Office of the Victorian Information Commissioner

Holmesglen TAFE

Sven Bluemmel – Victorian Information Commissioner

May 2021

Topics for today

Privacy and security obligations –

- *Victorian Protective Data Security Standards (**VPDSS**)*
- *Information Privacy Principles (**IPPs**)*

Where do we find ourselves?

- *Current threat environment - Remote / hybrid working arrangements*
- *Information security risks*
- *Data breaches / incidents (phishing / vishing)*

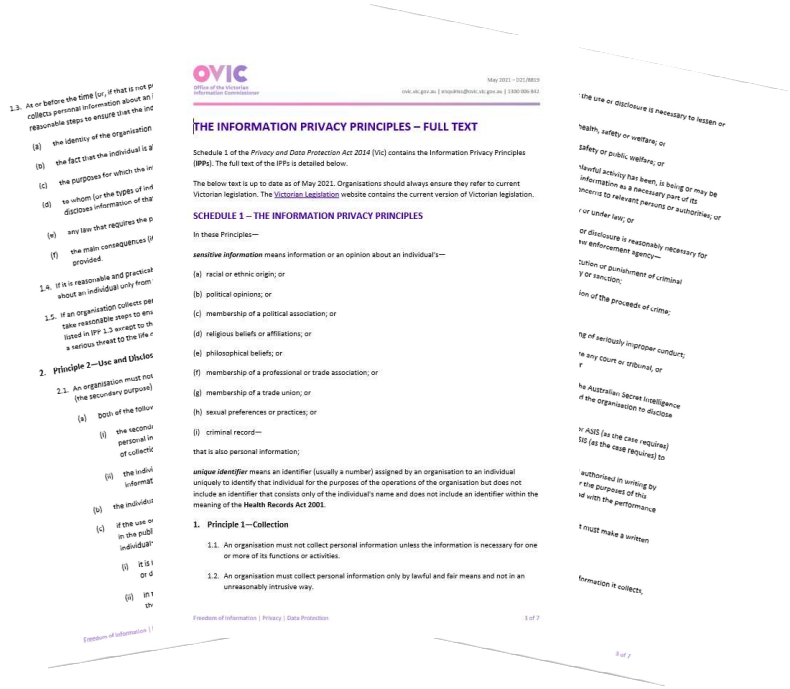
Phishing attacks

Tips when working remotely, and using collaboration and information sharing tools

Privacy and Security obligations

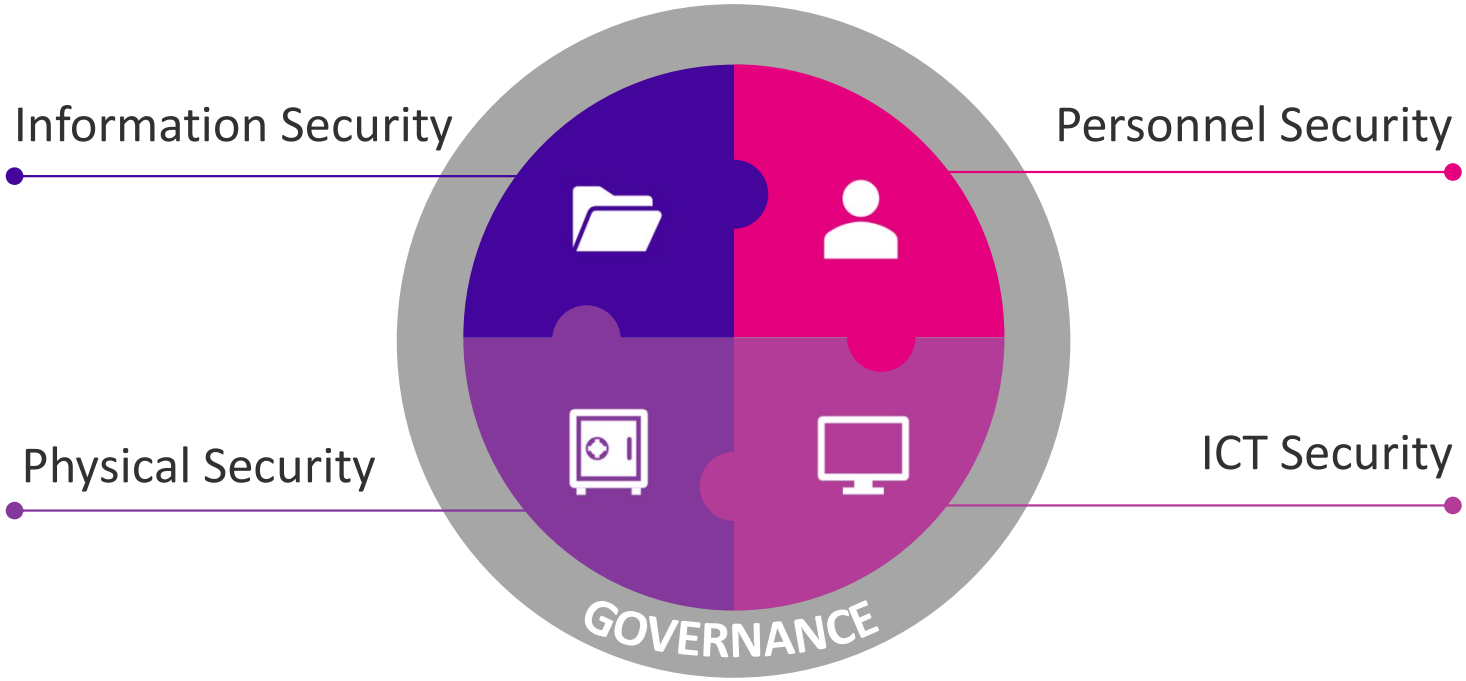
Victorian Protective Data Security Standards (VPDSS)

