Cyber Security Presentation

Group UG41

Intro

What is cyber security?

- Ways of protecting a system from cyber attacks

What is a cyber-attack?

- Any malicious attempt to harm, alter or access a computer system or the information it stores

Cyber-attacks are happening at an increasing rate

Today we'll discuss some attacks that have happened in the last year

Overview

Recent Cyber Security Issues

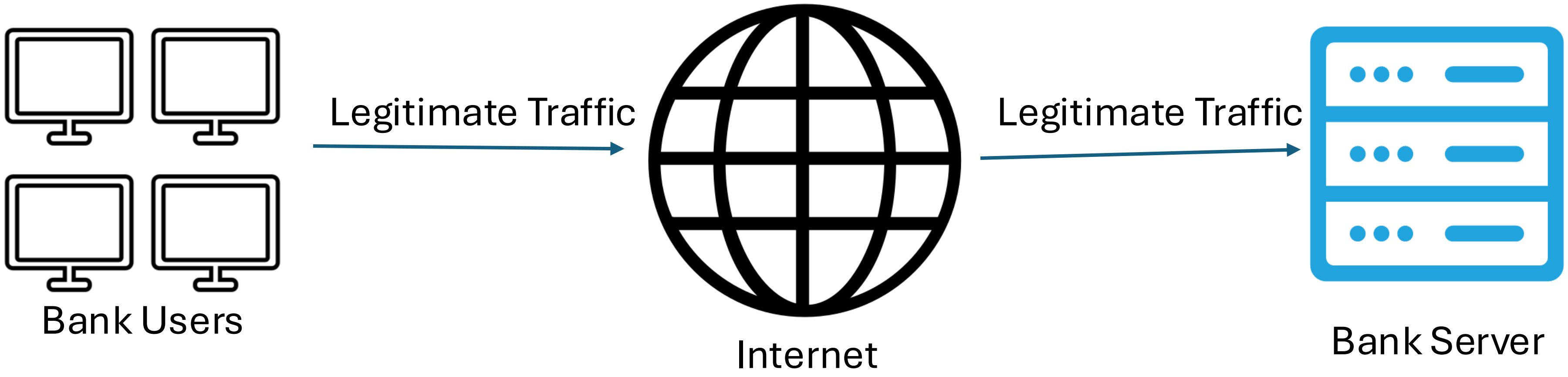
Overview: Public

- There has been a series of outages across multiple banks:
  - Taylors Bank and NWCU compromised:
    - NWCU breach in mid-July
    - Account details found being sold
    - Taylors Bank breach in August
  - Other major banks downtime:
    - Cause unclear currently

https://www.streamnetworks.co.uk/can-we-be-more-prepared-for-outages

Overview: Public

- Possible Distributed Denial of Service attack:



