INFS 5115 Security Principles

Social Engineering

University of South Australia

School of
Information Technology
and Mathematical Sciences

Social Engineering

- In this seminar we will discuss the various types of social engineering attacks and contemporary trends in this domain.
- We will also briefly discuss mitigation strategies against these types of attacks.

Definitions

- *An attempt to trick someone into revealing information (e.g., a password) that can be used to attack systems or networks.*[1]
- *A general term for attackers trying to trick people into revealing sensitive information or performing certain actions, such as downloading and executing files that appear to be benign but are actually malicious.*[2]

[1] SP 800-61 and [2] SP 800-114 cited in Kissel, R., 2013. Glossary of Key Information Security Terms. NIST Interagency Reports, NISTIR 7298.

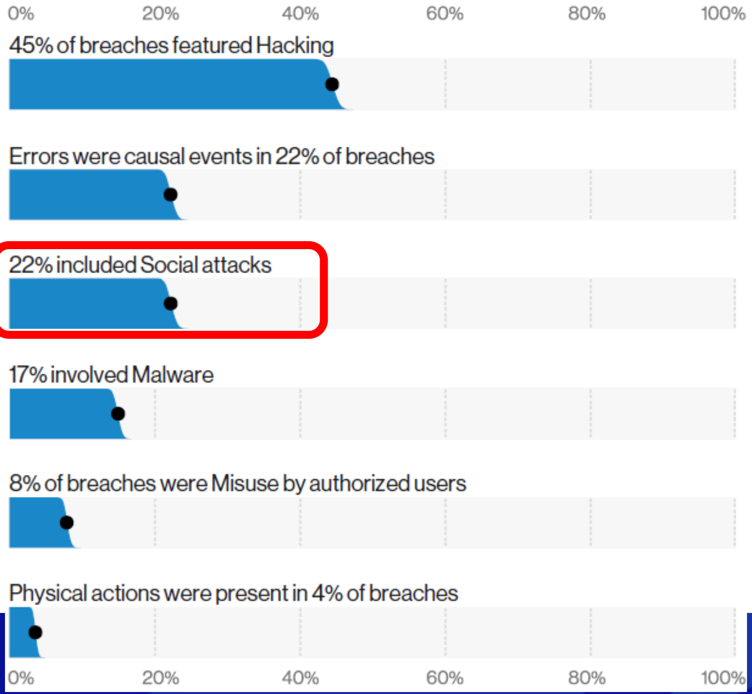
Social engineering attacks

- Employs psychological manipulation and deceit to establish trust and elicit information. In cyberspace it is commonly observed in spear phishing, and increasingly in exploitation attempts through social media.[1]
- Used proficiently, social engineering can enable adversaries to bypass security measures they were unable to overcome via technical means.[1]

[1] Australian Cyber Security Centre 2016, ACSC Threat Report, Commonwealth of Australia. p. 20.

Verizon’s Data Breach Investigations Report

Figure 2. What tactics are utilized? (Actions)



Verizon 2020, *2020 Data Breach Investigations Report*, Verizon, p. 7, https://enterprise.verizon.com/en-au/resources/reports/dbir/

Activity 1

Open the "Social Engineering Activity" under Week 7 of Security Principles.

