

A man wearing a dark hoodie is sitting at a desk, looking intently at a laptop screen. His hand is resting on his chin in a thoughtful pose. The background is a blurred blue screen displaying lines of CSS code. A semi-transparent grid of squares is overlaid on the right side of the image.

# Cyber Security & You

By Daniel Lillicrap



# DISCLAIMER

- Cyber security is a complex issue.
- The descriptions, analogies, links and advice contained within this presentation may not be suitable for all persons, circumstances and or purposes. The advice contained within this presentation should be considered of a general nature and should not be relied upon in any professional or financial capacity.
- No guarantees or warranties are made with regards to any material or information sourced within this presentation.
- Please contact your IT professional for further advice.
- Warning: this presentation may induce panic and or anxiety.

© Digital GP 2024

All Rights Reserved





# Why is cyber security important?

- There are a reported 31,000 new phishing threats generated every day .
- Phishing attacks increased by 1,265% in 2023 .
- \$17,700 is lost every minute due to a phishing attack .
- Nearly half (47.4 percent) of all internet traffic came from bots in 2022, which is a 5.1% increase over 2021 .
- By 2025, humanity's collective data will reach 175 zettabytes - the number 175 followed by 21 zeros .
- 74 percent of cybersecurity breaches are caused by human error .

# What is so important about my data?

- What is Data?
- What is Metadata?
- Who cares if someone has data about me?





# Introduction to metadata.

Meet Will Ockenden

With access just to Will's metadata people could tell the following:

- Where Will worked.
- When Will worked.
- Where Will lived.
- How Will travelled to and from work.
- Where Will went on holidays.
- Where Will's parents lived.
- When Will went to visit them.



# How do they get my information?

---

- It's not you, it's them.
  - Companies like Optus, Medibank etc
- You give your info away, for FREE!
  - Social media
- Even if you're not giving it away, you're inviting people to take it.
  - Easy, repeated passwords that remain unchanged;
  - No 2FA (Two Factor Authentication);
  - Inadequate anti-virus;
  - Poor or inadequate backups;

## How people think they get hacked



## How they really get hacked



# How else might they get my information?

---

- The most common attacks fall under the following categories:
  - DDos
  - Phishing
  - Brute force
  - Social engineering
  - MiTM (Man In The Middle)
  - Physical penetration
  - Spoofing
  - Scraping
  - Ransomware
  - Malware
  - Insider threats
  - DNS tunnelling
  - IoT-Based attacks



