



CYBERSECURITY AWARENESS DAY 6

Let's talk about
**Software Update
and Patching.**

Iwuchukwu Augusta Chioma





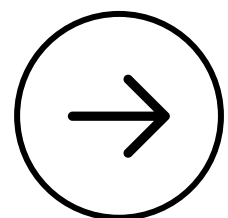
Software Update and Patching

**That “Update Now” pop-up you
keep ignoring?**

It’s not a distraction.

**It’s your device whispering let me
protect you before the hackers
come knocking**

Iwuchukwu Augusta Chioma



What is Software Update and Patching



Every app, operating system, or tool you use from WhatsApp to Windows, runs on software

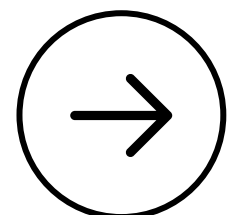
A **software update** is simply a newer, improved version of that software.

A **patch** is like a small “band-aid” developers release to fix bugs or seal security holes

Just like vaccines protect the body, software updates protect your devices from known cyber threats. Every day, hackers look for outdated systems to exploit.

That “**Remind me Later**” button may feel harmless but it could leave a door open for attackers.

Iwuchukwu Augusta Chioma



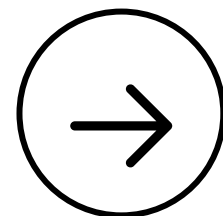


But here's the catch not every **“Update Now”** notification is real. Cybercriminals are getting smarter. They design fake update pop-ups that look identical to genuine ones often seen on compromised websites or phishing emails.

One careless click can install malware instead of security patches.

That's why knowing where to update matters.

Iwuchukwu Augusta Chioma



How to Recognize a Legitimate Update



Safe Updates Come from Trusted Sources:

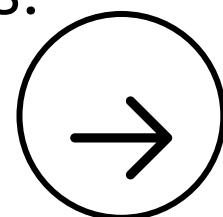
✓ Your device's system settings — e.g., Windows Update, macOS Software Update, Android/iOS Settings

✓ Official app stores — Google Play Store or Apple App Store

✓ Verified vendor websites — for tools like Microsoft Office, Adobe, or antivirus software

✗ Never click on update links from emails, pop-ups, or social media messages.

Iwuchukwu Augusta Chioma

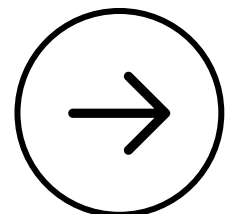


Why Updates & Patches Matter



- Fixes known vulnerabilities before hackers exploit them
- Improves system performance and stability
- Enhances compatibility with newer applications

Delaying them leaves security holes open for attackers.



Safe Update Practices

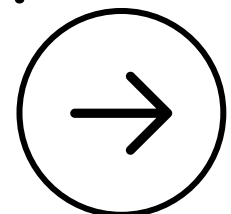


Smart Habits to Keep You Secure:

- Turn on automatic updates in your system settings
- Restart devices regularly so patches install completely
- Always verify updates through official channels
- Use a trusted antivirus that can detect fake update installers

Software updates protect you but only when done the right way.

Iwuchukwu Augusta Chioma





**Share, like and
follow for more
Cybersecurity
awareness tips**

Iwuchukwu Augusta Chioma