Australian Government
Australian Signals Directorate

ACSC Australian Cyber Security Centre

Security Tips for Online Gaming

First published: December 2020
Last updated: November 2022

Introduction

There are many things to think about when it comes to using your personal or gaming devices to create a safe and secure online gaming experience. The security tips in this publication can help you prevent your device or information being compromised.

Use legitimate software and keep it up to date

It is important that your online gaming devices are configured to automatically apply updates for operating systems, applications and games. These updates are regularly released by companies in order to introduce new functionality, balance game mechanics and resolve security problems. New versions of operating systems, applications and games can include new security features to make it harder for devices to be compromised, or for other gamers to cheat.

When the operating system on a device is no longer supported, you will no longer be able to receive updates. You should consider whether you need to change to another device that is currently supported.

When purchasing a new device, you should consider selecting a device that is currently supported by a company that has a proven track record of providing timely updates. This can be to varying degrees depending on the company.

Finally, you should always use legitimate applications and games purchased from reputable companies through a trusted physical store, online retailer or app store.

Do not use illegal applications and games. If you modify your device to bypass copyright or other security protections, or use pirated applications or games, the device may become compromised or won’t be supported with updates. Care should be taken to avoid applications or games that ask for excessive or suspicious permissions.

Backup your important files

Backup your important files (such as your games’ save files) to a USB, memory card, external hard drive or online storage service. If you have a problem with a device and it needs to be reset or replaced, you will still have access to your important files if you have completed a backup.

Having a recent backup can also assist you in recovering files if a device is compromised by malicious software.

Be suspicious of unsolicited communications

Unsolicited communications can come in the form of phone calls, SMS, instant messages, in-game chat and emails. They often try to get you to do something that will benefit someone else.

It might just be spam, or someone might be trying to get you to open a file or access a website that will:

- Compromise your device,
- Access your personal or financial information.

If someone has sent you an SMS, instant message, in-game chat or email that you think is strange (such as requests to open a file, access a website, or provide personal or financial information), ignore it.

Turn on multi-factor authentication

You should turn on multi-factor authentication (MFA) for your gaming accounts. This will help protect them from being compromised. MFA is when you use two or more different types of actions to verify your identify, and you may already be using MFA. For example, when you receive an authentication code by SMS text message after entering your password to log into an online account

Start with your most important accounts, such as those that store payment information or have digital purchases.

How to turn on MFA depends on the service you are using. Below are some links on how to use MFA on some of the most common gaming platforms:

- Steam
- PlayStation
- Microsoft
- Nintendo
- Epic

Note that this list is not exhaustive. If you don't see your account listed above, we recommend searching online for 'how to turn on MFA' for that service, or check the settings of your account.

Use different passphrases for accounts

Use different passphrases for accounts, especially for those that store any personal information. If you use the same username (such as an email address) and passphrase for a number of accounts, and one account is compromised, someone accessing that information is more likely to be able to access other accounts you use.

It is also important that the email address you use for accounts has a unique passphrase that has not been used elsewhere. Someone that knows, or can easily guess, the passphrase for your email address could use the reset functionality and gain unauthorised access to all the accounts your email address is linked to.

Avoid saving your payment details

Where possible, avoid saving your payment details within your accounts. This includes your credit card or bank account details. Alternatively, should you choose to save your payment details for convenience, consider enabling a prompt for your passphrase before each purchase is made.

You can also implement the parental controls that are provided by companies to limit the purchase of applications, games and in-game micro-transactions. Finally, if you are wary of providing your payment details to companies, consider whether there are viable alternatives. For example, using a trusted third-party, purchasing pre-paid cards or using pre-paid store credit.

Monitor your online presence

It is best not to put too many personal details online. Check your privacy settings for your accounts to make sure you know who can see your information and to what extent. Privacy settings sometimes change after functionality is added to online gaming platforms so it is important to check them regularly.

Also, consider checking the information that others put online about you. While some information might not seem important, many pieces of information can be put together to form a picture about you. Never assume that anything you do or post online or in-game will remain secret.

Do not provide personal information when requested by other gamers. If your personal information is available to others it can potentially be used against you. This could range from something as simple as sending you spam emails to something as serious as accessing your accounts, and stealing or deleting all your information. It can even result in identity theft.

Further information

Further information is available from the eSafety Commissioner on:

- online gaming by children
- popular apps, websites and games
- cyberbullying and abuse

Read more on common types of scams. Learn how to make a report if you have seen, or are a victim of a scam. You can also report if your device or information has been compromised.

More information on shopping online for devices and gaming securely is available from the following sources:

- the Australian Competition & Consumer Commission
- the eSafety Commissioner
- the Australian Securities & Investment Commission
- the Australian Border Force.

Contact details

If you have any questions regarding this guidance you can write to us or call us on 1300 CYBER1 (1300 292 371).