Dvuln

Fish in a barrel

Australia’s at-risk cleared personnel

March, 2024

@Dvuln

https://dvuln.com

“I appreciate people want to sell themselves to prospective employers, and may need to mention they have a security clearance, but doing it on a professional networking site is reckless.”

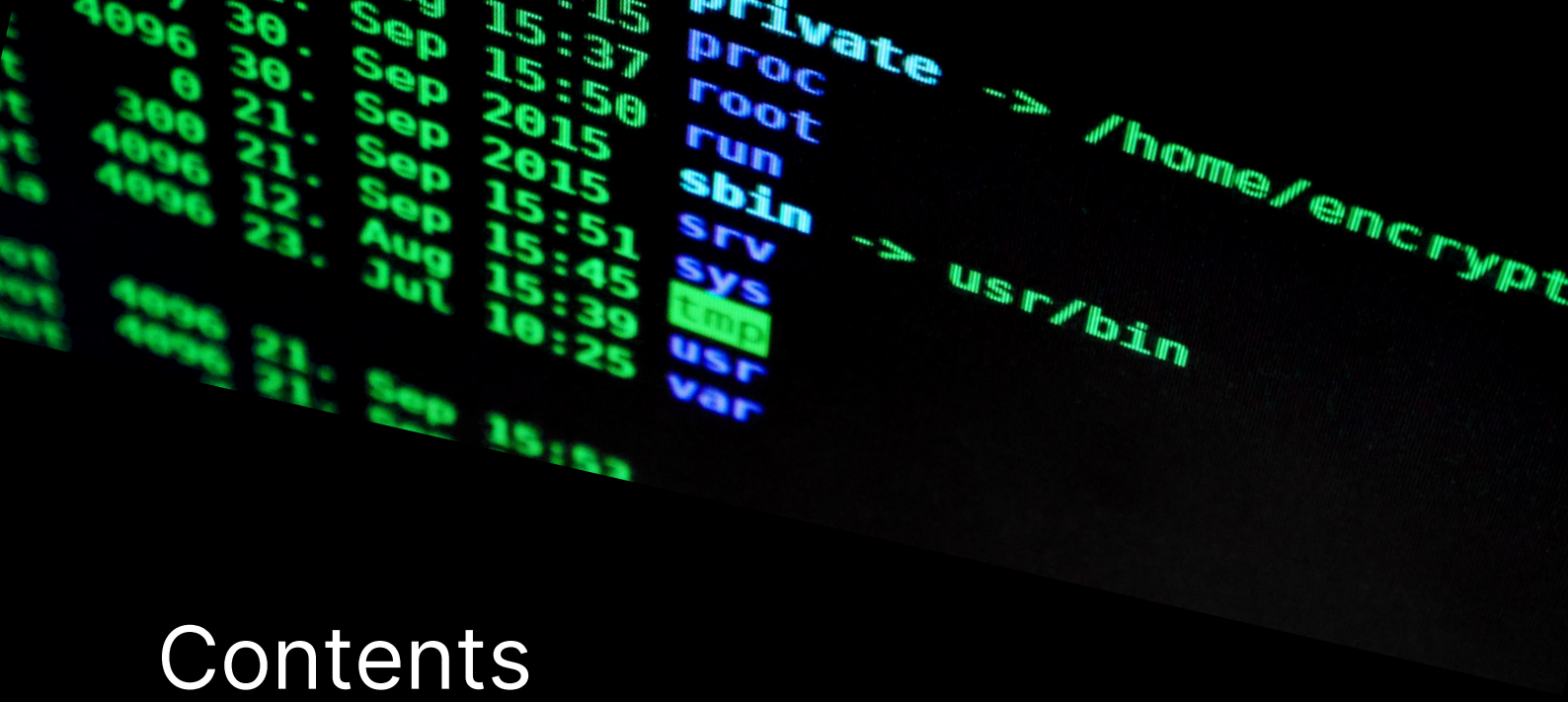
Mike Burgess

Director-General of Security of Australia

“The government spends hundreds of millions to protect their digital assets, but there’s no firewall that can fix a reckless person”

Jamieson O’Reilly

Director & Offensive Security lead of Dvuln



Contents

Background on Security Clearances in Australia

Security Clearance Levels

Under the Australian Government Protective Security Policy Framework, individuals who need access to security classified resources must hold a security clearance. This includes classified information, systems that hold classified information, and classified assets.

