

# REVERSE THE THREAT

STAYSMARTONLINE

WEEK 8-14 OCTOBER 2018

## Passwords Are Your First Line of Defence

**Think of your password like a key  
- instead of unlocking a door,  
it unlocks your online life.**

Weak passwords are easy for criminals to guess. There is software that can guess billions of passwords per second. If a cybercriminal guesses or steals your password, they can use it to commit a host of cybercrimes including:

- Sending emails from your accounts, pretending to be you
- Withdrawing money from your bank accounts
- Accessing files on your computers
- Stealing your identity

**59%**  
**OF PEOPLE**  
use the same password  
across all accounts\*

\* Last Pass, The Psychology of Passwords:  
Neglect is helping hackers win (2017)

### Create strong passwords

- **A long password is a strong password:**  
Develop a long password or passphrase made up of at least four words and at least twelve characters in length, such as 'horsecupstarshoe'. Pick words that are meaningful to you so it is easy to remember.
- **Don't use repeated or sequential characters:**  
Don't use the same characters (for example 999) or obvious sequences (such as 12345 or qwerty).
- **Don't use predictable information:**  
Never include your date of birth, name or other identifiable information in your passwords. Also avoid incorporating a month or a year in your password.
- **Use different passwords for every account:**  
Otherwise if a cybercriminal gets hold of your password, they could access all of your accounts.
- **Never share your password with anyone:**  
Your passwords belong to you. Never share them with anyone; not even your partner, parents or children.
- **Use a reputable password manager to store complex passwords:**  
Remembering lots of unique, complex passwords can be hard. A password manager can make this easier by generating strong passwords, remembering these passwords and syncing them across devices.

### Sign up for two-factor authentication

Two-factor authentication (2FA) adds an extra layer of security to your accounts. It provides a way of 'double-checking' that you're really the person you claim to be when logging into an online account.

With 2FA, you need to provide two things — your password and something else, such as a code sent to your mobile device or your fingerprint — before you can access your account.

Two-factor authentication is not a new concept but is gaining momentum. Some online services will automatically prompt for a second factor when you login while others might have to be manually activated. You will find this in the security or privacy settings of your online accounts.

### Tips to recover

- **If you think your password may have been compromised,** change it immediately and check for any unauthorised activity.
- **If a password has been compromised and you use it for more than one account,** change your password on all of your accounts.

**For more information**  
on how to reverse the  
threat of cybercrime and  
Stay Smart Online, please visit:  
[staysmartonline.gov.au/  
reversethethreat](https://staysmartonline.gov.au/reversethethreat)



Follow us on  
Facebook  
[fb.com/staysmartonline](https://fb.com/staysmartonline)



Sign up to our free alerts  
[staysmartonline.gov.au/  
alert-service](https://staysmartonline.gov.au/alert-service)