# HOW TO PROTECT YOUR ONLINE IDENTITY FROM CYBERCRIMINALS

**Every day cybercriminals steal the online identities of people just like you. It doesn't matter if you're young or old, whether you are male or female, or where you live. Cybercriminals are always looking to take advantage of people who make it easy for them to steal from.**

The internet is an essential tool in our everyday lives. We use it to shop, connect with family and friends, pay bills, run our business and more. But the online world can also give cybercriminals opportunities to steal your money, information or identity.

The good news is that you can take simple steps to better protect your personal and financial information online.

## What is your online identity?

Your online identity is made up of many things. It includes your name, date of birth, address, bank account details, credit card numbers, driver's licence, passport, and even photos you share with friends.

All these pieces of information can be accessed by cybercriminals if you don't take the necessary steps to keep your information private and secure online.

## Keep your social media private and secure.

It's fun to share updates and images on your social media. But when you do, you could be letting cybercriminals know all sorts of information.

Imagine this: It's your friend's birthday. You leave a happy birthday message on their social media page. If your social media is set to "public" a cybercriminal now has their name, date of birth, and location. All information they can use to steal their online identity.

Good privacy settings can keep your information safe so check the settings on all your social media accounts.

**Privacy Setting Top Tips:**

- Set your page or profile to private
- Limit who can see your contact and bio information and what you share
- Disable location sharing on social media platforms
- Only accept friend requests or connections from people you know or through people who you trust

## Don't get scammed by email, SMS or social media messages.

Many of us use the internet to do our banking, shopping and pay bills. It's made our lives easier, but with that ease, has come an opportunity for cybercriminals to steal important financial information.

For instance: Have you ever received an email from a bank asking you to click a link to log in to your account? Chances are it could have been a fake. A bank will never ask you for this type of information in an email. This is called "phishing" and it catches out thousands of people every year.

If you receive a message that seems suspicious, too good to be true, or you just have a funny feeling about it, there are a few things you can do.

**Phishing Top Tips:**

- Don't reply to suspicious messages.
- Never click a login button on a message.
- If a bank or business sends you a message asking for your account names, account numbers or similar, call them and ask if the really sent the message? Make sure the number you call is not from the message, but from their real website.
- Use a spam filter on your email. That often weeds out most suspicious emails.

## How to keep your passwords safe.

We all know passwords are important. They're the first line of defence in keeping our online information safe. But if you make yours too simple, or you use the same password on multiple online accounts, cybercriminals can quickly get into your accounts and steal your identity.

**Password Top Tips:**

- Create a long password, at least 13 characters long, using words only you would know. Such as "squirrelkneefly"
- Never use simple or sequential numbers or letters like "abc", "1234" or "000".
- Use different passwords for each account.
- Never share your passwords with ANYONE.
- Turn on a second-layer of security known as two-factor authentication (2FA). What's that? Many websites now give you an opportunity to sign in using your password and another form of ID (such as a unique code sent to your phone).

**Together we can reverse the threat of cybercrime.**
**staysmartonline.gov.au**/reversethethreat