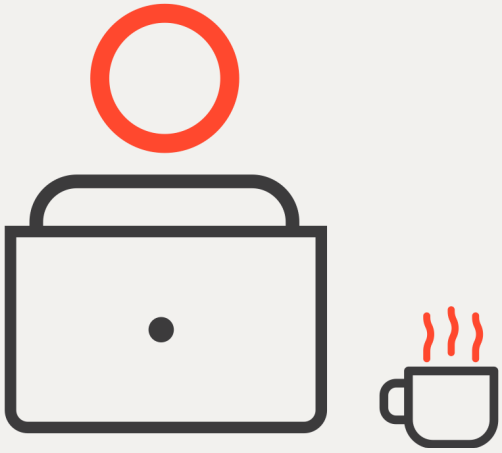
kyndryl

Why keeping your software updated is important

We all use software applications in our daily lives.

Software on your work laptop, home computer, printers, routers, phone, smart home devices in your home etc. We use software for online shopping, banking, social media, on demand streaming of TV shows and movies and more.[1]



Did you know that:

- Once the hackers gain access to one device, they can then search for others such as your computer.
- There are on-line websites showing vulnerable devices in the world that hackers can use.
- You can enjoy enhanced performance, data protection and security that comes with latest software.

Outdated software is **vulnerable** software and can make you into a **target**.

How to prevent it?

Keep your software up to date by upgrading promptly to new versions and install updates immediately available. Not all software is updated automatically. Remove it if you no longer require it.

Be careful when using “free” software at home. Make sure you understand the licensing and if it is reputable and legal. Some free software comes with additional software bundled in that can be classified as malware and be dangerous.

Take time to understand what devices you have at home that connect to the internet. Make sure the software in them is updated and access restrictions are set. Be aware of what devices may be listening to you and what they record.[2]

Avoid:

Unprotected Data

Phishing, Smishing & Vishing

Unreliable end-to-end encryption

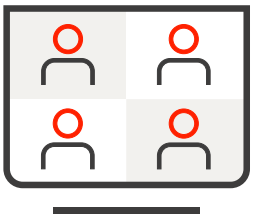
Chief Information Security Office

Examples:

You are hurrying to finish work on time to collect your children at daycare. Just as you are about to log off, you get a software update pop up message. You click ignore.

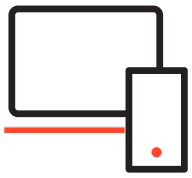
Life continues and you forget to go back and update your software. The longer you delay, the more vulnerable your device is to an attack. Each update closes security vulnerabilities. Consider switching on auto update options on your software. Set reminders to check your software regularly. **60% of hacks** are due to unpatched software.

Your friend tells you about this great new application that allows for sharing pictures and it is totally free. You download, install and start using the app. Everything looks great initially.[3]



Free software can contain Malware and may not always be safe. When you download and install the software it came with additional programs that start to track your activities. Always research how reputable the application and company are and how well protected your data and pictures are? What personal data is collected? Is it indeed a free software? Where is your data being stored? **Free does not always mean free.** Be cautious.

You have recently changed your internet services provider, and the technician provides you with a default password and network name to log on to the new router and wi-fi.[4]



Even if the default password does not look easy to guess, remember that hackers have password lists containing stolen or standard and easy to guess passwords to connect to your router, which then allows access to your computer and data. Remember to **change your default passwords and network names** that come with new devices.

Is your smart home smarter than you? You like the convenience of smart devices until your 6-year-old orders three new bicycles on Amazon and you're stuck with the bill. After all, Alexa was listening...[5]

Add a Virtual Private Network (VPN) to your home network for guest devices; use PINS and disable voice purchasing; turn the microphone off; set your device cache to delete itself every few months; switch off features that you do not use; disable remote access if not needed. Consider getting a **router with WPA3** capability.

For more information, explore more references and visit the following pages:

1. Want to avoid a cyberattack? Stop ignoring those pesky software updates.
   https://www.washingtonpost.com/technology/2022/02/24/software-update-security-cyberattack/
2. Think Twice Before Putting Off Updates!
   https://www.cisa.gov/secure-our-world/update-software
3. Why that free Windows download could cost you more than you bargained for.
   https://www.foxnews.com/tech/free-windows-download-cost-more-bargained
4. Risks of Default Passwords on the Internet.
   https://www.cisa.gov/news-events/alerts/2013/06/24/risks-default-passwords-internet
5. 5 Smart Home Dangers To Look Out For.
   https://www.safehome.org/news/smart-home-dangers