Information Privacy Principles (IPPs)



What do the VPDSS cover?

Victorian Public Sector organisations are required to adhere to **12 mandatory requirements** to protect public sector information. These protective measures draw on all security areas including:



What do the IPPs cover?

The IPPs are the core of privacy law in Victoria and set out the minimum standard for how Victorian public sector organisations should manage personal information.

- Principle 1 – Collection
- Principle 2 – Use and Disclosure
- Principle 3 – Data Quality
- Principle 4 – Data Security
- Principle 5 – Openness
- Principle 6 – Access and Correction
- Principle 7 – Unique Identifiers
- Principle 8 – Anonymity
- Principle 9 – Transborder Data Flows
- Principle 10 – Sensitive Information

Where do we find ourselves?

2020 signalled in a year of unprecedented challenges for both individuals and organisations and bore witness to significant changes in the information security threat landscape.

Organisations also submitted their second Protective Data Security Plans (PDSPs) to my office. These plans provided us with a unique insight into the state of information security across the public sector.

Many organisations shifted to remote / hybrid working arrangements

Regardless of where you are working, you need to remain mindful of how you are handling public sector information.

Information security risks

Significant increase in **Ransomware**, **email phishing** and malware-laden **SMS scams** including:

ACSC
Australian
Cyber Security
Centre

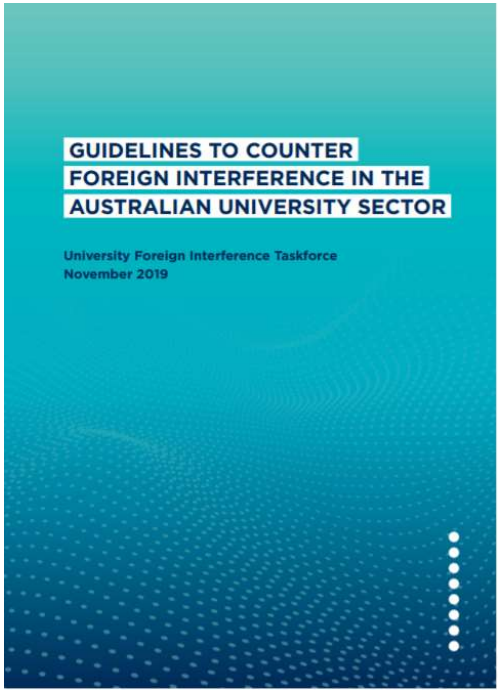
- targeting **vulnerabilities** in **remote work environments**
- attempts to **scam the public** by taking advantage of the public appetite for information and services, particularly those related to **COVID-19**
- professional syndicates operating **ransomware crime**
- **DDOS attacks**
- **Business email compromise** has significantly increased over the past year, and is expected to be a **continuing trend for 2021**
- Targeting of **service providers** and supply chain providers