Ontological Model of Attacks

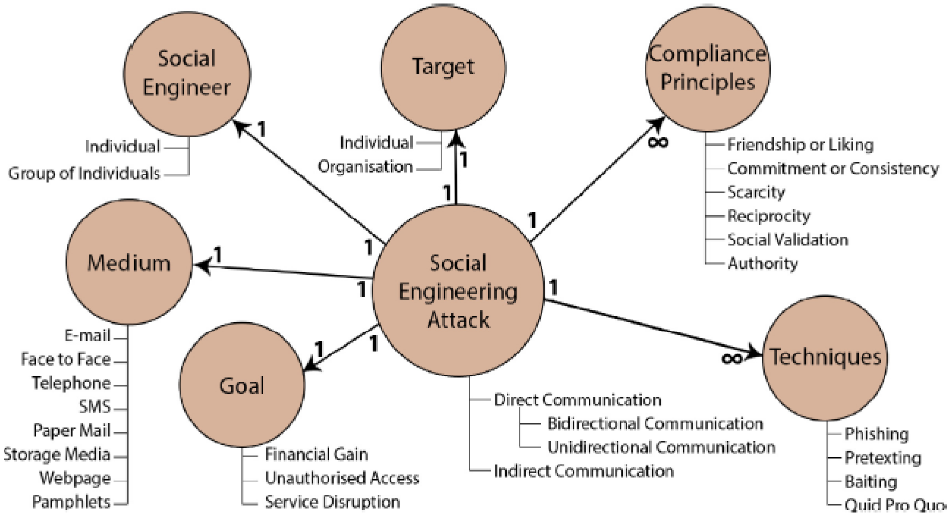


Fig. 1 – An ontological model of a social engineering attack.

Source: Mouton, F, Leenen, L and Venter, H S 2016, 'Social engineering attack examples, templates and scenarios', Computers & Security, vol. 59, pp.186-209.

Ontological Model of Attacks

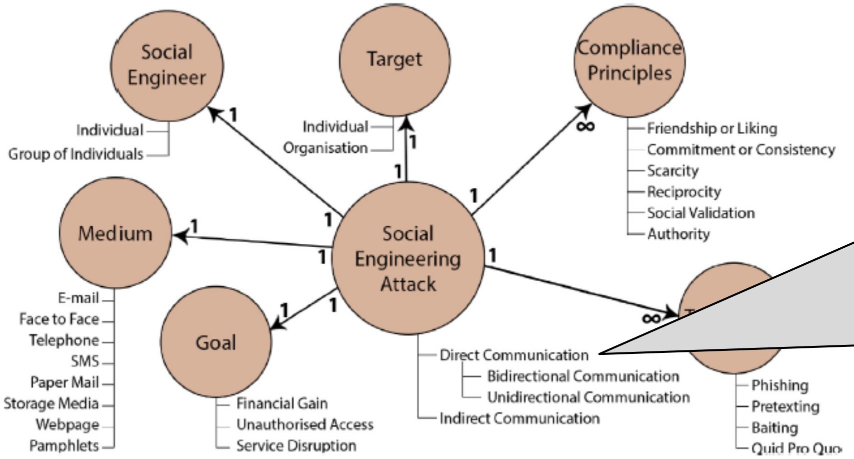


Fig. 1 – An ontological model of a social engineering attack.

Communication Types

Direct Communication

Bi-directional (e.g., email which requests a reply) or unidirectional (e.g., SMS without a reply number)

Indirect Communication

No interaction between the two parties – e.g., baiting

Mouton, F, Leenen, L and Venter, H S 2016, ‘Social engineering attack examples, templates and scenarios’, Computers & Security, vol. 59, pp.186-209.

Ontological Model of Attacks

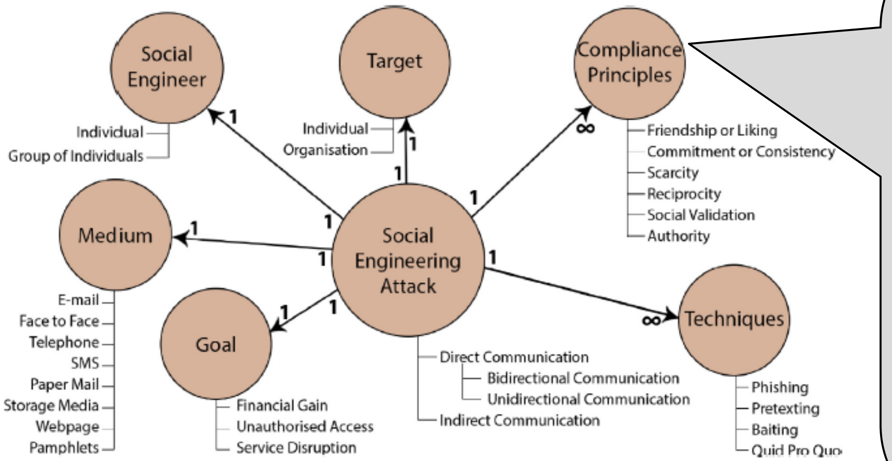


Fig. 1 – An ontological model of a social engineering attack.

