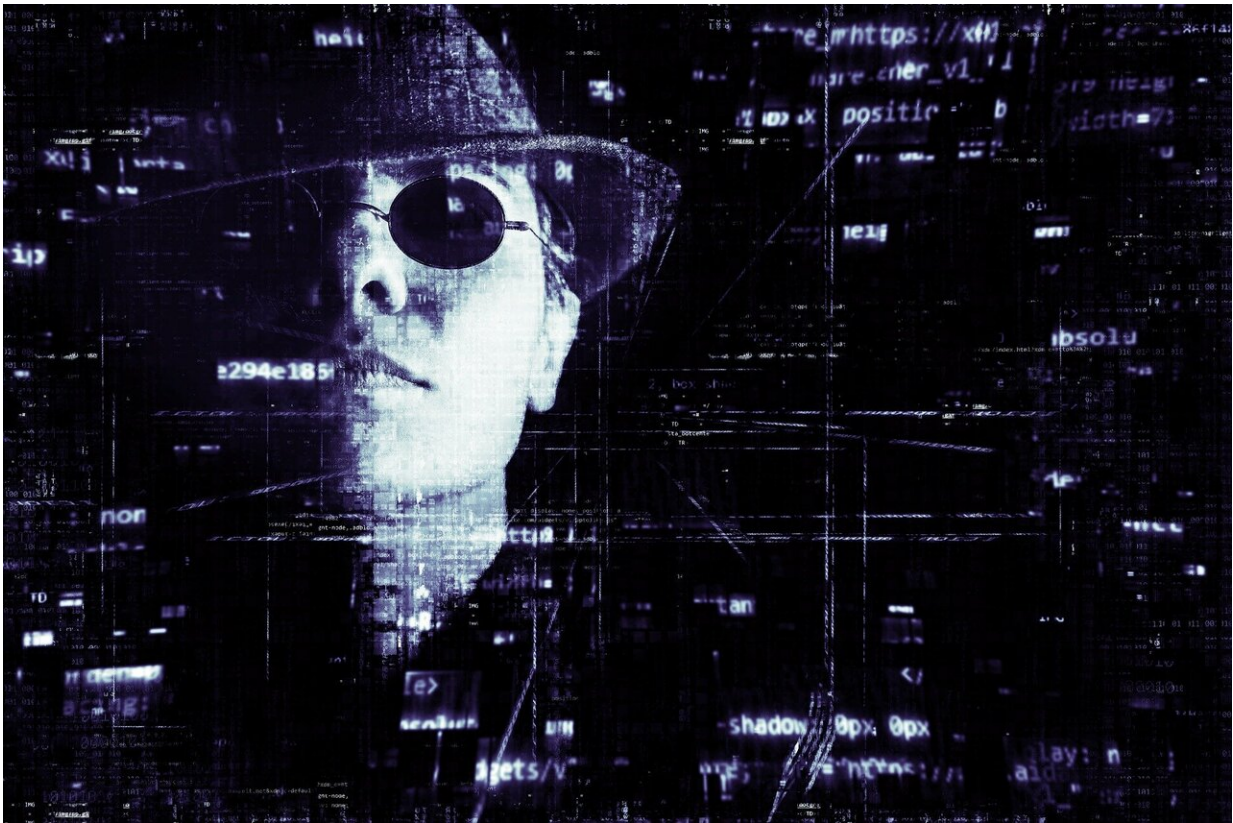# Warning on rising cybercrime during the pandemic

July 21 2021

Credit: CC0 Public Domain

A new [study](link) of almost 12,000 Australians has found one-third of the adult population has experienced pure cybercrime during their lifetime, with 14% reporting this disruption to network systems in the past 12

months.

With all forms of cybercrime already costing trillions every year globally, experts from the Australian Institute of Criminology (AIC) and Flinders University say the crimes involved substantial levels of personal victimization including direct losses as well as the high cost of preventing future attacks.

A pre-COVID-19 snapshot of the cost of 'pure cybercrime' in 2019 has found an approximate total economic hit of $3.5 billion—comprising $1.4 billion spent on prevention costs, $1.9 billion in money directly lost by victims and $597 million spent dealing with the consequences of victimization.

With only about $389 million recovered by victims—barely paying for the cost of dealing with the incidents—the survey estimated about 2.8 million Australians had been hit within the past year and nearly 6.7 million Australian adults could have been victims at any time in the past.

Only a small proportion of financial losses are recovered by victims.

"Pure cybercrime' activities include hacking, spreading viruses and other malware, and distributed denial-of-service attacks. While this involves crimes against machines and networks, it is estimated other forms of cyber-enabled identity crime cost Australian government agencies, individuals and businesses additional sums of more than $3bn a year.

"Pure cybercrime is a highly profitable criminal activity and results in substantial financial losses to Australians," says Flinders University Professor Russell Smith, who also warns of a potential rise in online fraud as a result of opportunities for dishonesty created by COVID-19-related economic disruptions.

"On current information, as cybercriminals become more sophisticated, it's clear the need for additional expenditure on prevention will need to increase.

"Equally, it is imperative that the financial harms associated with cybercrime are assessed so that resources for prevention and response activities can be targeted most effectively, and a baseline can be developed against which to measure the impact of future policy responses," Professor Smith says.

[A 2018–2019 investigation into identity crime (Smith & Franks 2020)](#) found a cost of $3.1 billion to Commonwealth entities, state and territory agencies (including police), individuals and businesses—most of which, but not all, was a consequence of cyber-enabled identity crime.

Cyber-enabled offenses use technology to make conventional crimes such as identity theft, fraud, stalking and harassment easier to commit and with a lower risk of detection.

"Cybercrime is a growing, borderless and continually evolving body of crimes which can threaten individuals, businesses, government and national security," says lead author in the new AIC publication," Mr Coen Teunissen.

"This study represents the first large-scale Australian study of pure cybercrime prevalence and financial harm.

"Importantly, this is a conservative estimate, as many victims were unable to report how much they had lost or how much they had spent dealing with the consequences of cybercrime. This also excludes the cost to business and government from pure [cybercrime](#)," Mr Teunissen says.

 More information: Coen Teunissen et al, Estimating the cost of pure

cybercrime to Australian individuals, (2021). DOI: 10.52922/sb78269
Coen Teunissen et al, Estimating the cost of pure cybercrime to Australian individuals, (2021). DOI: 10.52922/sb78269

Michael Levi et al, Fraud and its relationship to pandemics and economic crises: from Spanish flu to COVID-19, (2021). DOI: 10.52922/rr78115

Russell Smith et al, Counting the costs of identity crime and misuse in Australia, 2018-19, (2021). DOI: 10.52922/sr04756

Provided by Flinders University