University of CINCINNATI

Updating Software

Outdated software allows hackers to exploit vulnerabilities that have been fixed in newer versions. Just like you wouldn't expect a broken lock to protect your home—an outdated system is asking for trouble.

ALWAYS **UPDATE**

Updates patch insecurities and keep your programs running smoothly. Cybercriminals are always updating their attack methods; keep your software updated too.

SHIELD YOUR SYSTEM WITH **AUTO-UPDATE**

Legitimate programs will often give you the option to enable automatic updated. This lets your software automatically download updates and patches as soon as they become available, ensuring you are always running the latest versions.

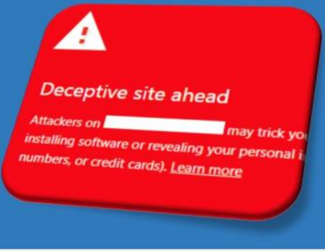
When updating your software, **REMEMBER...**

SOURCE **MATTERS**

Only download software updates from official sources. If the option to automatically update is not available, check the manufacturer's site for updates and patched; do not trust warnings asking you to download things.

CLICK **ATTACK**

A fake warning will ask you to download a file or fill out a form, but a real browser warning or an alert from a legitimate source will only ask you to not do something: don't click ahead, don't stay here.



Deceptive site ahead

Attackers on [redacted] may trick yo
installing software or revealing your personal i
numbers, or credit cards). Learn more

Using cracked or pirated software isn't just illegal—it's a security nightmare. You risk malware, compromised data, and endangering the network.

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