THE CYBER RESILIENCE CENTRE FOR LONDON

Update Software & Operating Systems

Cyber criminals scan for security flaws (vulnerabilities) in software (applications) and operating systems (OS) to gain unauthorised access to devices and online accounts, spread malware, spy on user activity, steal data and commit other cyber-attacks. The more vulnerable your software is, the more damage a cyber-attack can cause.

Updates not only enhance the user experience but provide security patches that fix known vulnerabilities. It is vital that you download and install updates within 14 days of release, to close the window of opportunity cyber criminals have, to use the vulnerability for an attack. Updates can be installed automatically so you are immediately protected.

Vulnerability Assessments

Vulnerability assessments will map out the software you have installed and will identify whether they are vulnerable and pose a threat to your device and other devices connected to the same Wi-Fi. Reports will rank the vulnerability from critical to low so you can prioritise what needs securing first. You can then consider uninstalling the software you no longer need or is no longer supported with updates, or work your way through the updates until your network is secure.

Migrating

Overtime, developers do not support their obsolete software and products with security updates, leaving them vulnerable and a target for cyber criminals. Where possible, move to a product that continues to receive updates. You can find timelines of support for each product on the developer's website. Should it not be possible for your business to migrate, take extra precautions to stay safe, as this guide on Obsolete Products by the National Cyber Security Centre (NCSC) explains.

Zero-Day Vulnerabilities

Zero-day vulnerabilities are new vulnerabilities that are yet to be fixed by the developer and remains susceptible to attack until an update is released. When informed of a zero-day, remain extra cautious when using the software and product until you receive the update.

This is where a multi-layered approach to resilience is critical, which includes antivirus, Firewalls, 2-step verification and more.