An individual may also be required to hold a security clearance if they occupy a position of trust that requires additional assurance.

There are 4 levels of security clearances:

- Baseline – permits ongoing access to classified resources up to and including Protected.
- Negative Vetting 1 – permits ongoing access to classified resources up to and including Secret, and temporary access to Top Secret classified resources in certain circumstances.
- Negative Vetting 2 – permits ongoing access to classified resources up to and including Top Secret.
- Positive Vetting – permits ongoing access to classified resources up to and including Top Secret, including some caveated resources.

The Purpose of Security Vetting

Security vetting aims to assess whether an individual is suitable to hold a security clearance, focusing on their integrity and character traits like honesty, trustworthiness, maturity, tolerance, resilience, and loyalty. This process ensures that the individual can protect Australian Government classified resources effectively.

In the security context, integrity is defined as a range of character traits that indicate the individual is able to protect Australian Government classified resources. These character traits are:

- honesty
- trustworthiness
- maturity
- tolerance
- resilience
  loyalty

The security vetting of an individual establishes confidence that they possess a sound and stable character, and they are not unduly vulnerable to influence or coercion.

Attack Paths

With the identification of clearance holders, the landscape of potential attack paths expands significantly. The proliferation of social media platforms and digital communication channels has opened up numerous avenues for attackers to exploit, making operational security more challenging than ever.

Shared Email
Sending the user e-mail based attacks.

LinkedIn
Fake job offers to NV1 users.

3rd Party Databases
Accessing NV1 users' breached data.

NV1 Cleared User
Security Project Manager
at Government Agency

Facebook
Gathering personal info of NV1 users.

Twitter/X
Analysing tweets of NV1 users for attack leverage.

WhatsApp
Direct messaging NV1 users for info phishing.

The LinkedIn Espionage Threat

Documented Risks

In a digital era where professional networking and social media intersect, the lines between connectivity and vulnerability blur.

The Australian Security Intelligence Organisation's (ASIO) recent focus on LinkedIn underscores this reality, where a tool for career advancement becomes a vector for foreign espionage.

ASIO's Warning on LinkedIn

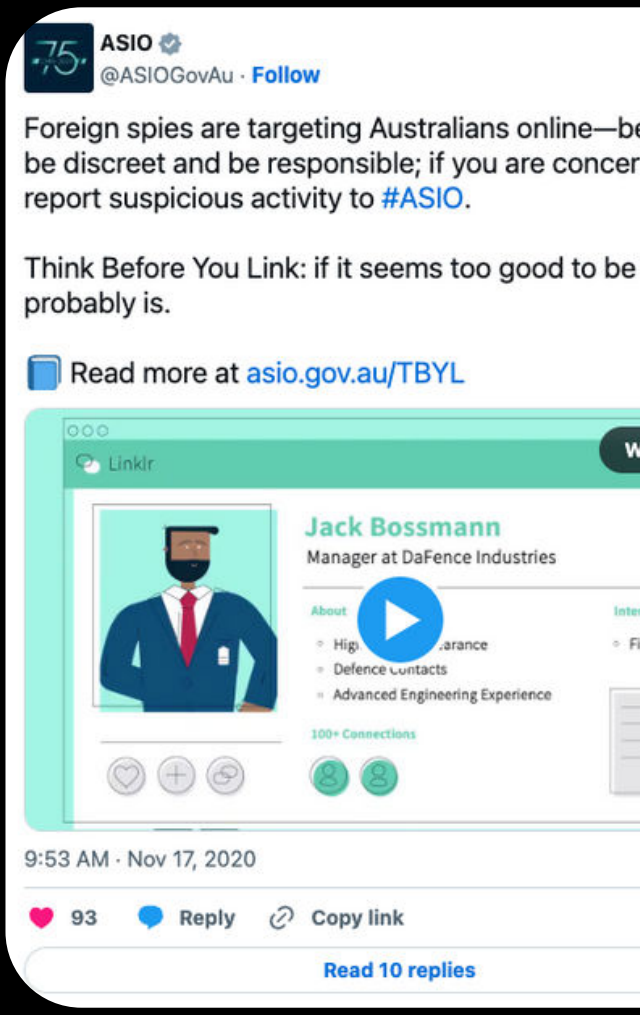
ASIO's advisory, as reported by Julian Bajkowski, paints LinkedIn not just as a professional networking site but as a fertile ground for hostile operatives.

