□ links open in new tab

WannaCrypt/WCry Ransomware:

As you would have seen in the media over the past weekend, **a major malware outbreak has spread across the world** affecting many Windows computers **running versions XP, 7, 8 and 10**. The WannaCrypt Ransomware can spread via computer networks and **does not rely** on a user opening an email attachment or visiting an affected website, making it particularly destructive. Once activated on a PC, it will **automatically encrypt every user-created file and document it finds** including Microsoft Word, Excel, PowerPoint, Adobe PDF and JPG format as well as dozens of other file types, rendering them inaccessible.

The WannaCrypt ransomware **spreads via a security exploit that Microsoft released a security patch for in March of this year**. All department-managed Windows computers (including eT4L and corporate) are protected via centrally-delivered patching and update services which have already deployed the necessary patch. However, **there are concerns about Windows computers** that are in schools and corporate offices that are **unmanaged or are personally owned.** *(eg. BYODs).*

Microsoft Critical Security Update MS17-010

It is critical that **all unmanaged Windows PCs and user-managed Windows BYODs** immediately ensure that **critical security update MS17-010** has been installed on their device(s). The **easiest way to achieve this** is to open Windows Update to determine if there are any outstanding updates and to apply them. On your unmanaged Windows device, complete these steps:

- ***Click the Windows button*** *to open the Windows menu and in the box, type* **Check for updates** *then press Enter.*
- *The* ***Windows Update screen*** *will appear. If it states "Your device is up to date" with a recent last checked date, nothing needs to be done with that PC.*
- *If the device has not been checked or updated for some time, click* ***Check for Updates*** *and apply any and all security updates that appear as available.*
- *To ensure all security updates are installed completely, it is* ***essential that the device be restarted*** *from the shutdown menu option.*

Important note for school staff and student devices

The above steps to check for Windows updates is **not possible at school during school hours** (9am - 3pm). It is strongly recommended that as per the department's **Communication Devices and Associated Services Guidelines**, staff and students are required to:

- ***ensure that BYO devices are running up to date anti-malware software, application software versions and patched operating systems.***

Student and staff owned BYODs should either have their **Windows security updates installed at home prior to bringing them to school**, or check for and install updates before 9am or after 3pm on school days.

Please pass this information onto all staff and students with unmanaged and BYOD Windows devices.
Thank you for your assistance with this important matter.

INFORMATION TECHNOLOGY DIRECTORATE - Security advice v1_16/05/2017