Compliance Principles
The reasons why the target complies with the malicious request:

- **Friendship or liking**
  People are more likely to comply if they are communicating with a friend.
- **Commitment or consistency**
  People are more likely to comply with requests that are consistent with their commitments.
- **Scarcity**
  People are more likely to comply when there is scarcity associated with a request.

Mouton, F, Leenen, L and Venter, H S 2016, ‘Social engineering attack examples, templates and scenarios’, Computers & Security, vol. 59, pp.186-209.

Social Engineering

Ontological Model of Attacks

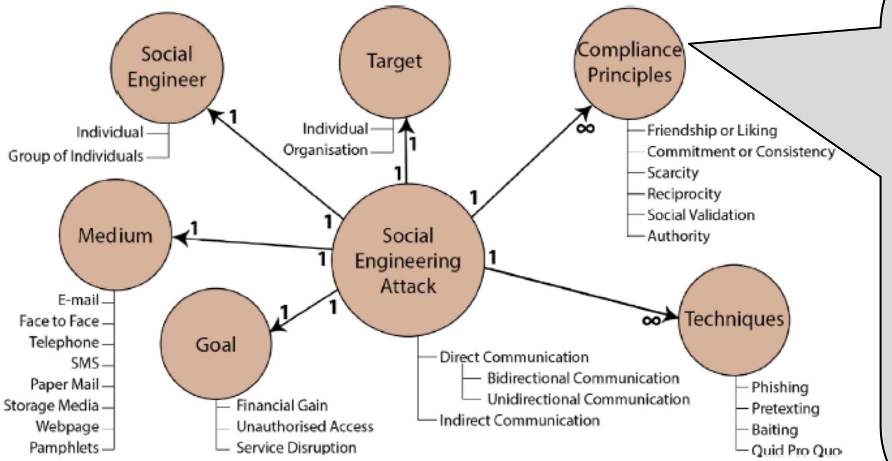


Fig. 1 – An ontological model of a social engineering attack.

Compliance Principles

- **Reciprocity**

  People are more likely to comply when reciprocating a past action or favour.

- **Social Validation**

  People are more likely to comply when they believe that it is a social norm for them to do so.

- **Authority**

  People are more likely to comply when communicating with people in positions of authority.

Mouton, F, Leenen, L and Venter, H S 2016, ‘Social engineering attack examples, templates and scenarios’, Computers & Security, vol. 59, pp.186-209.

Ontological Model of Attacks

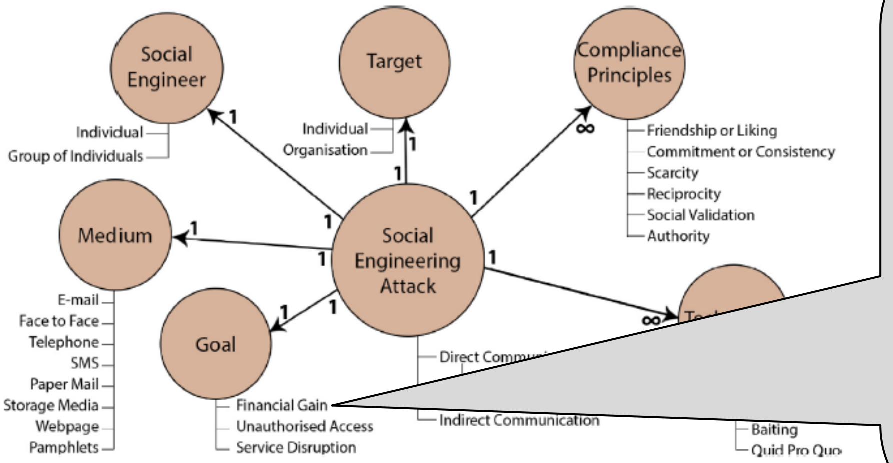


Fig. 1 – An ontological model of a social engineering attack.

Goal

- **Financial Gain**

  Actors gain access to financial information or redirect payments to their own accounts
- **Unauthorised Access**

  Requests user credentials to gain access to systems such as company servers or online banking.
- **Service Disruption**

  Often using Ransomware to produce a loss of business, customers, data, and productivity.

Mouton, F, Leenen, L and Venter, H S 2016, ‘Social engineering attack examples, templates and scenarios’, Computers & Security, vol. 59, pp.186-209.