Their warning extends beyond individual users to envelop entire sectors, particularly those involved in critical infrastructure and national security. ASIO's efforts in formulating and disseminating advice to stakeholders reflect the gravity of this concern.

The Impact of Open Source Intelligence

The leveraging of LinkedIn for intelligence gathering isn't a newfound tactic but the validation of an age-old strategy adapting to modern platforms.

LinkedIn's vast reservoir of professional data makes it an ideal source for open-source intelligence, a fact not lost on those with adversarial intent.



Navigating LinkedIn with Security Awareness

LinkedIn is Generally Good

LinkedIn, as a premier professional networking platform, offers immense opportunities for career growth and connections. However, it's crucial for users, especially those with security clearances, to navigate this space with awareness and discretion.

A Call for Strategic Professional Sharing

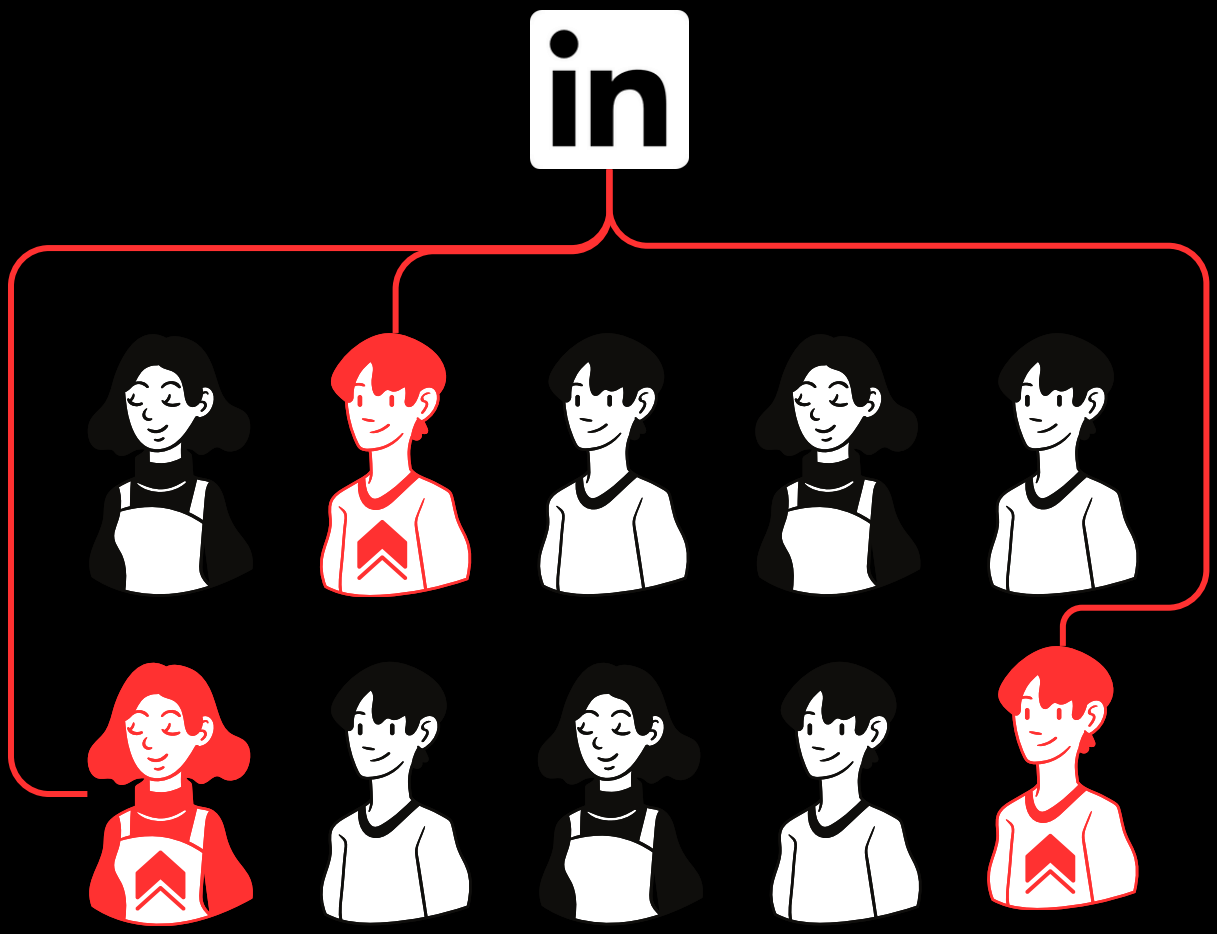
The message is not to retreat from LinkedIn but to use it strategically. This means highlighting professional skills and experiences without specifically mentioning clearance levels or sensitive project details.

