## User Tips

**Update your software and operating system regularly**

Computer users became victims of the WannaCry attack because they had not updated their Microsoft Windows operating system.

Had they updated their operating systems regularly, they would have benefited from the security patch that Microsoft released before the attack.

This patch removed the vulnerability that was exploited by EternalBlue to infect computers with WannaCry ransomware.

Be sure to keep your software and operating system updated. This is an essential ransomware protection step.

**Do not click on suspicious links**

If you open an unfamiliar email or visit a website, you do not trust, do not click on any links. Clicking on unverified links could trigger a ransomware download.

**Never open untrusted email attachments**

Avoid opening any email attachments unless you are sure they are safe. Do you know and trust the sender? Is it clear what the attachment is? Were you expecting to receive the attached file?

If the attachment asked you to enable macros to view it, stay well clear. Do not enable macros or open the attachment as this is a common way ransomware and other types of malware are spread.

**Do not download from untrusted websites**

Downloading files from unknown sites increases the risk of downloading ransomware. Only download files from websites you trust.

**Avoid unknown USBs**

Do not insert USBs or other removal storage devices into your computer, if you do not know where they came from. They could be infected with ransomware.

**Use a VPN when using public Wi-Fi**

Exercise caution when using public Wi-Fi as this makes your computer system more vulnerable to attack.

Use a secure VPN to protect yourself from the risk of malware when using public Wi-Fi.

**Install internet security software**

Keep your computer protected and prevent ransomware by installing internet security software. Go for a comprehensive solution that protects against multiple complex threats.

**Update your internet security software**

To ensure you receive the maximum protection your internet security has to offer (including all the latest patches) keep it updated.

**Back up your data**

Be sure to back up your data regularly using an external hard drive or cloud storage. Should you become victimized by ransomware hackers, your data will be safe if it is backed up. Just remember to disconnect your external storage device from your computer once you’ve backed up your data. Keeping your external storage routinely connected to your PC will potentially expose it to ransomware families that can encrypt data on these devices as well.

**Find and fix the weak links before attackers do**

Any internet-facing account that doesn’t require MFA is a brute-force attack away from a compromise. Any unpatched internet-facing server is an exploit away from script-kiddie payday.

**Assume breach and fix weak links inside**

Threat actors look for quick ways to obtain domain admin credentials. Service or admin accounts with SPNs that also have weak encryption, or worse still, privileged accounts with weak or no password requirements are too-easy targets.

In too many organizations, attackers don’t even need elevated credentials to harvest data – the average employee has access to far more data than they require. Lockdown sensitive data so that only the right accounts have access, and then monitor file systems for unusual access and change events.

**More lights, please, especially on stuff that matters**

Organizations with comprehensive monitoring solutions detect and investigate attacks like these more quickly. If you have blind spots on core data stores, in Active Directory, DNS, remote access systems, or in web connections, you’ll struggle to determine which systems were compromised and whether sensitive data was stolen.

**If you detect a breach, let Active Directory triangulate the blast radius**

Active Directory events can help you quickly identify compromised accounts and devices. Instead of focusing on one endpoint at a time, once one compromised account or system has been identified, query Active Directory for signs of lateral movement by that account or accounts used on that system.