Ontological Model of Attacks

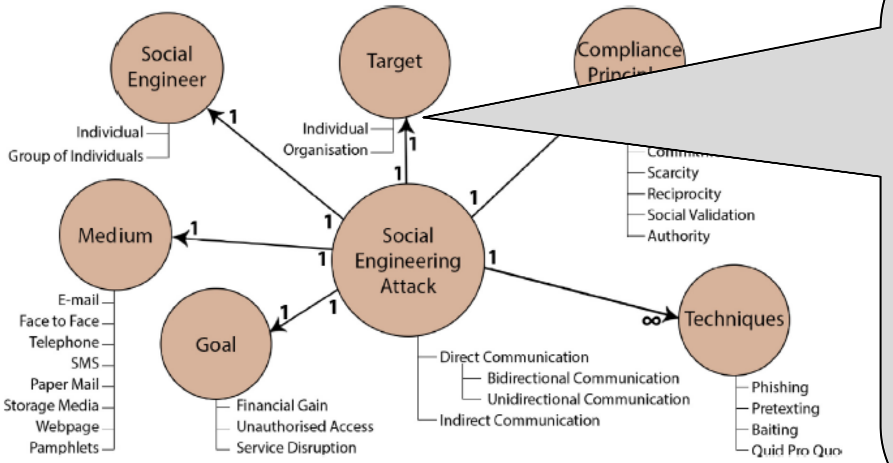


Fig. 1 – An ontological model of a social engineering attack.

Targets

- **End Users**

  Normal everyday web users are often targeted in random opportunistic attacks

- **Executives in a Business**

  Executives are targets to gain access to their business emails, calendar, accounts etc..

- **Organisations**

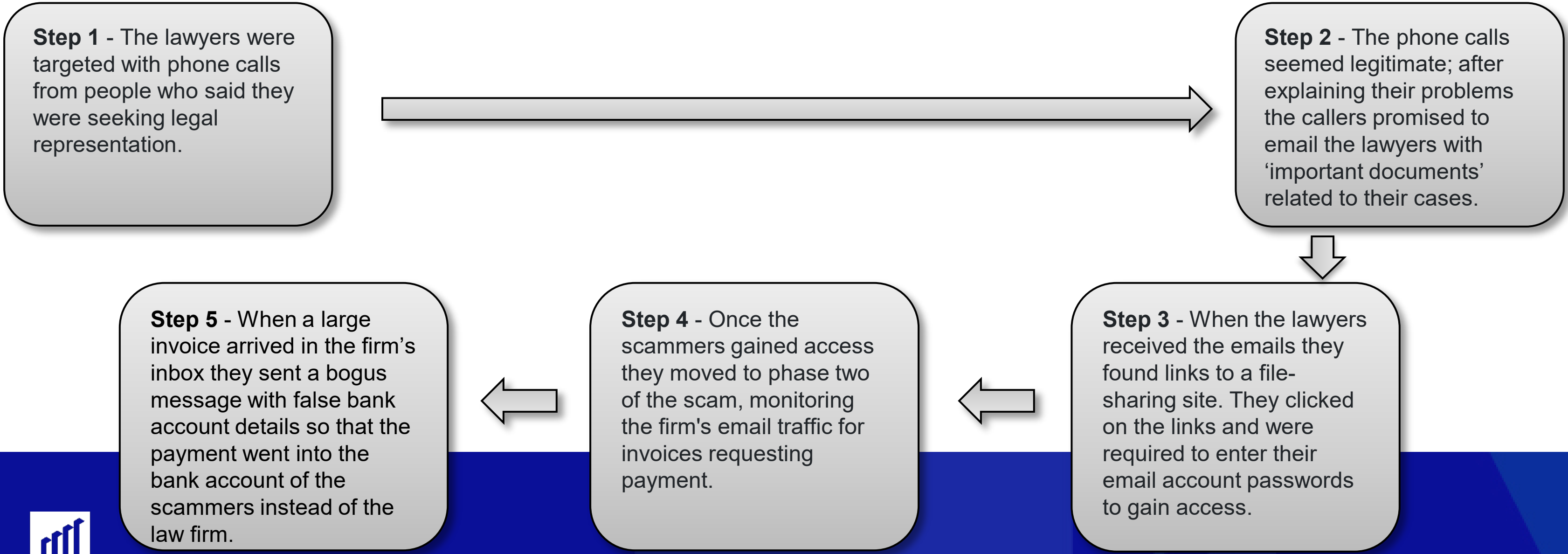
  Usually targeted to get user information and emails to further target individual accounts with spear phishing techniques.

