Cyber Security Tip - Bluekeep: Windows RDP Vulnerability

What is Bluekeep?

Microsoft has advised users that there is a vulnerability within its Remote Desktop Services. Remote Desktop Services allow others to access your computer without physically being at the machine. Cyber attackers can connect to targeted computers and send specially crafted commands. This can happen without you allowing them to do so.

Computers running with the following Windows operating systems are vulnerable to this attack:

Windows 7

Windows Vista

Windows XP

Risk Mitigation

Microsoft Windows users must install a 'patch' to fix this vulnerability. If you are using one of the above Windows operating systems, please click the relevant link below to install the patch.

Windows 7 : https://portal.msrc.microsoft.com/en-US/security-guidance/advisory/CVE-2019-0708

Windows Vista/XP: https://www.catalog.update.microsoft.com/Search.aspx?q=KB4499180

What is the impact?

A Remote Desktop Service left unpatched may remain exposed and your information could be exploited. Taking no action can lead to:

- Cyber-attacks taking place across a network of computers, e.g. shared folders
- Theft of data and intellectual property on your computer
- An attacker compromising your web browser - Google Chrome, Internet Explorer etc.
- Usernames and passwords being stolen from your computer

Who should I contact?

If you have any questions or require support installing the patch, please contact the Kindergarten IT Program helpdesk and someone will assist you on **0386647001.**

References:

Australian Cyber Security Centre: https://www.cyber.gov.au/publications/BlueKeep

Microsoft: https://blogs.technet.microsoft.com/msrc/2019/05/14/prevent-a-worm-by-updating-remote-desktop-services-cve-2019-0708/