Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE

ACSC Australian Cyber Security Centre

# Security tips for online gaming

Content Complexity
**SIMPLE** ●○○

cyber.gov.au

# For more cyber security advice

For more information on how to improve your cyber security, see our other guides at cyber.gov.au

## *Personal Cyber Security Series*

PERSONAL
CYBER SECURITY
FIRST STEPS

cyber.gov.au

PERSONAL
CYBER SECURITY
NEXT STEPS

cyber.gov.au

PERSONAL
CYBER SECURITY
ADVANCED STEPS

cyber.gov.au

## *Protect your children online*

Protect your children online

A guide to cyber security for parents and carers

Content Complexity
SIMPLE ●○○

cyber.gov.au

## *Protect yourself online*

Protect yourself online

A guide to cyber security for young people

Content Complexity
SIMPLE ●○○

cyber.gov.au

# Table of contents

# Security tips for online gaming

The world of online gaming is a popular target for scammers and cybercriminals. Gaming accounts can provide access to game licenses and linked payment methods, making them highly valuable.

You should protect these accounts the same way you would protect your bank or email accounts. Cybercriminals might also use gaming as a way to scam you or compromise your device with malware.

Follow these tips to protect against security risks such as viruses and account takeovers.

## Case Study

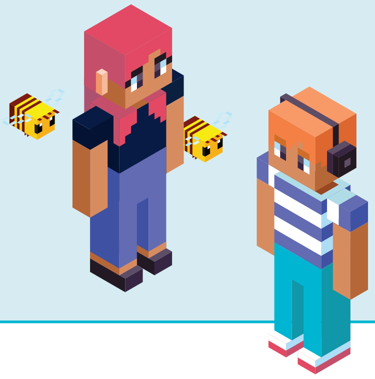
A teenager from WA made an online friend on the social messaging platform Discord. The two friends chatted online and played Minecraft together.

Through Discord, the online friend shared a file and told the teenager to download it. Even though they felt unsure about it, the teenager decided to trust the online friend.

When the teenager opened the file, a malicious screen opened and closed.

The online friend then sent back personal information about the teenager to threaten them. This included details such as their device location and email address.

This incident could expose the teenager or their family to further attacks.



## Turn on multi-factor authentication

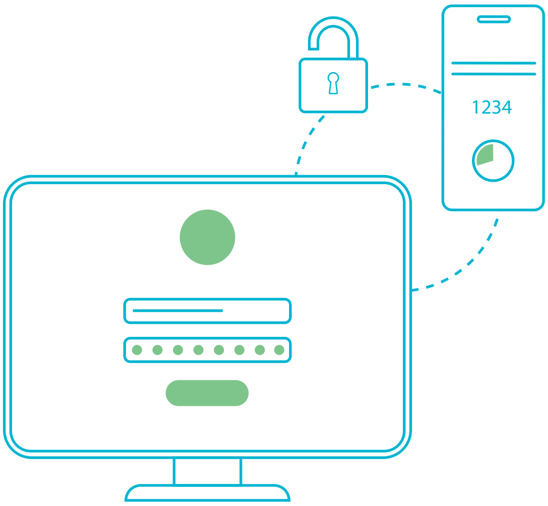
Protect your gaming accounts with multi-factor authentication (MFA) where possible. This will add an extra layer of protection to your account that helps keep cybercriminals out. MFA can also warn you when someone is trying to use your login details.

Prioritise accounts that have payment information saved or that are high value. For example, accounts with large game libraries.

How to turn on MFA depends on the service you are using. If possible, use an authenticator app instead of SMS or email verification methods.

MFA is often switched on in the settings menu of your accounts. If you're not sure, do an online search for 'how to turn on MFA' for that service.

For more information, including links to how-to guides, visit cyber.gov.au/mfa



## Use different passphrases for accounts

Use a different passphrase for each of your accounts. If you use the same login details for every account, and just one of these accounts is compromised (for example, in a data breach), all your other accounts are at risk.

You should especially use a different passphrase for your email account. If someone gains access to your email account, they could use this to reset passphrases for all your accounts that your email address is linked to.

Consider using a password manager to help you create and store strong, unique passwords for each account.

For more information on passphrases and password managers, visit cyber.gov.au/passphrases

## Avoid saving your payment details

Avoid saving payment details (such as card numbers and PayPal information) for your accounts. If someone gains access to your account, they could use this to make purchases with your money. For example, purchasing games or currencies as "gifts" for other accounts.

Sometimes you may be required to provide payment details to create an account or use a service. If this is the case or you want to save payment details for convenience, consider the following protections:

- Where possible, turn on settings that ask for your passphrase when making a purchase.
- Turn on parental controls to limit purchases, including in-game microtransactions.
- Use a pre-paid Visa or Mastercard instead.

This will minimise the potential costs if your account is compromised.

You could also consider using pre-paid gift cards for purchases, instead of your card details. For example, Steam or Nintendo eShop cards available at major retailers.

## Be wary of scams

Cybercriminals target gamers using scams. These tricks aim to take money, account information, and even things from in-game, like items or currency.

