**Protect Your Accounts**

* **Use strong, unique passwords** for each account (consider using a password manager).
* **Enable multi-factor authentication (MFA)** wherever possible.
* **Update passwords regularly** — especially after any breach.

**Be Smart About Sharing**

* **Think before you post**: Avoid sharing sensitive info like your address, phone number, or travel plans.
* **Adjust privacy settings** on social media and apps to limit who can see your information.

**Recognize Scams and Phishing**

* **Don’t click suspicious links** — even if they look like they come from a trusted source.
* **Verify email senders** before responding to unexpected requests, especially for money or personal information.
* **Look for red flags**: Urgent language, typos, or unfamiliar addresses.

**Secure Your Devices**

* **Keep software and apps updated** with the latest security patches.
* **Use antivirus and anti-malware tools** and run regular scans.
* **Lock your devices** with a password, PIN, or biometric security.

**Practice Safe Browsing**

* **Use secure websites** (look for “https://” and a lock icon).
* **Avoid using public Wi-Fi** for sensitive activities (use a VPN if needed).
* **Be cautious with downloads** — only install apps from trusted sources.

**In Case of a Security Breach**

* **Report it immediately** to our IS department or your service provider.
* **Change affected passwords** and monitor accounts for unusual activity.
* **Notify financial institutions** if banking information was exposed.