## Email Phishing in 2022

22 percent of data breaches are a result of phishing.<sup>[1]</sup>



3.4 billion scam or phishing emails are sent each day.<sup>[3]</sup>



Microsoft is the most impersonated brand in phishing attacks.<sup>[4]</sup>



Phishing is the most common type of cybercrime.<sup>[2]</sup>



2021 was the most expensive year for data breaches in 17 years.<sup>[3]</sup>

### RANSOMWARE



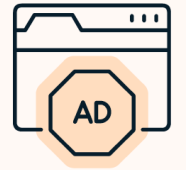
Blackmails you

### SPYWARE



Steals your data

### ADWARE



Spams you with ads

## Types of Malware

### WORMS



Spread across computers

### TROJANS



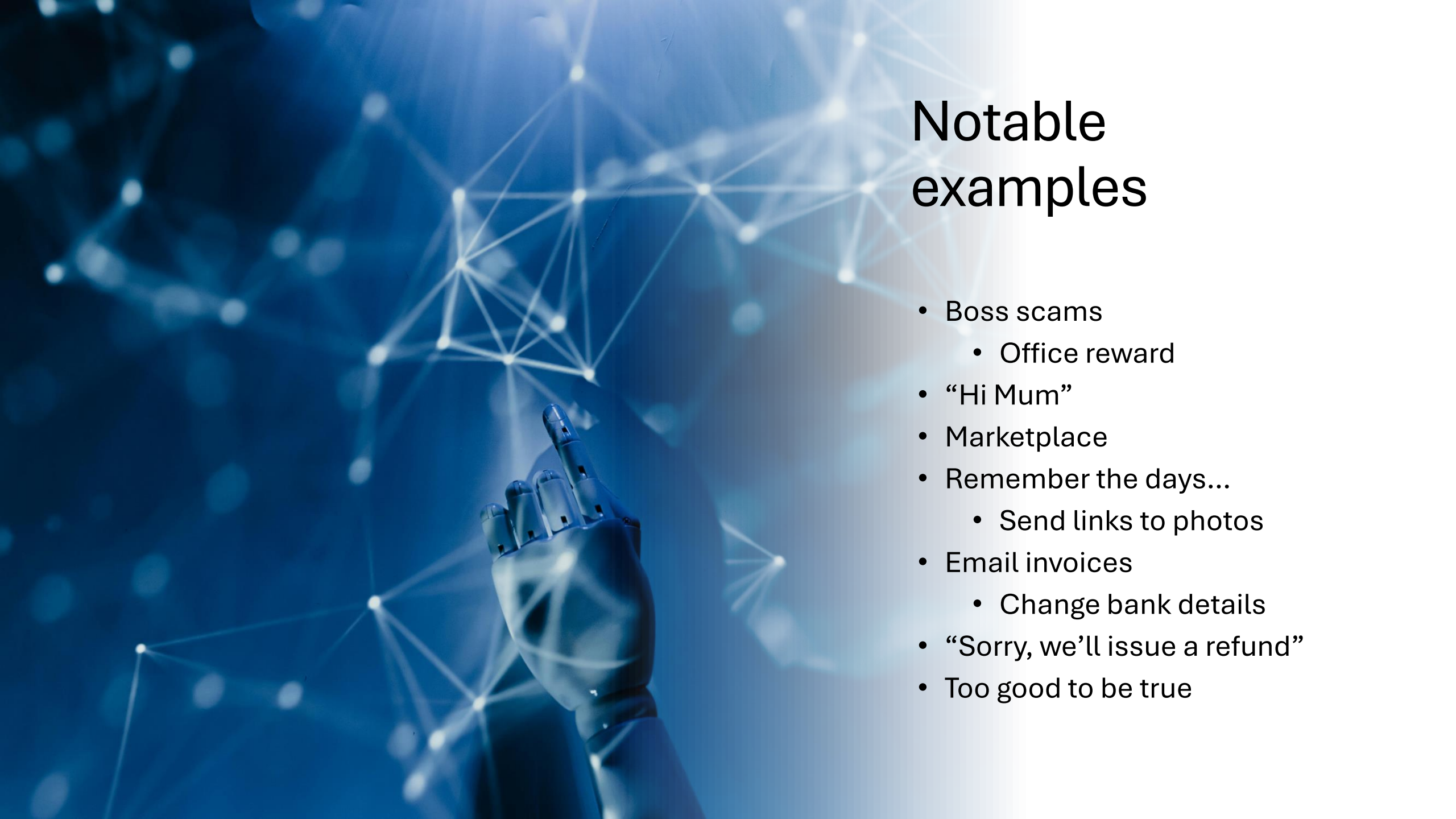
Sneak malware onto your PC

### BOTNETS



Turn your PC into a zombie





# Notable examples

- Boss scams
  - Office reward
- “Hi Mum”
- Marketplace
- Remember the days...
  - Send links to photos
- Email invoices
  - Change bank details
- “Sorry, we’ll issue a refund”
- Too good to be true

# What to watch out for

- Use of proper names, not user names
- Links point to where they purport to go
- Sender address is unusual
  - Not from the actual sender
  - Weird address
  - Misspellings
- Signature block has an authorized person
- Different payment method/details
  - Gift cards
- Threaten urgent action if ignored
- Misspellings and poor grammar
- Requesting sensitive information



# Where is my data going and how is it being used?

- The Dark Web
- The regular web (the Internet as you know it)
- What is the Dark Web?
- How much does it cost to buy info on the Dark Web?





