Build your own computer defence shield

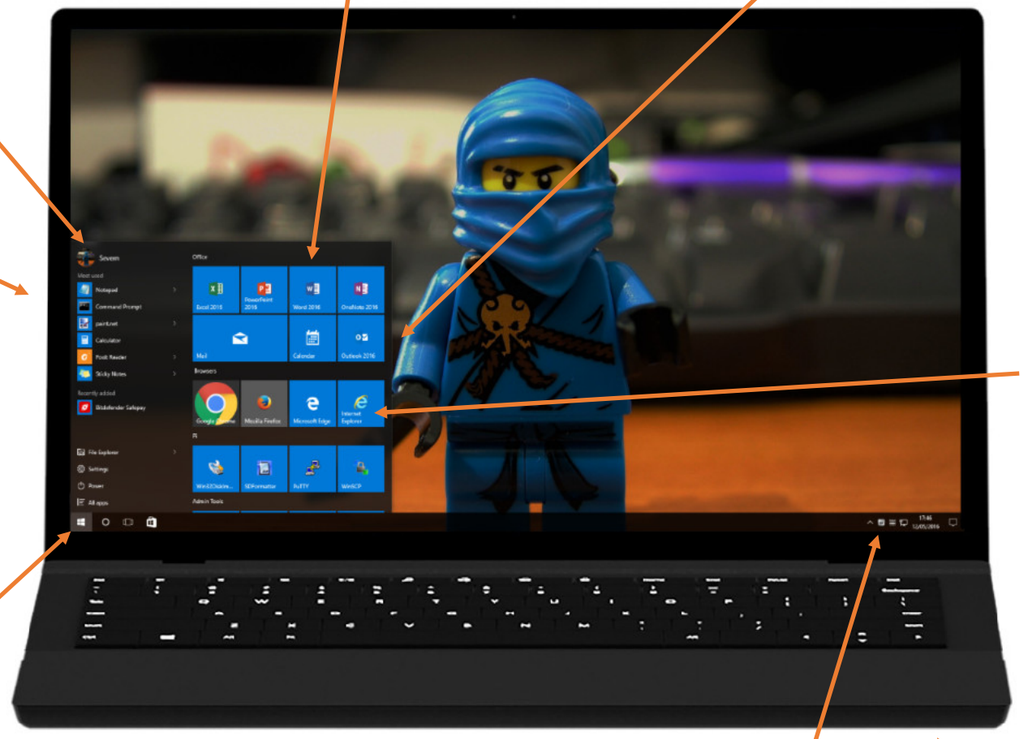
Run as a restricted windows user

"97% of critical vulnerabilities in Microsoft software could have been prevented by removing admin rights"

Login as an standard user, have a separate "admin" account for installing applications.

Lock your device

Use a pin, or a secure password.
It will help keep your data safe if it becomes lost or stolen!



Patch those apps!

Many security exploits come from popular 3rd party software.

For example, in 2015, there were 314 exploits found in the popular browser plugin Adobe Flash, 80 in JAVA, 129 in Adobe Reader, and 100 in Apple iTunes! Keep your applications patched!

Email

Consider using a 3rd party email filter. These remove spam, infected & phishing email's before they enter your network.

Use a modern operating system

Make sure you're using an up-to-date & supported operating system.

Microsoft no longer provides support, or security updates for Windows XP, Vista or Server 2003 (both were retired back in 2014!)

Take advantage of the security improvements made in newer operating systems, such as a reduced attack surface, built-in disk encryption and multifactor authentication.

If you're not using Windows, don't assume you're safe - Apple OSX and iOS topped the list of reported vulnerabilities in 2014 and 2015!

Antivirus & Anti-malware

Antivirus & Antimalware protection is your last line of defence against malicious threats.

Always use a reputable AV vender to protect your data.

In addition, several dedicated anti-ransomware products are now on the market.

Choose your web browser wisely.

Recent tests showed Microsoft Edge to be more secure than its rivals.

Be careful which sites you visit, and always keep your browser up-to-date.

Exploit mitigation

Microsoft EMET is a free tool that blocks the most common actions and techniques used to compromise a computer.

EMET can help protect your computer systems, even from new and undiscovered threats before they're addressed.

Content filtering

Use content filtering to prevent access to malicious and nefarious websites.

Password security

Use a password manager to generate & store secure passwords, prevent phishing attacks, and keep informed of website security breaches.

AD Blockers

Consider using an AD blocker to prevent a new growing threat called Malvertising.

Malvertising involves injecting malicious or malware-laden adverts into legitimate webpages, then infecting computers as they load the advert.

Using the router supplied by your ISP? STOP!

Many routers supplied by Internet Service Providers (ISPs) can be compromised easily!

ISP supplied routers often have unpatched vulnerabilities, allowing a remote hacker to take control.

Consider replacing your router with a business or enterprise grade unit. Always keep the firmware up-to-date and change the default password.

Backup, Backup, Backup!

Keep a backup! In the event of infection or hardware failure, this could be the only way to recover your data.

Encrypt your data

If your operating system supports it, use drive encryption such as Bitlocker.

This will protect your data in the event of your device becoming lost or stolen.

For the latest news, tips & advice, follow us on twitter, or online:

Stay Educated, Stay Informed! @the_serverninja **www** the-server.ninja