# PROTECT YOURSELF KNOW THE SCAM



## ROMANCE

Scammers use the internet to target people and build fake relationships. They convince individuals that the relationship is real and manipulate them into giving them money.



#### **INVESTMENT**

Scammers use convincing marketing to make their fake "investment opportunity" sound risk free and promise large returns. People are put under pressure and told to act fast or miss out.



## **THREAT OF ARREST**

Scammers will impersonate organisations, claiming people owe money or need to make a payment. They often use threats of arrest, deportation or harm if they don't agree.



### **REMOTE ACCESS**

Scammers impersonating banks and other businesses will offer technical support by requesting remote access to their computer or device. Once granted, the scammers will have access to their personal information and money.



### SEXTORTION

Scammers trick people into sending intimate images or videos of themselves and then threaten to share them unless a payment is made.



## **ONLINE SHOPPING / MARKET PLATFORMS**

Scammers create fake websites and advertisements or pose as buyers on market platforms leading people to pay for items they'll never receive or give away items without receiving the money.



#### IMPERSONATION

Scammers trick people into believing they're communicating with a family member, friend or a well-known person or business. They will request money or personal information.



## **BUSINESS EMAIL COMPROMISE**

Scammers use compromised business email accounts to carry out fraudulent activities, such as issuing false invoices or redirecting funds from legitimate invoices into their own bank accounts.

If you are the victim of a cybercrime, you are encouraged to report at cyber.gov.au/report