# Who are these Cyber Criminals and what do they want?

- Cyber criminal environment.
- Cyber criminals want to take the path of least resistance.
- The more of the puzzle they have, the more effective or efficient they can be in their attacks.
- Government sponsored cyber attacks can still impact you.
  - You may unwittingly be the path of least resistance.
  - Dedicated hackers may use you and your devices to work against another government target.
  - You may have records with a government agency that is attacked.

# What can we do?

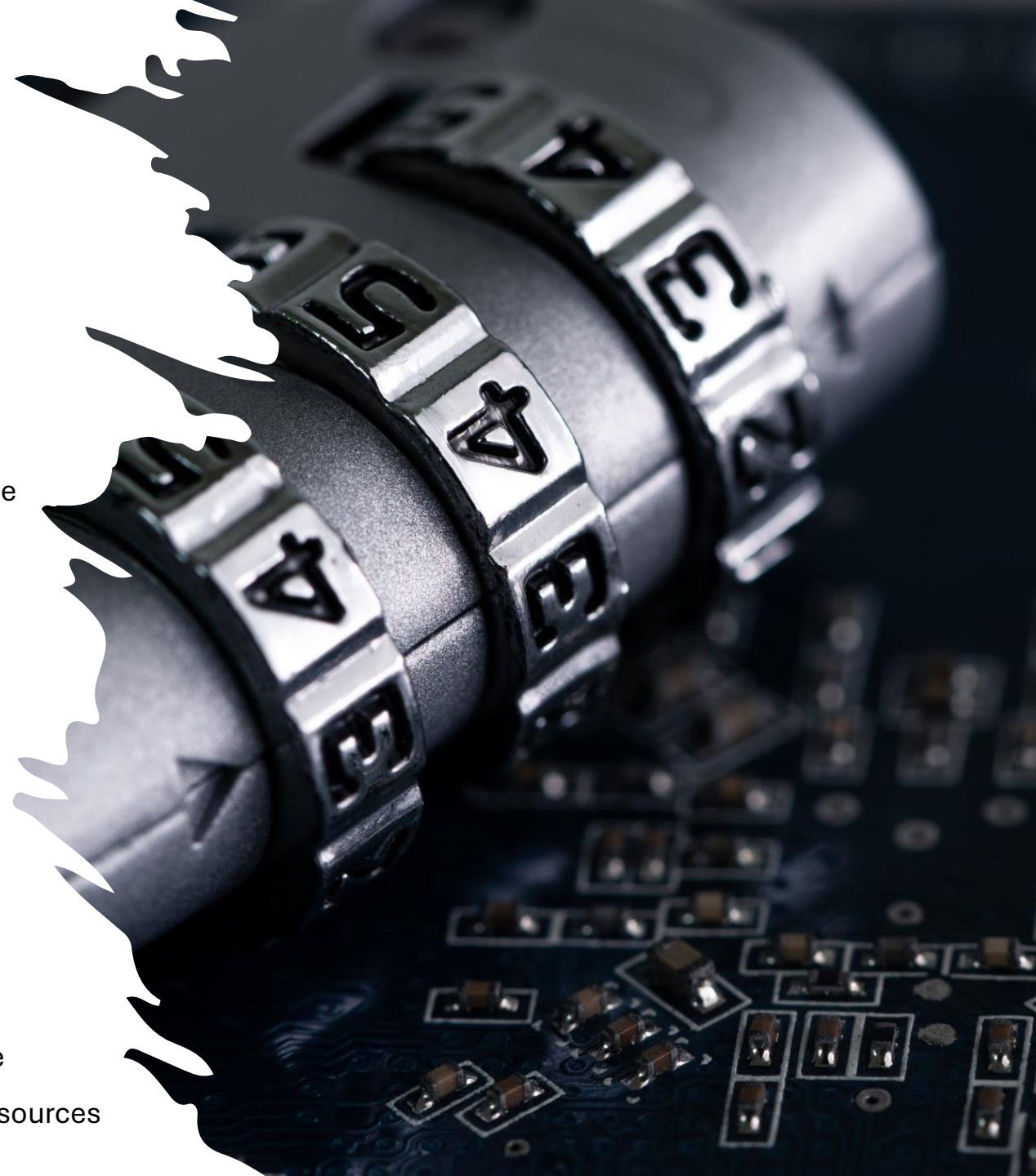
- Don't abandon hope just yet.
- Options for increased cyber security:



" MAYBE WE SHOULD TRY A DIFFERENT  
SECURITY APPROACH THIS YEAR. "

# Increased security precautions.

- Remain vigilant
  - Adopt a “zero trust” mentality – Question everything
    - If it doesn't look right, don't respond
    - If in doubt, ask for help from a reliable, trusted source
- Passwords
  - Create and use long, random passwords
    - FIVE=green+SYDNEY2019
  - Don't use the same password for multiple accounts
  - Don't use variations of the same password
  - Keep passwords in a secure password vault
  - Change passwords regularly
  - Enable two-factor authentication where possible
- Software
  - Install and maintain reliable, reputable, anti-virus software
  - Ensure all software/applications are from verified, trusted sources



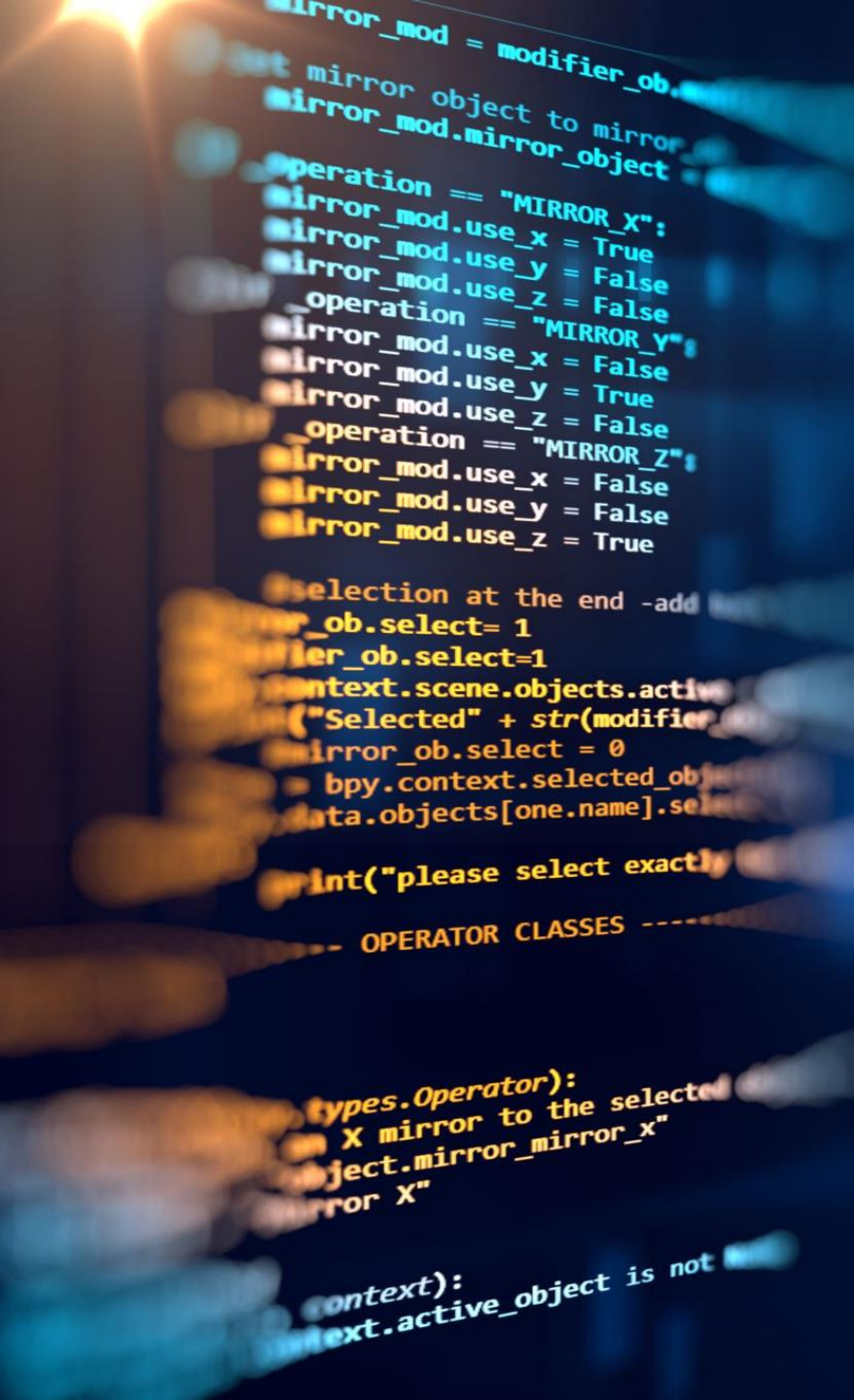


- Devices
  - Keep your devices updated with legitimate updates
  - Don't allow others, especially strangers, to use your devices
- Backups
  - Backup your data/files/information regularly with a trusted medium/source
- Communications
  - Have a disposable separate email address for online shopping etc.
  - Don't interact with questionable communications (phone/message/email)
  - If uncertain, contact the source directly via confirmed safe channels
  - Don't provide information to individuals and entities that contact you directly. Ask for a reference number and call the company back directly using trusted methods
  - Use a VPN (Virtual Private Network) where possible



# Additional links

- Tools
  - Check your passwords, phone numbers and email addresses for breaches
    - <https://haveibeenpwned.com/>
  - Check for scam messages
    - <https://us.norton.com/products/genie-scam-detector>