LinkedIn's Structure and User Responsibility

While LinkedIn facilitates professional visibility and networking, it also requires users to be mindful of the information they share. This is particularly important for clearance holders, whose details about their job roles and clearances can attract unwanted attention.

Educating Users on Discretion

Educational initiatives and awareness campaigns can empower users to make informed decisions about their online presence. Clear guidelines and examples of best practices can help clearance holders understand the fine line between networking and oversharing.



Educating on the risks of Oversharing Security Clearances

The Case of Over-Disclosure

In a striking example, we observed an individual on LinkedIn not only sharing their current NV1 clearance status but also detailing their progression towards an NV2 clearance.

This level of disclosure is a textbook case of oversharing sensitive information in a public forum.

This information although seemingly trivial, provides powerful context for attackers who would use this as context in spear phishing campaigns.

For example, they may contact the user claiming to be someone involved in the NV2 vetting process.

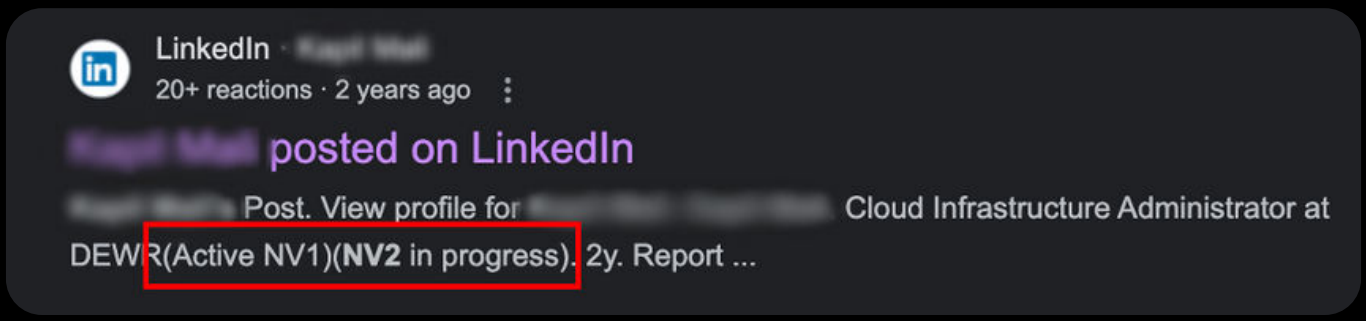
Understanding the Implications

Target for Espionage

By divulging such specific information, the individual becomes an immediate target for foreign intelligence agencies or cybercriminals. It signals access to highly sensitive information, making them a valuable asset for espionage efforts.

Risk to Personal and National Security

This kind of over-disclosure not only puts the individual at risk but also jeopardizes the security of the projects and organizations they are associated with.



Overview of Cleared LinkedIn Users Analysis and Data Breach Exposure

Overview of Analysis

Our study conducted a detailed examination of LinkedIn profiles, focusing on individuals with security clearances. We then cross-referenced these profiles with data from historic data breaches using the Have I Been Pwned tool, seeking to determine the extent of exposure these users have had in past data breaches.