Mouton, F, Leenen, L and Venter, H S 2016, ‘Social engineering attack examples, templates and scenarios’, Computers & Security, vol. 59, pp.186-209.

Social Engineering Example

Sophisticated social engineering attacks often involve simultaneous use of different communication channels, including phone. For example:

Cybercriminals stole millions of dollars from Queensland law firms. The cybercriminals didn’t hack into the lawyer's network or infect their computers with a virus - they just sent them an email.



Step 1 - The lawyers were targeted with phone calls from people who said they were seeking legal representation.

Step 2 - The phone calls seemed legitimate; after explaining their problems the callers promised to email the lawyers with ‘important documents’ related to their cases.

Step 3 - When the lawyers received the emails they found links to a file-sharing site. They clicked on the links and were required to enter their email account passwords to gain access.

Step 4 - Once the scammers gained access they moved to phase two of the scam, monitoring the firm's email traffic for invoices requesting payment.

Step 5 - When a large invoice arrived in the firm’s inbox they sent a bogus message with false bank account details so that the payment went into the bank account of the scammers instead of the law firm.

https://securitybrief.com.au/story/case-study-how-cybercriminals-targeted-qld-law-firm-social-engineering

Group Activity

Ontological Model of Attacks

Which tactics were used by the attackers?

Target?

Communication Method, Direct or Indirect?

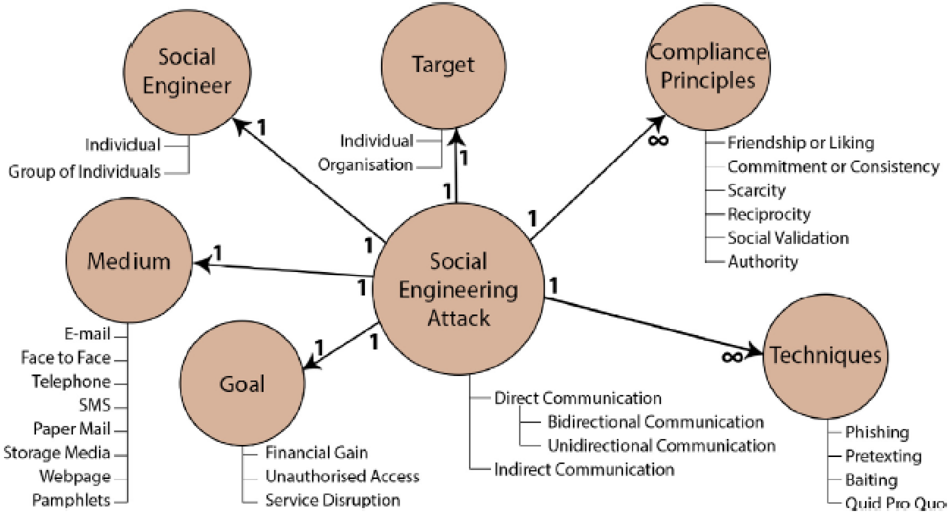
Compliance Principle?

Technique?

Medium?

Goal?

What mitigation techniques could be used for this kind of attack?



Source: Mouton, F, Leenen, L and Venter, H S 2016, ‘Social engineering attack examples, templates and scenarios’, Computers & Security, vol. 59, pp.186-209.

Mitigation Strategies

- **Build a positive security culture**
  - Staff are aware of their security responsibilities and report potential phishing attacks as soon as possible
  - Not think they shouldn't say anything because they might get in trouble
- **Learn the psychological triggers**
  - Attackers exploit several psychological triggers to get past people's natural defenses
  - Create situations of false urgency and heightened emotion
  - Rely on people's conditioned responses to authority
- **Train your staff**
  - Understand the consequences of social engineering attacks
  - Don't open suspicious email attachments
  - Think before providing sensitive information
- **Test the effectiveness of the training**
  - Simulated phishing attacks will give you a good idea of your employees' susceptibility to phishing emails
- **Implement appropriate technical measures**
  - Using firewalls, antivirus, anti-malware, whitelisting and spam filters to keep malicious traffic to a minimum
  - Applying patches and keeping your systems up to date
  - Implementing a policy of using strong, unique passwords