Foreign Interference in the Higher Education Sector

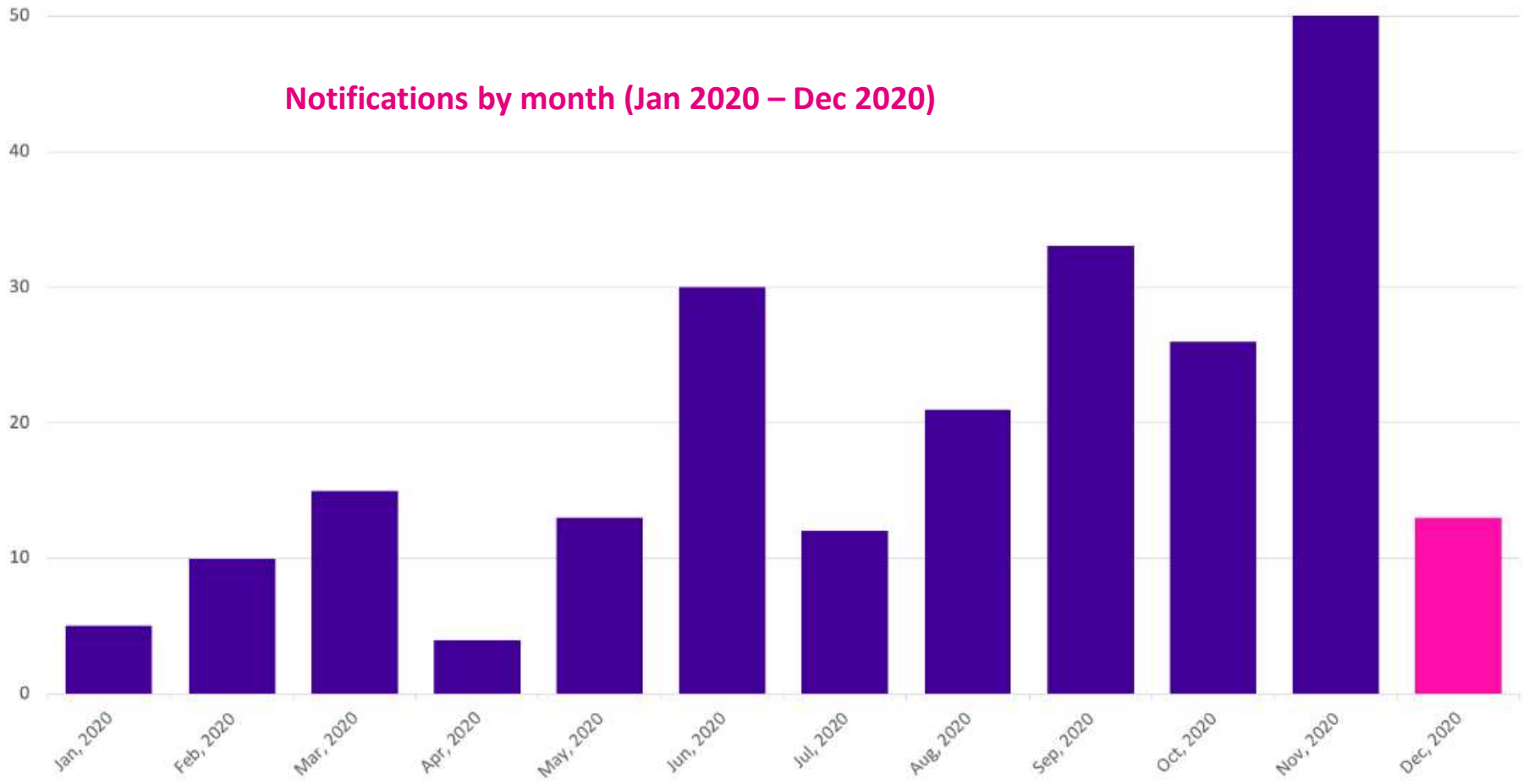
In October 2019, Australia's Director-General of Security, Mr Mike Burgess, noted the **unprecedented scale of foreign interference activity** against Australia's interests, with 26% **of attacks in 2017 attributed to the education sector.**

Higher education providers play a key role in the development of new knowledge and technological innovation. This is vital to continued productivity and economic growth.

The guidelines are intended to further **empower institutions** in a way that is both durable and responsive to **emerging threats and pressures** as these develop and change over time.

