



# Cyber Hygiene Checklist

Simple steps to stay safe online.

MONTCLAIR  
STATE UNIVERSITY | Information Security



## Daily/Ongoing

- ☐ **Think before you click:** Don't click suspicious links in emails, texts, or social media.
- ☐ **Lock your devices:** Use a PIN, fingerprint, or face lock on your phone and laptop.
- ☐ **Use secure Wi-Fi:** Avoid public Wi-Fi or use a VPN if you must connect.

## Weekly

- ☐ **Check for system updates** on your phone, laptop, and apps.
- ☐ **Empty your trash/recycle bin** and clear browser cache for better privacy.
- ☐ **Review app permissions** – are you oversharing your location or contacts?

## Monthly

- ☐ **Run antivirus/malware scans** if your device has antivirus protection.
- ☐ **Review your social media** privacy settings – limit who can see your posts and profile.
- ☐ **Check your accounts** for suspicious activity (e.g., unknown logins).

## Quarterly

- ☐ **Update your passwords** – especially for email, bank, and school accounts.
- ☐ **Enable or test Multi-Factor Authentication (MFA)** on all of your accounts.
- ☐ **Back up your important files** to cloud storage or an external drive.

## When Something Feels Off

- ☐ **Report phishing** or suspicious emails using the PAB or forward it to [phishfiles@montclair.edu](mailto:phishfiles@montclair.edu).
- ☐ **Change your password** immediately if you think an account was compromised.
- ☐ **Check your devices** for new apps or settings you didn't enable.

**Pro Tip:** Use a password manager to keep your logins secure and unique – you only need to remember one strong password!