Source: https://www.grcelearning.com/blog/5-ways-to-mitigate-social-engineering-attacks

Mitigations

- As cyber adversaries refine their social engineering tradecraft, legitimate communications are sometimes becoming almost indistinguishable from social engineering attempts.
- Robust technical controls are becoming increasingly important to protect networks from this kind of malicious cyber activity.
- The data shows simulated phishing makes a difference, **but someone will always click**. See this example!
- Focus on detection and reporting of clicks rather than just prevention.

Source: Verizon's 2017 Data Breach Investigations Report, p. 34, http://www.verizonenterprise.com/verizon-insights-lab/dbir/2017/

https://cyberforces.com/en/the-pizza-method-a-social-engineering-case-study

Mitigation referencing the Mitre ATT&CK framework

- ❑ Initial access (TA0001) - The adversary is trying to get into your network.
  - Phishing (T1566)

- ❑ Execution (TA0002) - The adversary is trying to run malicious code.
  - User Execution (T1204)

- ❑ Lateral movement (TA0008) - The adversary is trying to move through your environment.
  - Internal spearphising (T1534)

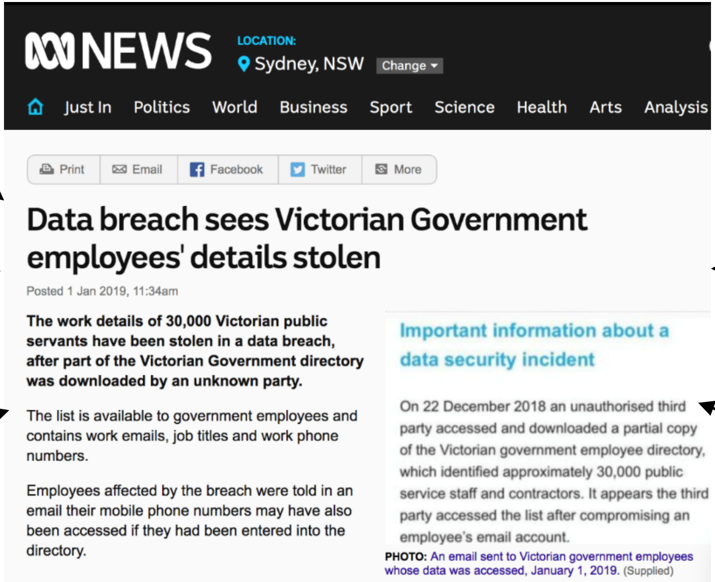
Social Engineering Example

Spearphishing

Data leaked in previous breaches is often used in spear phishing attacks.

Customisations are often made based on information relevant to the target or the purported sender.

Information is often sourced from public information published by the individual or organisation.



Data breach sees Victorian Government employees' details stolen

Posted 1 Jan 2019, 11:34am

The work details of 30,000 Victorian public servants have been stolen in a data breach, after part of the Victorian Government directory was downloaded by an unknown party.

The list is available to government employees and contains work emails, job titles and work phone numbers.

Employees affected by the breach were told in an email their mobile phone numbers may have also been accessed if they had been entered into the directory.

Important information about a data security incident

On 22 December 2018 an unauthorised third party accessed and downloaded a partial copy of the Victorian government employee directory, which identified approximately 30,000 public service staff and contractors. It appears the third party accessed the list after compromising an employee's email account.

PHOTO: An email sent to Victorian government employees whose data was accessed, January 1, 2019. (Supplied)

Describes phishing designed to target specific individuals

Increasingly sophisticated spearphishing attacks mean that user education becomes less useful as a mitigation technique.

The use of technical mitigations must be increased to combat this threat.

