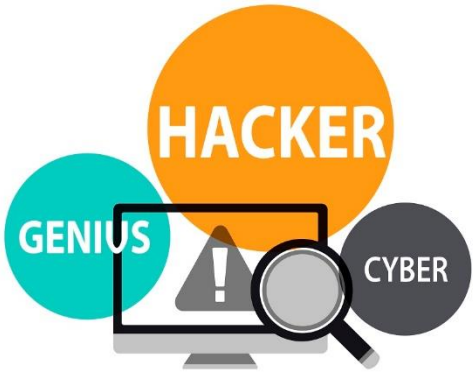
Endeavour Foundation

# Cybercrime

## 6 fast facts you should know!

**Cyber crime or cyber attacks describe a range of online criminal activities carried out against individuals, businesses and governments.**

**It's on the rise and there are key threats everyone should know about and how to protect yourself and Endeavour Foundation against them.**




**60%** of cyber crime is committed by a "frenemy" – a cyber criminal posing as an employee, customer or supplier!

Cybercrime costs the Australian economy **$1billion** directly each year

**1 in 3** Endeavour Foundation employees clicked on a link in a test spam email in 2018

**$1.9million** is the average cost to medium-sized Australian businesses

**25 hours** average downtime is experienced by businesses hit by cyber attacks

**One** is the number of employees hackers need to fool to gain access to our business data


**Cybercrime can take many forms, and in nearly all instances the goal of cyber criminals is to either steal directly from you, or force you to pay a ransom.**

## Some common ways include:

1. Tricking you into revealing your username and password for sites such as online banking, webmail, share trading or online auctions.

2. Stealing your identity to impersonate you and gain access to other accounts and services.

3. Crafting scams to appeal to human curiosity, empathy and emotion.

4. Convincing you they are a manager requesting funds to be transferred, supplier requesting an invoice payment, or you are the recipient of a large gift or inheritance.

5. Using social media accounts to identify key personnel within a company.

## Don't be a victim of cybercrime!

1. Treat every email as suspicious. No matter how authentic an email looks, don't click on a link which takes you to a login page or asks you to install software. Visit the company's web page using its known address to log in.

2. Don't provide personal information if the caller asks to connect to your computer or to provide your login details. If in doubt, ring the company they claim to be from on its published phone number.

3. Our computers have up-to-date anti-virus and firewall protection, but you should do this for your home computer as well.

4. Try to use a different password for each of your online services.

### What should you do if you receive a suspicious email of phone call?

Notify the Technology Service Desk.

✉ Never reply to emails which appear suspicious. Instead, attach the spam email to a new email and forward to spam@endeavour.com.au.

✆ 1300 742 212

▶ Watch the cyber security video that is part of you mandatory training program.

## More information

Stay up-to-date on the latest cyber scams at the Australian Government's Scam Watch website

NDVR Endeavour Foundation