COVID-19 cyber and online risks in Australia

The stats

150+
malicious COVID-19 themed websites disrupted by ACSC

645
COVID-19 related products identified by Australian Institute of Criminology for sale on dark web

1,100+
reports of COVID-19 cyber scams to Scamwatch

20+
cyber security incidents impacting COVID-19 response services responded to by ACSC

86%
increase in online image based abuse reports

115+
cybercrime and cyber security incident reports to ACSC

40%
increase in cyber bullying

What the regulators are saying

"With social isolation now in full force in most homes around the country, children and young people's online activities are increasing — for education, to socialise with friends and for entertainment. … we know first-hand the risks associated with children and young people spending more time online"

Julie Inman Grant
eSafety Commissioner

"The social distancing measures that help protect the community against COVID-19 can also make them more vulnerable to malicious cybercriminals. The unauthorised compromise of information can have a devastating impact on a person's emotional, financial and working life."

Abigail Bradshaw
Australian Cyber Security Centre

"We are hitting back through the Australian Signals Directorate, who have already successfully disrupted activities from foreign criminals by disabling their infrastructure and blocking their access to stolen information."

Senator Linda Reynolds
Minister for Defence

"…scammers are using the uncertainty around COVID-19 … to take advantage of people … Understandably, people want information on the pandemic, but they should be wary of emails or text messages claiming to be from experts."

Delia Rickard
Deputy Chair, ACCC

COVID-19 scams - case studies

1. International health organisation

Phishing email inviting recipient to click link for information about COVID-19 in their local area.

2. Postal service phishing email

Phishing email impersonating Australia Post providing link to travel advice.

3. COVID-19 testing

SMS phishing campaign from 'gov' inviting recipients to click a malicious link to a website hosting malware.

4. Economic stimulus payment

Phishing email sent to employees of a company with a link to receive a benefit payment.

5. Fake bank phishing text

SMS impersonating banks requesting confirmation of personal information for their safety due to COVID-19.

HWL EBSWORTH
LAWYERS