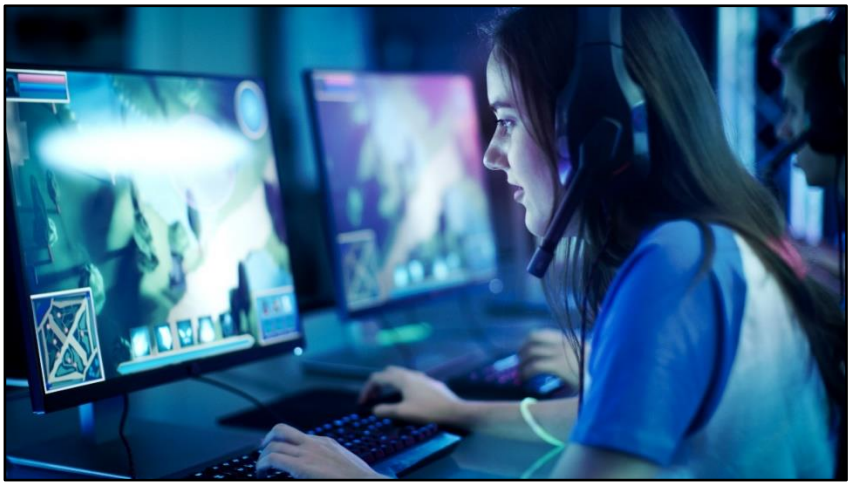
East Midlands Special Operations Unit

EMSOU CYBER SECURITY ARTICLE

Thursday 15th April 2021

This article has been written by EMSOU and seeks to promote good cyber security among businesses and the public. If you require any further assistance or guidance please contact the EMSOU Protect Team or your local Force Protect Team.



Today's Topic is: Online Gaming.

If you have any reason to doubt that gaming is big business, allow me to introduce Grand Theft Auto and Call of Duty. Rockstar Games purchase Grand Theft Auto for $265 million dollars back in 2013 and Call of Duty for a cool £250 million. Star Citizen by Cloud Imperium Games, surpassed both totals on development costs alone.

Part and parcel of this trend, is the rapid growth of online gaming. With faster data transfer speeds, and more powerful handheld devices (mobile phone, tablets and consoles), gaming is set to dominate the entertainment industry for some time to come. Unfortunately, the success of this industry has attracted all manner of cybercriminals. Learn how to protect your device, information and loved ones from such threats here:

1. Keep it up to date

No matter what your preferred device for online gaming is, it is important that it is configured to automatically update the operating systems, apps and games. Updates are regularly released by companies in order to introduce new functionality, balance game mechanics and resolve security issues. If your device is no longer supported – that's fine, but be wary of connecting it to the internet otherwise you could be opening back doors that are better kept shut. When purchasing a new device, consideration should be given to selecting a company that has a proven track record of providing timely updates.

2. Keep it legitimate

Modifying your device to bypass copyright or other security protections or buying pirated applications might, inadvertently, download malware or prevent apps from performing necessary updates, significantly increasing your chances of being compromised. Always download apps from legitimate well known suppliers and be wary of any applications that ask for excessive or suspicious permissions.

3. Backup your important files

Backup your important files to a USB stick, memory card, external hard drive or online storage service. That way, if you suspect malicious software on your device you can reset it without losing access to your important information. Ransomware is surprisingly common in the gaming industry these simple precautions maximise your chances of a full recovery without having to pay a cybercriminal and risk losing everything.

4. Always be suspicious of unsolicited communications

Unsolicited communications in the form of phone calls, SMS, instant messages, in-game chat and emails are often annoying and sometimes downright dangerous. These messages might encourage recipients to open a file or access a website that will compromise their device, access personal or financial information, or generate revenue for someone else via premium phone numbers, advertisements or app downloads.

Be especially wary of anyone who rings to tell you that a device, account or internet connection has technical problems. Always hang up and call the appropriate organisation using a trusted phone number.

5. Use different passphrases for accounts

Use unique passwords or passphrases for different accounts, especially for those that store any personal information. Using the same username and password for multiple accounts gives a single point of failure.

Users with many online accounts, should consider whether it is time to invest in a password manager. These affordable solutions will generate complex passwords, store them securely and autocomplete login pages on the users behalf.

Some accounts also offer the ability to use multiple steps to logon, such as a number sent via SMS to a mobile phone in addition to using a password or passphrase. The use of such mechanisms will vastly improve online security.

6. Avoid saving your payment details

Where possible, avoid saving payment details (such as credit card or bank account details) within accounts. Alternatively, look for options that enable a prompt, for a password, before a purchase can be made or using parental controls to limit purchases and in-game micro-transactions.

7. Monitor your online presence

Check privacy settings for your accounts especially if additional goods or services are added to an online gaming platform because these settings are likely to change. Also consider what information you post or is posted about you. Unfortunately, the larger a digital footprint the easier it is to steal personal data or commit identity theft.

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).