University of South Australia

School of Information Technology and Mathematical Sciences

https://www.abc.net.au/news/2019-01-01/victorian-government-employee-directory-data-breach/10676932

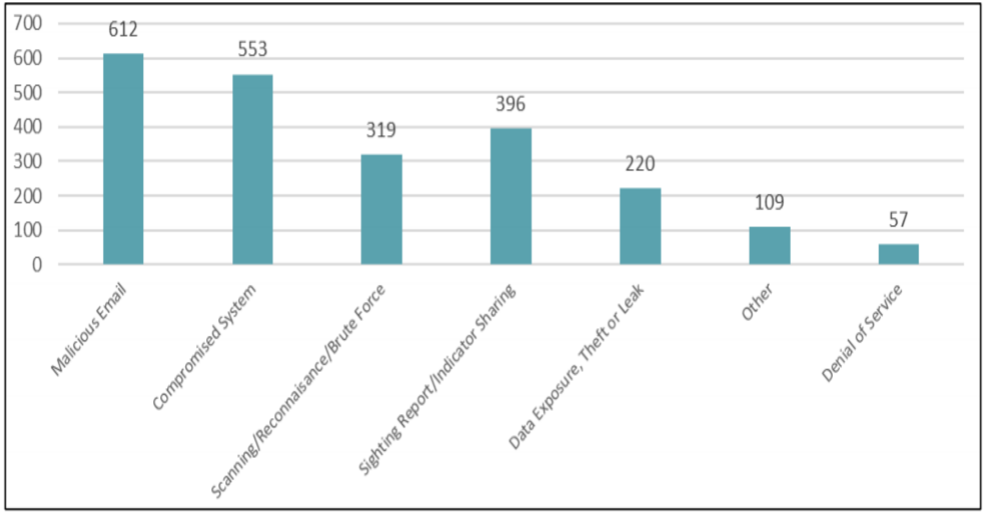
Social Engineering Impact

- The use of social engineering is particularly prominent in business email compromise (BEC), a scheme which targets businesses for financial gain.

- BEC scams involve a range of email, instant message, SMS and social media tactics used by cybercriminals to fraudulently access money or goods.

- In 2019-20 financial year there were 4,255 reports of BEC scams reported through the ACSC's ReportCyber tool, representing losses of over $142 million

Figure 4: Cyber security incidents, by type (1 July 2019 to 30 June 2020)



Australian Cyber Security Centre July 2019 – June 2020, ACSC Threat Report, Commonwealth of Australia, p.8.

Social Engineering Impact

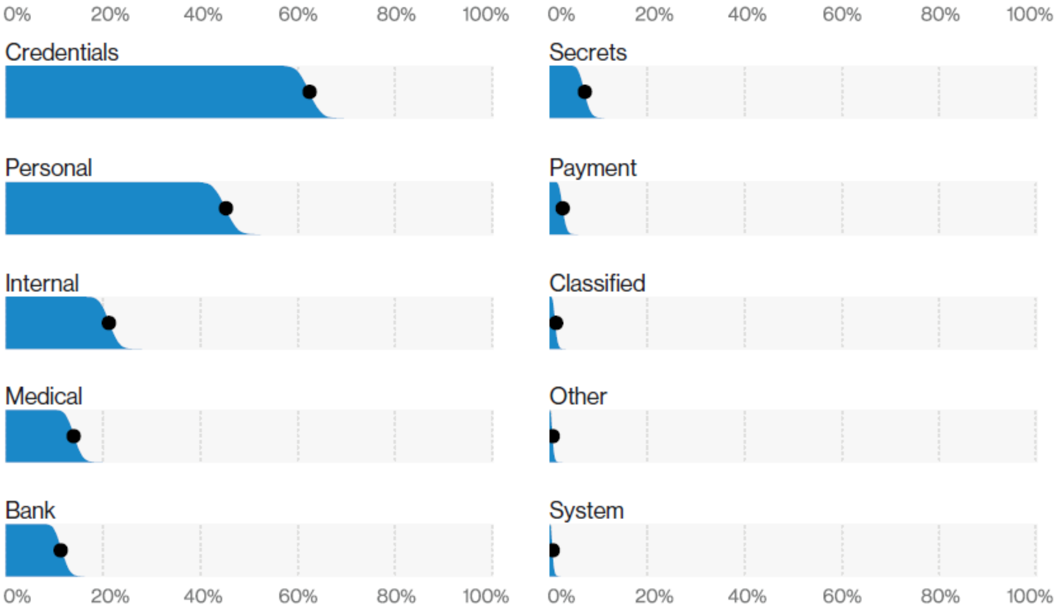


Figure 29. Top data varieties compromised in Phishing breaches (n = 619)

Most Likely Targets

- Senior executives and their executive assistants
- Help desk staff, system and network administrators, and other users who have administrative privileges to operating systems or applications such as databases
- All users who have access to sensitive data, including data that could provide a foreign government or organisation with a strategic or economic advantage
- Users with remote access

Australian Cyber Security Centre 2019/20, ACSC Threat Report, Commonwealth of Australia.