    - <https://nordvpn.com/link-checker/>
  - Cyber security tips
    - <https://www.cyber.gov.au/resources-business-and-government/essential-cyber-security/essential-eight/essential-eight-explained>
    - <https://www.homeaffairs.gov.au/about-us/our-portfolios/cyber-security/strategy/act-now-stay-secure>
- Resources
  - Data breaches
    - <https://www.upguard.com/blog/biggest-data-breaches-australia>
  - Cyber Crime Reports
    - [https://www.aic.gov.au/sites/default/files/2023-06/sr43\\_cybercrime\\_in\\_australia\\_2023.pdf](https://www.aic.gov.au/sites/default/files/2023-06/sr43_cybercrime_in_australia_2023.pdf)
    - <https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics>
    - <https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023>
  - Statistics
    - <https://aag-it.com/the-latest-cyber-crime-statistics/>





```

mirror_mod = modifier_ob.
set mirror object to mirror
mirror_mod.mirror_object
operation == "MIRROR_X":
mirror_mod.use_x = True
mirror_mod.use_y = False
mirror_mod.use_z = False
operation == "MIRROR_Y":
mirror_mod.use_x = False
mirror_mod.use_y = True
mirror_mod.use_z = False
operation == "MIRROR_Z":
mirror_mod.use_x = False
mirror_mod.use_y = False
mirror_mod.use_z = True

selection at the end -add
mirror_ob.select= 1
modifier_ob.select=1
context.scene.objects.active
("Selected" + str(modifier
mirror_ob.select = 0
= bpy.context.selected_obj
data.objects[one.name].select

print("please select exactly

-- OPERATOR CLASSES -----

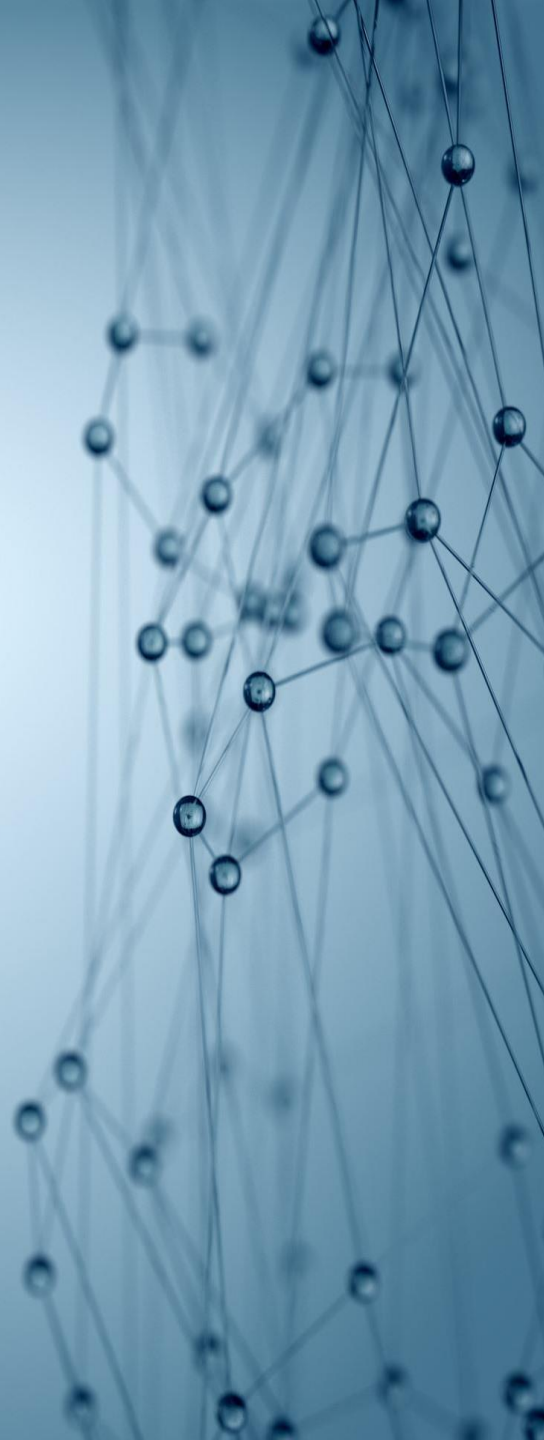
types.Operator):
X mirror to the selected
object.mirror_mirror_x"
mirror X"

context):
context.active_object is not

