East Midlands Special Operations Unit

COVID-19 CYBER AND FRAUD PROTECT MESSAGES

Wednesday 17 June 2020

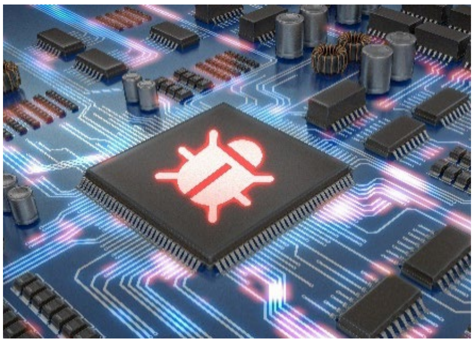
This advice has been collated by EMSOU and is intended for wider distribution within the East Midlands Region to raise awareness among businesses and the public.

Advice and information is changing daily as we navigate our way through the COVID-19 pandemic, so please ensure you only take information from reputable sources.

If you require any further information, assistance or guidance please contact the EMSOU Protect Team EMSOU Protect Team **or your local Force protect team.**

Today's topic is: Spyware

'Spyware', refers to a category of software that, when installed on a computer, may send pop-up ads, redirect your browser, or monitor the web sites visited. More invasive versions of spyware can even record what is typed on the keyboard.



Spyware may cause a computer to become slow or sluggish. There are also privacy implications including:

- What information is being gathered?
- Who is receiving it?
- How is it being used?

Spyware that record keystrokes, passes, important credentials and sensitive data to malicious threat actors to exploit for personal gain (identity theft, fraud etc.).

Symptoms that indicate spyware is installed on a computer may include the appearance of new and unexpected:

- Toolbars in the web browser
- Icons on the toolbar at the bottom of the screen
- Search engines employed by the browser
- Home page
- Pop-up windows
- Random Window error messages

Other indicators may be:

- The computer suddenly becoming sluggish (for example, when saving files).
- Being redirected to web sites other than the one entered into a browser

Mitigation strategies

Be wary of:

- **Links within pop-up windows**: These windows often install spyware. To close a pop-up window, click on the "X" icon in the title bar and not the "Close" button within the window.

- **Unexpected dialog boxes**: Which asks to run a program or perform another type of task. If in doubt, select "no" or "cancel," or close the dialog box by clicking the "X" icon.
- **Free software**: There are many sites offering customised toolbars or software that will appeal to users. Downloading programs from untrusted sites may expose you to spyware.
- **Following email links for anti-spyware software**: Like email viruses, these links may serve the opposite purpose and actually install the spyware it claims to be eliminating.

Also consider adjusting browser preferences; to limit pop-up windows which contain active content, which can be harmful. Certain types of cookies can reveal what pages a user has visited. Rather than deny by default, most browsers allow the user to fine tune which sites can use cookies so that the overall surfing experience is not adversely affected.

Removing spyware

Run anti-virus software for detection and removal. If problems persist run legitimate spyware removal tools from, trusted vendors. Be careful that the spyware removal software is compatible with the existing anti-virus software.

Always keep anti-virus software up to date and update your systems

Hot topics

Citizens Advice Bureau has warned users not to fall for a new scam campaign that sends fake messages, purportedly from the UK government. These messages come in the form of calls, text messages, or emails and relate to the new NHS test and trace service. Citizens Advice Bureau has reportedly received thousands of reports of this nature.

Claire’s Accessories online site checkout page was hacked by insertion of a malicious “card skimming” code which collected payment card information. The retail giant admitted that the malware exfiltrated payment card information from its e-commerce website but assured customers that cards used in retail stores were not affected by the issue. Any customers who made purchases on Claire's website between **April 30th** and **June 13th**, should contact their card company and monitor statements for fraudulent purchases.

Cycling equipment shop Wiggle were targeted in this type of attack and a small number of customer details were acquired. In response, Wiggle have taken steps to identify the compromised accounts and contact individual impacted. All accounts will now require the re-entry of card details for the next purchase. Wiggle customers are strongly advised, to change login passwords and check any cards previously used to make purchases.

Reporting

Please report all Fraud and Cybercrime to Action Fraud by calling 0300 123 2040 or online.

Forward suspicious emails to report@phishing.gov.uk.

Report SMS scams by forwarding the original message to 7726 (spells SPAM on the keypad).