November BFBS Messaging: Online Gaming

Ensuring you are cyber aware when playing games online

Our reliance on the internet is ever growing and the popularity of online games has grown in tandem. Online gaming can be a great way to relax and provides social interaction between players. However, there can be a darker side as adversaries use the opportunity to build a shared online experience and gather information about you.

Most players you may play against are only identifiable by their gamertag and are often untraceable in the events of abuse of fraud. You could easily be playing with an adversary and may not even know. Sharing information about your work risks your personal and Defence's security.

For more guidance surrounding **Online Gaming**, visit the Cyber Confident in Defence SharePoint site, the Defence Connect page, or email the team at cyberconfident@mod.gov.uk. Remember, the cyber front line is you.

Keep your information private and protected

How many of us use the same password for every device, or even the same password to access our online accounts? This makes it incredibly easy for a hacker to intercept our accounts. According to Google, 52% of gamers reuse passwords across accounts. Just imagine how much information an adversary could gather across such a variety of accounts. Choose strong passwords for your accounts, following three random words guidance and use different passwords for each account. Remember to never share your password with others.

Just as important as passwords, is your username and gamertag. If your username reveals personal or work information, then it gives adversaries an opportunity to explore your profile more. If you're required to set up a personal profile, make sure you don't include any personal or work information and never use your MOD email address.

For more guidance surrounding **Online Gaming**, visit the Cyber Confident in Defence SharePoint site, the Defence Connect page, or email the team at cyberconfident@mod.gov.uk. Remember, the cyber front line is you.

Update your internet security

The internet is a massive network that connects your computer with the rest of the world, including malicious actors. It is a good idea to use firewalls to protect your computer from these threats. These can help safeguard your device from data-based malware dangerson the internet.

Before you play online games on a PC, Mac or mobile device, ensure you have effective and updated internet security running and the firewall switched on. Antivirus utilities are available on a variety of consoles, including PlayStation. Antivirus is not deemed relevant for Xbox owing to its software architecture.

For more guidance surrounding **Device Cyber Security**, visit the [Cyber Confident in Defence SharePoint site](#), the [Defence Connect page](#), or email the team at cyberconfident@mod.gov.uk. Remember, the cyber front line is you.

Play Safe

Do you know what credential stuffing is? Well, it's a subset of brute force attacks where adversaries attempt multiple passwords against one or multiple accounts. The gaming industry accounted for 11 billion credential stuffing attacks in 2020!

It's vital that we play safe and ensure we exhibit responsible cyber security behaviours whilst online gaming. For instance, only play games purchased from authorised sources and for which you have a licence. Be alert for scams and cons when buying or selling in-game assets and check forums for reports of negative activity. In the worst-case scenario where you become the victim of any kind of online abuse, do not retaliate, instead, close the conversation, block and report the abuser.

For more guidance surrounding **online gaming**, visit the [Cyber Confident in Defence SharePoint site](#), the [Defence Connect page](#), or email the team at cyberconfident@mod.gov.uk. Remember, the cyber front line is you.