```

- Resources continued
  - SCAM Watch
    - <https://www.scamwatch.gov.au/types-of-scams/>
- Support
  - ID Care
    - <https://www.idcare.org/contact>





- Test your knowledge
  - <https://www.abc.net.au/news/2023-11-18/bank-bogus-octo-scam-apps-phishing/102992426>
- Reporting cyber crime
  - <https://www.cyber.gov.au/report-and-recover/report>
  - <https://www.afp.gov.au/crimes/cybercrime>
- DEFCON Videos
  - Social engineering
    - <https://www.youtube.com/watch?v=lc7scxvKQOo>
    - [https://www.youtube.com/watch?v=bU\\_ydNRZ\\_9s](https://www.youtube.com/watch?v=bU_ydNRZ_9s)
  - Penetration testing
    - <https://www.youtube.com/watch?v=VJ4FDOw9Ncl>
- Background image
  - [https://www.freepik.com/free-photo/html-css-collage-concept\\_36295537.htm](https://www.freepik.com/free-photo/html-css-collage-concept_36295537.htm)
    - Image by Freepik

---

- References

- <https://www.upguard.com/blog/biggest-data-breaches-Australia>
- <https://slashnext.com/state-of-phishing-2023/>
- <https://www.techtarget.com/whatis/34-Cybersecurity-Statistics-to-Lose-Sleep-Over-in-2020>
- <https://www.csoononline.com/article/3153707/top-cybersecurity-facts-figures-and-statistics.html>
- <https://www.imperva.com/resources/resource-library/reports/2023-imperva-bad-bot-report/>
- <https://www.techtarget.com/whatis/34-Cybersecurity-Statistics-to-Lose-Sleep-Over-in-2020>
- <https://www.verizon.com/about/news/2023-data-breach-investigations-report>

- Metadata

- <https://www.abc.net.au/news/2015-08-24/metadata-what-you-found-will-ockenden/6703626>
- <https://kieranhealy.org/blog/archives/2013/06/09/using-metadata-to-find-paul-revere/>

- How they get my info

- <https://www.upguard.com/blog/biggest-data-breaches-Australia>

- Facebook breach

- <https://haveibeenpwned.com/PwnedWebsites#Facebook>

<https://digitalgp.com.au/2024/04/cyber-security-presentation/>

