SOFTWARE UPDATES: NEVER HIT SNOOZE

Software is everywhere—school, work, social, and every aspect of our daily lives. Updating software often feels like chore, but it's what keeps each one of us and our community safe and our systems running smoothly.

Outdated software is an open invitation to cybercriminals. By neglecting updates, you ignore security patches and improvements that close vulnerabilities.

RISK BY THE NUMBERS

90% of cyber attacks exploit outdated software

60% of breaches involve vulnerabilities for which a patch was available

43% of cyber attacks target educational institutions

SOFTWARE UPDATE SCAMS

LOOK OUT FOR RED FLAGS:

- **"Urgent" Alerts**: Real updates don't rush you.
- **Text Speak**: Legit updates use formal language.
- **Weird Links**: Always hover to check the URL.
- **Random Pop-Ups:** Be wary on non-official sites.
- **Unknown File Types**: Stick to .exe or .dmg.
- **"Free Premium" Bait**: Too good to be true? It is.
- **Off-brand Design**: Look for official branding.
- **Asks for Student ID**: Real updates won't ask for this.

TIPS TO SAFE SAFE

Verify Source: Always double-check where the update is coming from.
Email Caution: If the update comes via email, scrutinize the sender's address.
Use Antivirus Software: Employ trusted antivirus software to flag malicious activity.
Official Channels: Download only from official websites or built-in software features.

HOW TO REPORT

To learn more and/or report suspicious behavior, email the Office of Information Security at infosec@uc.edu.

For any Cyber Security questions, please visit the
Office of Information Security or email us at infosec@uc.edu