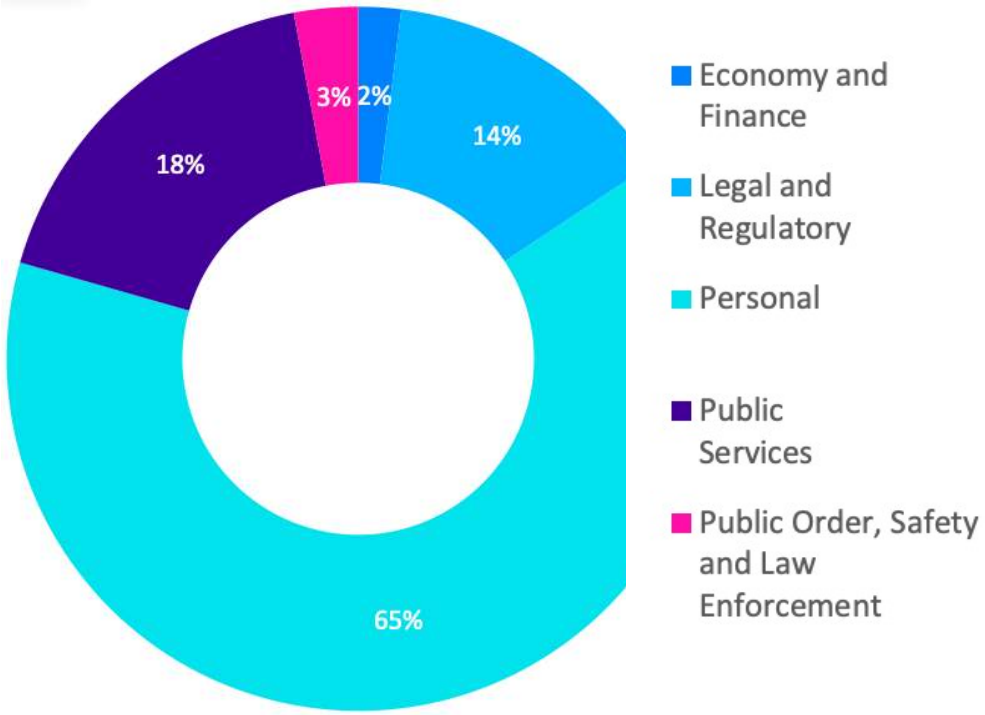


Incident Insights

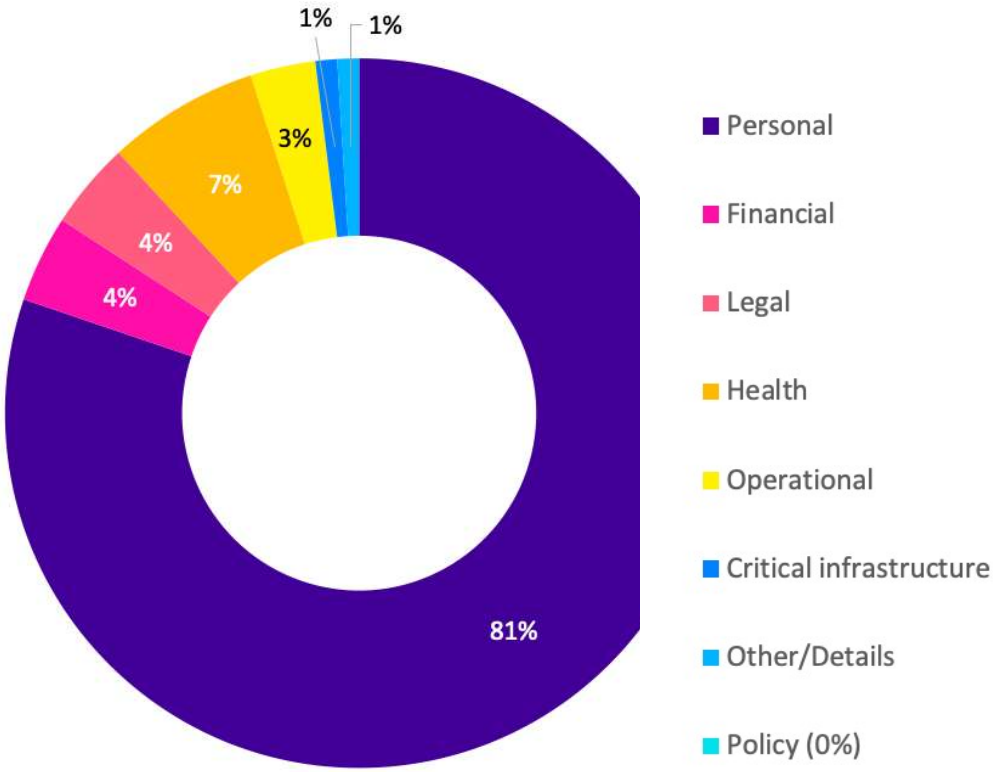


Key takeouts

Potential business impact category affected

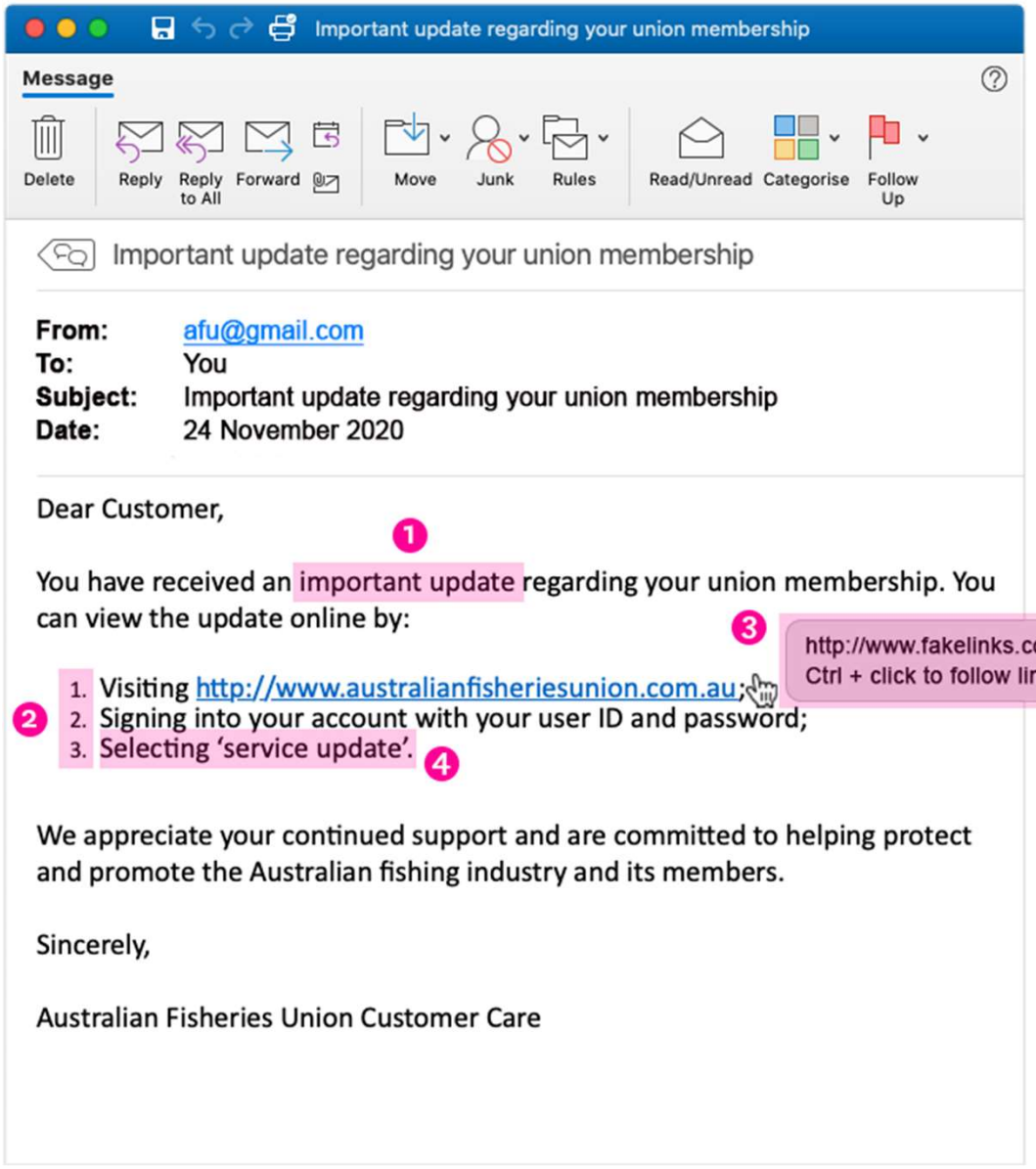


Type of information impacted



Phishing attacks

1. It is unexpected or creates a sense of urgency for you to do something
2. It asks you to click a link, open an attachment or sends you to a website which asks you to enter your information
3. The link suggests that it will take you to a legitimate website but, when you hover over the link, it shows that it is actually for a different website
4. It asks for information that the real or legitimate sender would not necessarily need to know



Working remotely, and using collaboration and information sharing tools

- Refer to your organisation's policies and procedures
- Avoid working in public places and set up a private workspace where possible
- Be conscious of what you say to members of your family, friends or household
- Use a secured wifi network or ethernet
- Only use workplace approved devices and accounts for work-related purposes
- Only use workplace approved third party collaboration and communication platforms for work-related communication
- Avoid inserting peripheral devices into your workplace device that require drivers to be installed
- Secure devices and documents when you leave them unattended
- Notify your organisation of any incidents
- Be especially wary of phishing scams
- Be careful of what you post to social media

Questions

For those with questions please email ***enquiries@ovic.vic.gov.au***

Resources

Privacy - https://ovic.vic.gov.au/privacy/privacy-resources-for-organisations/

Security - https://ovic.vic.gov.au/data-protection/for-agencies/vpdsf-resources/

OVIC
Office of the Victorian Information Commissioner