### In-game currencies, items, cosmetics or services

Be wary of **unofficial** or third-party advertisements for free or paid add-ons, such as:

- game currencies
- cosmetics and skins
- power upgrades
- services such as cheats and boosts.

**You should only purchase these add-ons from official sources. For example, from within the game or from the game's official website.** Avoid third-party websites and services, as these could be a scam or an attempt to get your login details.

Be wary of other players who may attempt to steal your in-game items or currency, especially on games or platforms that allow trading.

### Buying games and consoles online

Buying games or consoles through an unofficial online store or marketplace can carry a risk. Search 'online shopping' on cyber.gov.au for tips on avoiding scams.

### Unsolicited communication

You may receive unsolicited communications through in-game chat, emails and messaging apps such as Discord. It might just be spam, or someone might be trying to get you to compromise your device or information.

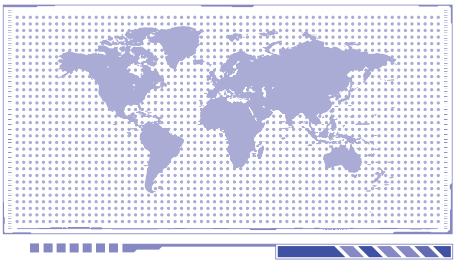
If you receive a strange message or request, for example to download a file or open a link, ignore it and report it to the service you are using. Never click on links asking you to confirm your login details.

## Monitor your online presence

Avoid sharing too many personal details online. If your personal information is available to others it can potentially be used against you. This could result in targeted scams, account takeovers, or even identity theft.

Follow these tips when online gaming or streaming:

- Do not use personal information in display names or profiles.
- Check your privacy settings for your accounts to make sure you know who can see your information and to what extent.
- Do not give out personal information to other players.



## Keep software up to date

Software updates are important for your security. They can also improve your gaming experience by introducing new features, improving performance and fixing bugs. Most games and devices will require you to have the latest updates in order to play online.

Install updates when they are available for your games and devices. Where possible, enable automatic updates. If you are PC gamer, you should also update your operating system (e.g. Windows, macOS or Linux) for the best security. For more information visit cyber.gov.au/updates

Ensure you also install or enable antivirus software on your device.

## Use legitimate software

Only use games, applications and mods that you know are legitimate. Fraudulent or pirated software could contain malware, or may not receive updates. When downloading and installing new software, follow these tips:

- Only use software from official sources such as reputable retailers and app stores.
- Before downloading new software, even from app stores, verify it is legitimate (e.g. look at reviews or do a search online).
- Do not use pirated software, or modify your device to bypass copyright or security protections.
- Avoid software that asks for excessive or suspicious permissions, or software that recommends turning off your antivirus.
- Avoid third-party services, such as unofficial trading or account marketplaces.

## Back up your important files

Regular backups can help you recover your information if it is lost or compromised.

Back up your important files (such as save files) to a USB, memory card, external hard drive or online storage service. You may require a paid subscription to back up to the cloud on some devices. For more advice, visit cyber.gov.au/backups

## Reset your gaming devices

Make sure to reset your gaming devices, including any memory or SD cards, before selling, trading, or giving them away. If you do not, other people could access information stored on these devices.

## Tips for parents and carers

- Make sure your child's accounts have **multi-factor authentication** switched on and are protected with **unique passphrases**.
- **Avoid saving card details** to accounts when making a purchase, or remove them from the account once no longer required.
- **Use parental controls** to limit financial loss if accounts become compromised.
- If your child asks you to purchase games or items such as currencies or cosmetics, make sure you **use an official platform**. For example, the game's official website or from within the game itself.
- Make sure gaming devices are **updated and backed up regularly**, and reset them to factory settings before getting rid of them.

More detailed advice is available at cyber.gov.au/families

## Further Information

### Have you been hacked?

If you believe one of your accounts or devices has been compromised, use our Have you been hacked? tool for further advice. Search 'Have you been hacked' on cyber.gov.au

### Information on scams

Learn more about scams at cyber.gov.au/scams, including 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.

### Resources from eSafety

The eSafety commissioner has further information on online gaming, popular apps, and cyberbullying available at eSafety.gov.au

**Disclaimer**

The material in this guide is of a general nature and should not be regarded as legal advice or relied on for assistance in any particular circumstance or emergency situation. In any important matter, you should seek appropriate independent professional advice in relation to your own circumstances.

The Commonwealth accepts no responsibility or liability for any damage, loss or expense incurred as a result of the reliance on information contained in this guide.

**Copyright**

**Use of the Coat of Arms**

The terms under which the Coat of Arms can be used are detailed on the Department of the Prime Minister and Cabinet website (www.pmc.gov.au/government/commonwealth-coat-arms).

**For more information, or to report a cyber security incident, contact us:**

cyber.gov.au | 1300 CYBER1 (1300 292 371)

Australian Government
Australian Signals Directorate

ASD AUSTRALIAN SIGNALS DIRECTORATE
ACSC Australian Cyber Security Centre