Remind them to **never approve** a Duo request they didn't initiate.

Talk About Phishing & Scams

- Help them spot red flags like urgent language, misspellings, and unknown links.
- Remind them:
    - When in doubt, don't click! Report it using the **Phish Alert Button (PAB)** or send it to **phishfiles@montclair.edu**.
    - Montclair State University will **never** ask users for their NetID passwords or Duo codes.
- Check the **Phish Files** for updates on phishing attacks.

Watch for Financial & Job Scams

- College students are prime targets for fake job offers, "urgent" payment requests, and tax scams.
    - Remind your student that job offers on campus should come through **Handshake**.
- Some scammers might even contact you personally.
- If it sounds too good to be true—it probably is.

Respect Their Privacy, Support Their Awareness

- Give them space to manage their accounts—but talk regularly about security.
- Share resources like news articles available on the **Phish Files** weekly.

Help Yourself, Help Them

Cyber awareness starts at home. Strengthen your own digital habits and lead by example:

- **Use a Password Manager (Family Plans)**
  Secure your logins with tools like 1Password, LastPass or Dashlane. It's safer and easier than writing them down.
- **Set Up a Family Code Word**
  Pick a phrase only your family knows to confirm it's really *you* in case of emergency texts, emails, or calls.

- **Think Before You Share**
  Avoid oversharing on social media—details like your student’s school, dorm, or travel plans can aid scammers.
- **Update Devices Regularly**
  Make sure your phone, computer, and apps are running the latest security updates.
- **Use Multi-Factor Authentication**
  Just like your student, you should turn on MFA wherever possible—email, banking, and shopping accounts included.

Cybersecurity is a shared responsibility.

With your support and awareness, your student can build safer online habits that last a lifetime.