WHY ARE GOVERNMENT ORGANISATIONS A TARGET FOR CYBER CRIMINALS?

CYBERCRIME INDUSTRY SNAPSHOT

Government

CYBER
READY

mailguard

Governments are targeted by cybercriminals due to the value of mass data

Government agencies are gate keepers for highly confidential data records. Massive databases are a treasure trove for cybercriminals, who attempt to hack the data using common email scams and sell it on the dark web. The larger the data set, the larger the potential victim pool and financial gain.

Cyberterrorism, compromising and attempting to cripple a country's critical infrastructure, is also a prime motivation for criminals. These insidious attacks result in enormous financial damage and operational downtime, triggering economic turmoil and potential risk to human lives, as demonstrated in 2010 during Iran's nuclear facility crisis.

The Stuxnet worm virus gained access to a government computer network through targeted phishing emails, infecting a Ukrainian power grid, and causing a six-week blackout for 235,000 households.

Due to brand recognition and authority of government agencies, **people are more likely to open an email from the tax office, federal police, or other government agencies.** Government bodies are susceptible to spear phishing email attacks, where seemingly legitimate emails containing malicious links or files are sent mimicking established and trusted government agencies, businesses, or individuals (also called 'social engineering' or 'brandjacking') giving cybercriminals unauthorised access to confidential data.

Some high-profile incidents

21.5 million personal details stolen

in a phishing scam targeting U.S. Federal Agency Office of Personnel Management

FBI & DHS records were siphoned

totalling 200GB by a hacker in 2016

Global Petya hit Queensland Health

affecting patients across five public hospitals and compromising electronic medical records in 2017

Brisbane City Council were victims

losing $450,000 of taxpayers' money in August 2017

The cybersecurity landscape for government

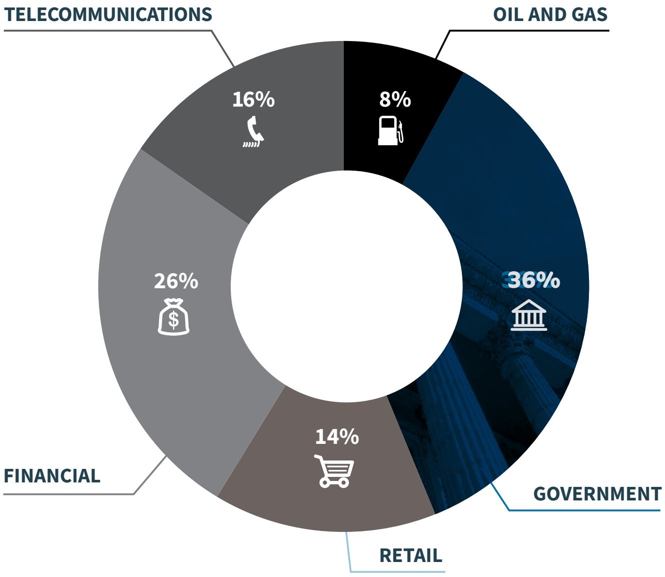
As government services go digital, with some countries now allowing people to vote, pay bills, and access prescriptions using a single digital citizen identification (ID), criminals have lapped up the potential for fraudulent claims and theft. According to a KPMG report, more than 11 million users or 44.6% of Australia's total population, are registered with myGov which holds sensitive information from the Australian Taxation Office, Medicare and Centrelink.

Nation-state attacks are being carried out with increasing frequency. In 2016 the US Presidential election was thrown into turmoil when Russian Military Intelligence purportedly sent phishing emails to over 100 local election officials. The Australian government was hacked in 2015 by spies using malware and CryptoLocker ransomware to compromise Bureau of Meteorology and Reserve Bank of Australia data networks .

Attacks are now prevalent and incessant: cyber assaults spiked by 1,303% in ten years alone leading up to 2015, according to US Department of Homeland Security, and Control Risks' Riskmap Reports show one third of all cyberattacks are aimed at the public sector. Threats to human life due to cyberattacks have grown from 0 to 28% in the past ten years.

756,000 Californians' records stolen

by a single phishing email targeting 108 local county employees across 13 government agencies



Sectors targeted (% total attacks)

GOVERNMENT & FINANCE HIGH PROFILE TARGETS

Graph reproduced from Control Risk 2016 Riskmap Report

MailGuard reporting on recent phishing scams

MailGuard has reported that the most common email scams to hit Australian inboxes 'brandjack' (brand hijack) organisations with large customer bases. Government agencies such as ATO, ASIC and ACCC are regular victims of brand impersonation.

Seasonal scams include fraudulent ATO and ASIC end-of-financial-year phishing campaigns. Falsified Business Activity Statements, business name renewal and tax return documents lure recipients to click to execute a malware. During the Christmas season, pseudo-government agency Australia Post is regularly brandjacked in delivery notification phishing emails.

Evergreen attacks include traffic infringement and e-toll notices from state authorities such as VicRoads and the NSW Roads and Maritime Services. There are also frequent attempts to harvest personal credentials via myGov-branded fraudulent emails.

Government testimonal

"By implementing MailGuard email security, Moira Shire Council has dramatically reduced its exposure to email-related cybersecurity threats. MailGuard is a proven performer in blocking advanced email threats such as phishing, spear phishing and whaling, and their expertise in detecting threats specific to Australia also helps us with risk mitigation.

The service exceeds all our expectations, and the amazing Australian-based tech support was a key factor when weighing up vendors. I also appreciated the reporting provided at trial stage. The statistics provided clearly demonstrated our vulnerabilities, and helped us gain the C-level buy-in we needed."

—Network Administrator, Moira Shire Council

GET CYBERREADY WITH MAILGUARD

We identify and stop fast-breaking attacks in real-time, 2-48 hours ahead of the market
Contact your IT service provider now for an obligation-free, 14-day trial

PHONE 1300 30 44 30
EMAIL expert@mailguard.com.au
WEB mailguard.com.au

CYBER READY

mailguard