GUIDANCE

Online gaming for families and individuals

How to enjoy online gaming securely by following just a few simple tips

Many people love playing games online. In fact, an estimated 1.2 billion of us are regularly logging on, signing up and playing online.

Unfortunately, whenever money or personal data is changing hands online, criminals can be watching, looking for some way to turn the situation to their advantage.

The advice outlined below is intended to help safeguard you and your personal data when gaming. Whether you use a PC, console, phone or tablet, these steps will help prevent you falling victim to a criminal. This will leave you free to focus on enjoying the game.

1. Secure your devices

The majority of cyber attacks exploit publicly known weaknesses in devices and software. Keeping your software up to date will help to prevent these attacks from being successful.

Keep operating systems, and other software up to date. The easiest way to do this is to turn on automatic updates, if you can.

Where possible, adding another layer of defence to your devices in the form of antivirus software is a sensible precaution. This should also be kept up to date.

2. Account protection

Your gaming account (or accounts) should be well protected with a strong password, ideally one which you don't re-use on other accounts. You should also turn on two factor authentication if available which will provide you with an extra layer of protection to prevent someone hacking into your account.

3. Protect your privacy

Try to keep the information that you share online to a minimum. Apply privacy settings to ensure your personal data isn't visible to other players, and do not give out personal information to other players, 'in-game'.

When disposing of your old game consoles and other devices, make sure you delete all your personal data and account details.

4. Use official sources or stores

Whatever device you are using to play games, you should always attempt to verify the source of anything you install. The easiest way to do this is to use official sources and stores.

Cyber attackers often attempt to circumvent in-game security measures by persuading you to do something outside of the game itself. For example, a player you don't know may suggest that you install an 'upgrade' and supply a link for the download. The offer could also come in the form of a well crafted phishing email, promising some kind of freebie related to a game you enjoy.

By relying on the official sources for all your software you are much less likely to accidentally install malware on your computer, tablet or other device.

Protecting younger players

For those with younger family members to think about, online gaming can be a concern. From cyberbullying, to excessive time spent playing games, to unscrupulous games which encourage children to pay for content. Here are some useful external links to sources of information:

Gaming: What parents and carers need to know *(www.thinkuknow.co.uk)*

Online gaming safety tips for parents *(www.internetmatters.org)*

Buying a games console for your child *(www.internetmatters.org)*

Review of sites, apps and games *(www.net-aware.org.uk)*

PUBLISHED

17 January 2019

REVIEWED

17 January 2019

VERSION

1.0

WRITTEN FOR

Individuals & families