East Midlands Special Operations Unit

COVID-19 CYBER AND FRAUD PROTECT MESSAGES

Monday 27 July 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: Malicious Code

Malicious code is any computer program that can cause harm to a computer and which can damage or expose data. Examples include:

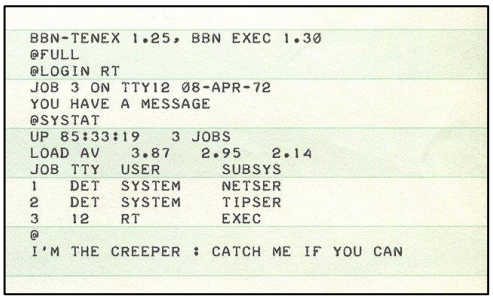
Viruses:

Viruses have the ability to damage or destroy files and are spread by; sharing infected media (such as a USB drive), opening a malicious email attachment, or visiting a malicious web site.

The 'Brain' virus, written in 1986 by Basit and Amjad Farooq Alvi, is thought to be the very first computer virus. The brothers ran a computer store in Pakistan and were so fed up of customers making illegal copies of their software, that they created code to display a copyright message on start up.

Worms:

Unlike a virus which requires a user to intentionally or unknowingly transfer it, a worm needs no human intervention. A worm will spread throughout a network by relying on the security vulnerabilities it finds. Worms can carry all sort of malicious payloads, including ransomware, backdoor access or code that will clog network traffic.



The very first worm appeared in 1971 and was written by Bob Thomas of BBN engineering. The program did little but self-replicate and display the message "I'M THE CREEPER. CATCH ME IF YOU CAN!"

Trojan Horses:

A Trojan horse appears to be innocent software but actually contains another, more malicious, program. Trojans can exfiltrate or destroy data; disable security mechanisms, cause a denial of service or turn the victim's computer into a proxy. The proxy can be used to commit identity theft, host illegal content or use the victim's system to attacks others.

In 1975, John Walker created a game based on 'guess what animal I am in 20 questions'. The game was extremely popular but could only be given to friends using magnetic tapes. To make life easier, Walker embedded the game in another program called 'Animal'. Animal examined the user's available directories and replicated itself, if it was not already installed.

Malicious data files:

Malicious data files exploits weaknesses in the software designed to open them. Classic examples include; a Microsoft Word document containing a macro, an Adobe PDF, a ZIP file, or an image file. Attackers frequently use malicious data files to install malware on a victim's system, commonly distributing these files via email, social media, and poisoned websites.

Mitigation Strategies:

- **Use antivirus software / firewall:** which will detect, block, sanitize or remove malware. Download antivirus software from a reputable vendor rather than clicking on advertisements or email links. Make sure the product updates to combat new threats and perform a 'manual' scan of any new files and folders. Many modern anti-virus packages come complete with a firewall that will block malicious traffic from the Internet.
- **Be careful of links & attachments:** Especially within unsolicited email.
- **Block pop-ups:** As some contain malicious code. This can be done in any modern browser via the privacy or security settings.
- **Disable auto run:** To prevent external media infected with malicious code from automatically running when plugged in.
- **Update software and patch:** Newer versions of software and a comprehensive patch management program will stop attackers exploiting known security flaws.
- **Back up data:** In the cloud or to an external hard drive. In the event of an infection, critical information will not be lost. Just be sure to back data up data, system configurations and anything else of value. Store backups securely and mark as read only.
- **Monitor accounts:** Such as bank accounts for unauthorized use, or unusual activity. Contact the account provider if there are problems.
- **Avoid public Wi-Fi:** Which can be used by an attacker to intercept network traffic and gain access to sensitive data.
- **Change passwords:** If systems have been infected. Consider using a credential manager to generate and safely store complex passwords.
- **Minimize damage.** Contact the IT department immediately - the sooner they can investigate and sanitise the less likely the machine will cause additional damage to other systems on the network. If at a home, disconnect the computer from the internet and run anti-virus.
- **Surf with limited permissions:** Network managers should never use administrative accounts to perform routine operations, to minimize damage across the network.

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).