Sample Size and Methodology

- We analysed a sample of 103 randomly selected LinkedIn users with security clearances.
- Percentage of Cleared Users Compromised in Data Breaches: Approximately 51.46% of the users with security clearance were compromised in data breaches.
- Most Impacted Sector with Cleared Users Compromised was the Telco industry.
- The job title 'Senior Project Manager' was the most compromised.
- One high-ranking NV2 user had their device compromised in 2022 by password stealer malware
- One NV1 users email was involved in 21 data breaches and found 4 pastes/online dumps

The Risks of Public Directories

The Risks of Public Directories

The InfoSec Registered Assessors Program (IRAP) plays a critical role in Australia. IRAP assessors are individuals certified to evaluate and endorse the security of systems for the Australian government, holding a position of significant trust and responsibility.

However, the public availability of assessor contact information can inadvertently create a comprehensive target list for cyber attackers, akin to "shooting fish in a barrel."

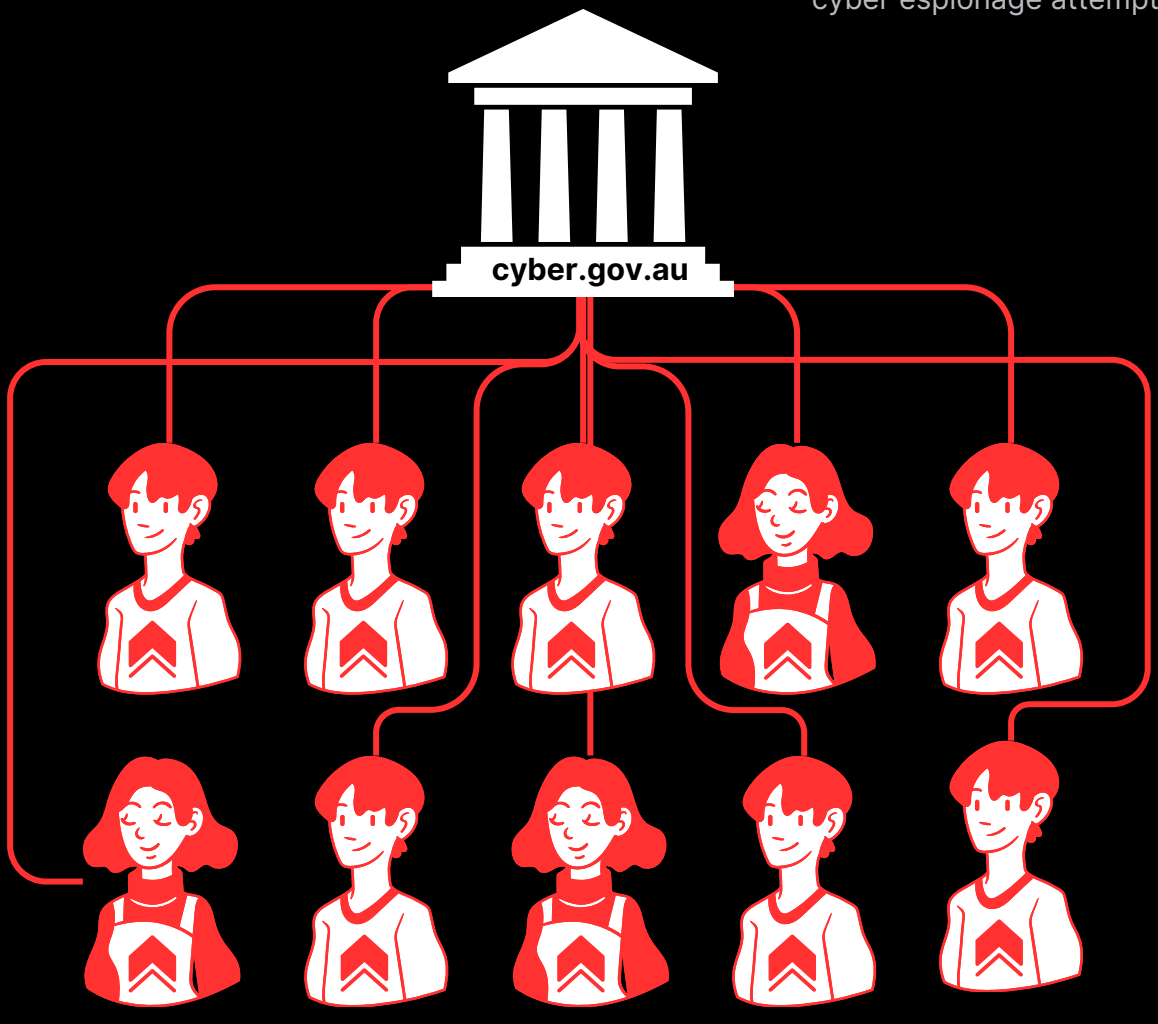
The Significance of IRAP

IRAP assessors are gatekeepers of national cyber defense, entrusted with the evaluation of sensitive government systems. Their work ensures that security measures in place can defend against threats and maintain the integrity of national infrastructures.