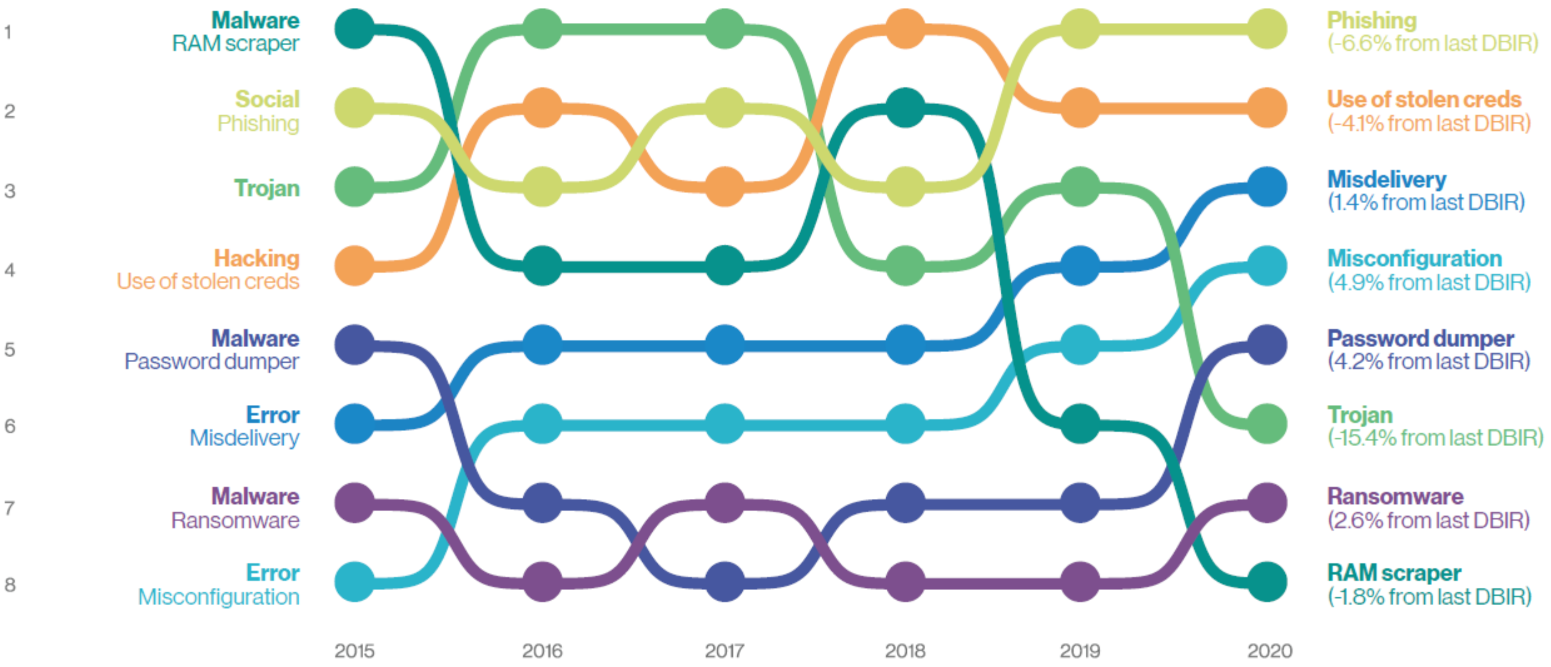
Current trends

- Ransomware and external adversaries with destructive intent
- Malicious insiders
- Business email compromise
- Industrial control systems
- Control of application and network activities

Australian Cyber Security Centre 2019/20, ACSC Threat Report, Commonwealth of Australia.

Trends

Figure 6. Select action varieties in breaches over time



Verizon 2020, *2020 Data Breach Investigations Report*, Verizon, p. 7, https://enterprise.verizon.com/en-au/resources/reports/dbir/