MONSTER SMASH

SOFTWARE PATCHES

INSTALL SOFTWARE PATCHES AS SOON AS POSSIBLE. HACKERS LIKE TO TAKE ADVANTAGE OF OLD VULNERABILITIES. ONLY UPDATE FROM TRUSTED VENDORS, LINKS IN EMAIL/POPUPS TELLING YOU TO UPDATE MAY BE PHISHING ATTEMPTS.

END OF LIFE

END OF LIFE SOFTWARE MEANS THE MANUFATURER NO LONGER SUPPORTS THE DEVICE, AND STOPS RELEASING SECUIRTY PATCHES. IT IS BEST TO UPGRADE TO A NEWER VERSION ONCE THIS HAPPENS, AS USING EOL DEVICES WILL LEAVE YOU VULNERABLE.

UNTRUSTED NETWORKS

DO NOT UPDATE YOUR SOFTWARE ON A UNTRUSTED PUBLIC NETWORKS (HOTELS, AIRPORTS, COFFEE SHOPS), AND IF YOU MUST THEN BE SURE TO USE A VPN.

AUTOMATIC OR MANUAL UPDATES?

IT IS RECOMMENDED TO USE AUTO UPDATES SO THAT YOUR SYSTEM IS SECURED AS SOON AS POSSIBLE, HOWEVER BE CAREFUL NOT TO AUTO UPDATE ON PUBLIC WIFI.

CYBER HOUSE ROCK:

CYBERHOUSEROCK.INFO

CISA INFORMATION:

HTTPS://WWW.CISA.GOV/SHIELDS-UP

CISA SOURCES:

HTTPS://WWW.CISA.GOV/NEWS-EVENTS/NEWS/UNDERSTANDING-PATCHES-AND-SOFTWARE-UPDATES

HTTPS://WWW.CISA.GOV/RESOURCES-TOOLS/TRAINING/KEEP-YOUR-DEVICES-OPERATING-SYSTEM-AND-APPLICATIONS-DATE