Understanding Patching

What is patching?

A patch is a piece of software designed to update a computer program or it's supporting data to enhance performance and/or address vulnerabilities. Security vulnerabilities, commonly called bug fixes is a key outcome for most patches.

Why is patching important?

By not applying a patch you might be leaving the door open for a malware attack, including ransomware. Malware exploits flaws in a system in order to do its work. Unpatched defects in software may allow malicious websites, etc. to infect or compromise your computer with no action on your part.

Detecting vulnerabilities & weaknesses in software

- Check your server or operating system provider's website for updates.

- Vulnerabilities may present as missing encryption for sensitive data, a reduction in system performance, and incompatibility with other networks and applications. These vulnerabilities and weaknesses make your network susceptible to hackers and scammers looking to take advantage of unaddressed vulnerabilities and weaknesses.

Preventing compromises

- Operating software is imperfect, so it is always important to keep your software up to date.

- Use an automated patching tool to keep your software updated.

- Use a traffic scanning tool to keep you from accessing infected web locations.

- Use an application that can block advanced forms of malware, which antivirus can't detect or block. These will sometimes require payment.

- Use an antivirus in case you get infected.

- Remove software you no longer require or do not recognise.

- Regularly check your operating system and server sites for updates.

Understanding Patching

How to patch software

- How to turn on automatic patching software for windows:

- How to turn on automatic patching software for mac:

- Alternatively, you can access the individual software program you want to patch, and follow the prompts to "update" the software.

- Explore different patch management tools to ensure you are always up to date with patching.
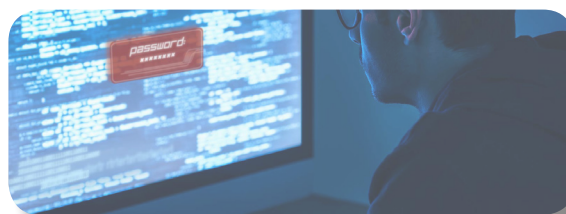
What are hackers interested in when they exploit flaws on your computer?

When flaws are located and exploited they can give scammers just enough time to download keylogging software (as an example). Hackers are then able to capture passwords you enter on the device. This can include your banking passwords and also email passwords that give the hackers access to all of your contacts to become targets as well.

Other fact sheets

- Credit Reporting Agencies
- Scam Prevention and Education
- Engaging Organisations
- Social Media
- Devices and Technology
- Your Rights