The Directory Dilemma

While a public directory of IRAP assessors may seem practical for networking and accessibility, it also simplifies the reconnaissance work for potential attackers.

With this information readily available, adversaries can pinpoint individuals with access to critical security information, turning them into targets for sophisticated social engineering and cyber espionage attempts.



Fish in a barrel - Australia’s at-risk cleared personnel

The Australian Signals Directorate‘s InfoSec Registered Assessors Program (IRAP)

A Closer Look at the Directory

The directory showcases IRAP assessors' names, contact details, and their availability. While designed for convenience and transparency, it also provides a ready-made list for those with malicious intent.

The Need for Controlled Access

It may be prudent to consider controlled access measures for such directories. Access could be limited to verified entities through secure authentication methods, reducing the risk of information falling into the wrong hands.

IRAP Assessors

Compromise and Exposure Analysis

This section of our report delves into the security of IRAP assessors' email addresses by cross-referencing them with known data breaches indexed by Have I Been Pwned. Our analysis reveals a concerning level of exposure that underscores the need for improved cybersecurity measures and personal vigilance.

- **Percentage of Compromised Email Addresses**: Approximately 30.74% of the email addresses in the dataset have been compromised in data breaches.

- **Proportion of Personal vs. Business Email Accounts**:
- Personal email accounts (like Gmail, Yahoo, Hotmail, Outlook): Approximately 29.05%.
- Business email accounts: Approximately 70.95%.

- **Trends in Companies with Most Compromised Users**: The top five domains with the most compromised users are:
- gmail.com: 35 instances
- hotmail.com: 10 instances
- defence.gov.au: 2 instances
- outlook.com: 2 instances
- yahoo.com: 2 instances

- **Overall Dataset Review**: In our thorough review of 296 IRAP assessors, 91 have been identified as compromised in at least one data breach from external sources.

- **Extent of Breaches**: The total count of individual compromises involving these users is 447, indicating that several assessors have been compromised multiple times or across different data sources.

The Compromise of ASD.ASSIST

Highlighting a Critical Breach

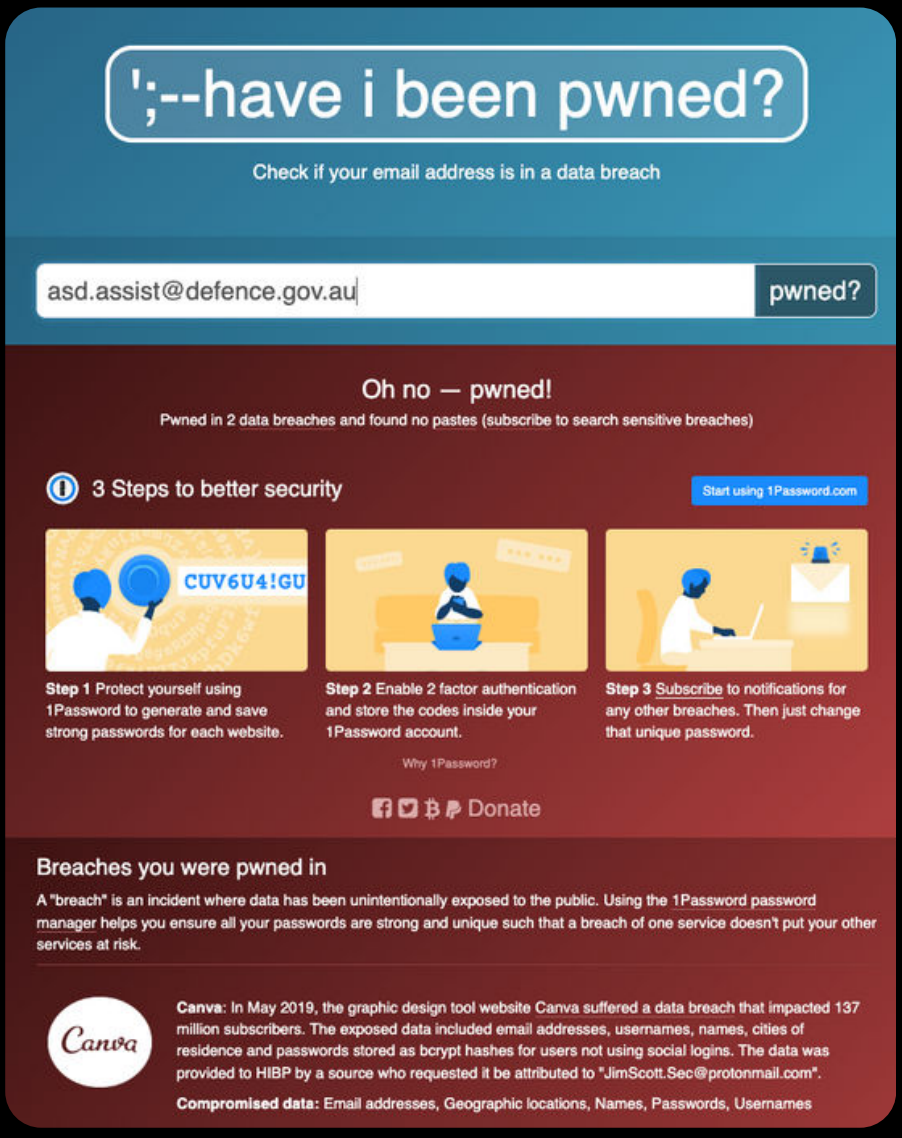
Our analysis has uncovered a concerning fact: the email address asd.assist@defence.gov.au, which serves as a critical contact point for IRAP assessors to communicate with the IRAP team, was used for registering with the third-party service Canva.

This discovery raises serious questions about the secure and appropriate use of sensitive government email addresses.

The Risks of Using SaaS Platforms

The use of a critical defense email address for a Software as a Service (SaaS) platform like Canva is highly irregular, especially given the sensitive nature of the ASD's operations.

This practice opens up avenues for potential security vulnerabilities, such as unauthorized access to sensitive communications and the risk of spear-phishing attacks targeted at high-profile users.



Recommendations for Clearance Holders

As individuals with access to sensitive information, clearance holders must navigate the digital world with heightened security awareness. To protect both personal and national security interests, the following practices are recommended.

Limit Public Disclosure

Avoid discussing security clearance levels and sensitive work details on public platforms. If disclosure is necessary, do so discreetly and only in direct communication with verified and trusted parties.

Profile Security

Conduct regular checks and updates of social media and professional networking site settings to ensure that only the intended audience can access your employment and personal information.

Awareness of Phishing Attempts

Remain alert to unsolicited contacts or job offers. These can be sophisticated attempts by adversaries to gain sensitive information.

Regular Training

Participate in continuous cybersecurity training to keep abreast of emerging threats and the latest safe practices online.

Secure Communication

Always use secure and encrypted channels when discussing sensitive work information to prevent eavesdropping and data breaches.

Personal and Professional Separation

Maintain a distinct separation between your personal and professional online personas to reduce the risk of exposing work-related information on personal platforms.

Recommendations for Organisations

Organisations play a crucial role in safeguarding their employees, especially those with security clearances. The following strategies can help in building a resilient security culture:

Employee Training and Awareness
Host regular training sessions to educate employees about the dangers of oversharing on social media and the importance of maintaining operational security.

Incident Response Plan
Develop a strong incident response framework to quickly and effectively address security breaches or suspicious activities related to employees' online social activities.

Policy Development
Create and enforce comprehensive policies that guide online behaviour, with a particular focus on employees who handle sensitive information.

Encourage Discretion
Cultivate an organizational culture that prioritizes security and discretion, underscoring the significance of careful online information sharing.

Monitoring and Support
Implement systems to monitor for and address potential online risks to employees. Provide robust support for those who may become targets due to their security clearances.

Secure Communication Tools
Equip employees with secure communication tools for work-related discussions, thereby minimising the reliance on potentially insecure platforms.

CREST

CRN FAST50 2023

@Dvuln

https://dvuln.com