Bank Users

Legitimate Traffic

Internet

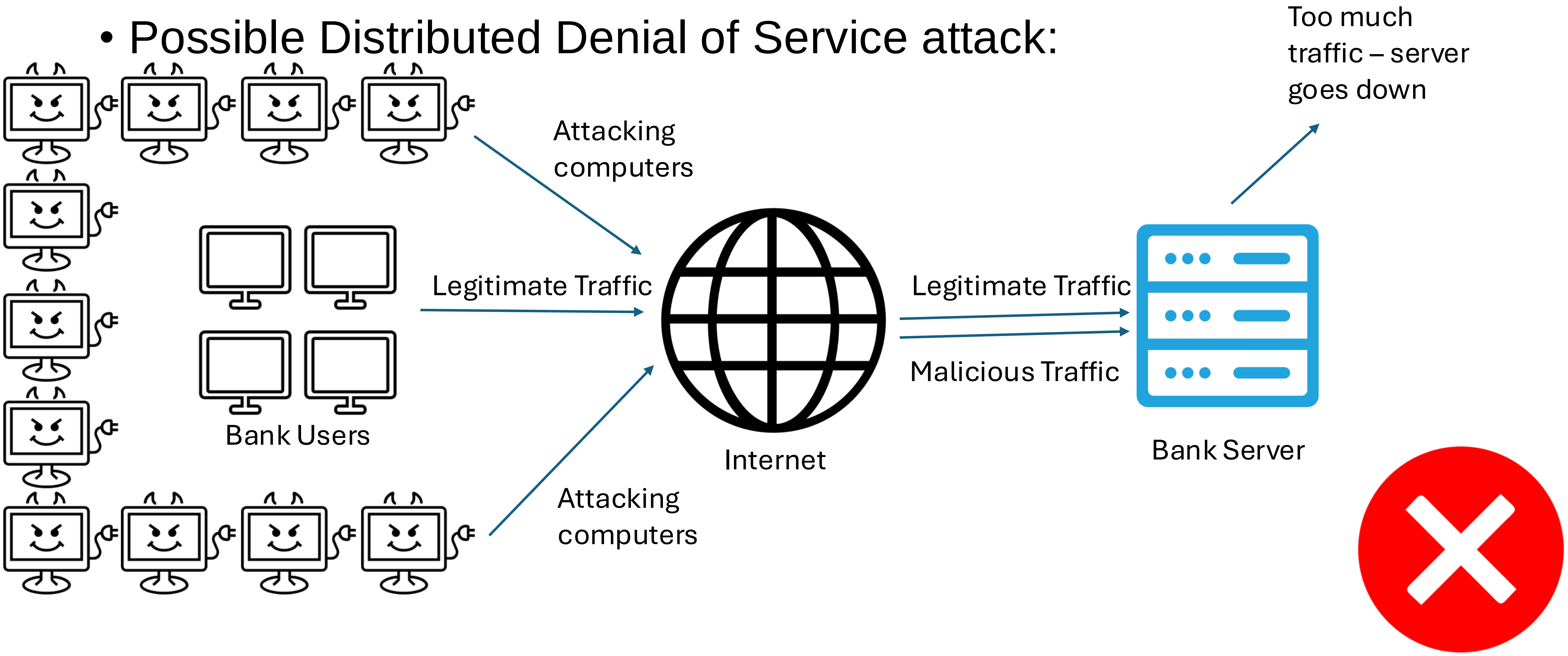
Legitimate Traffic

Bank Server

✓

Overview: Public

- Possible Distributed Denial of Service attack:



Too much traffic – server goes down

Attacking computers

Bank Users

Legitimate Traffic

Internet

Legitimate Traffic

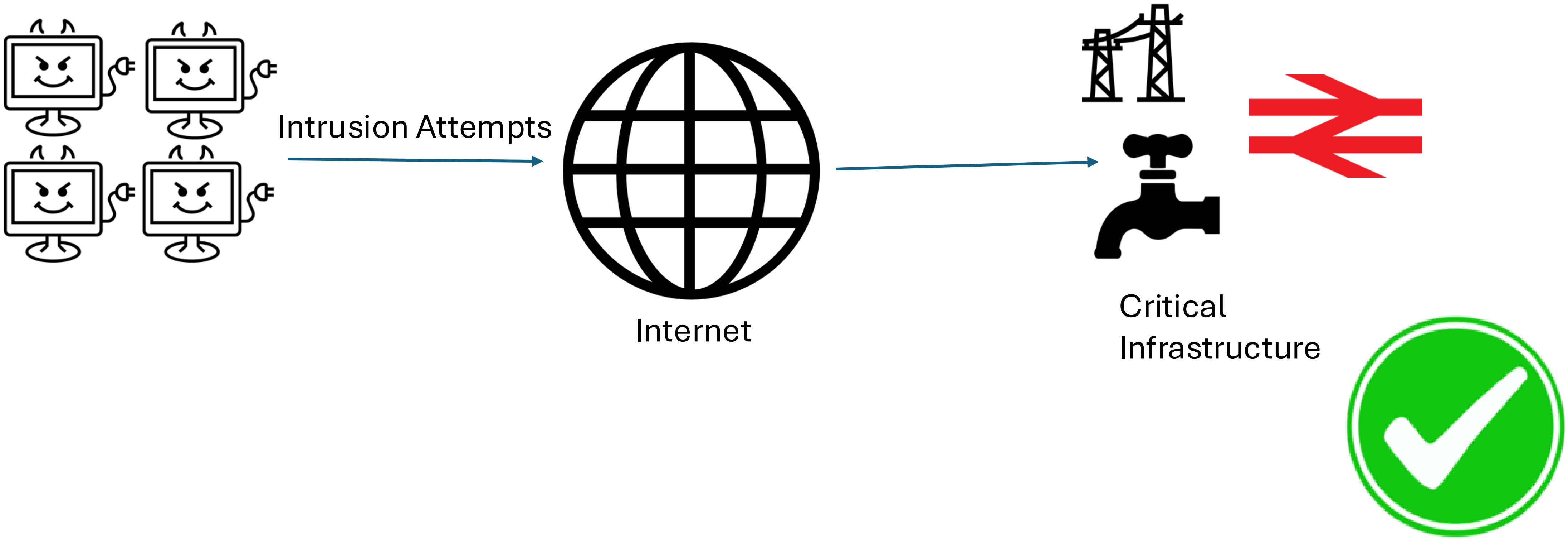
Malicious Traffic

Bank Server

Attacking computers

Overview: Public

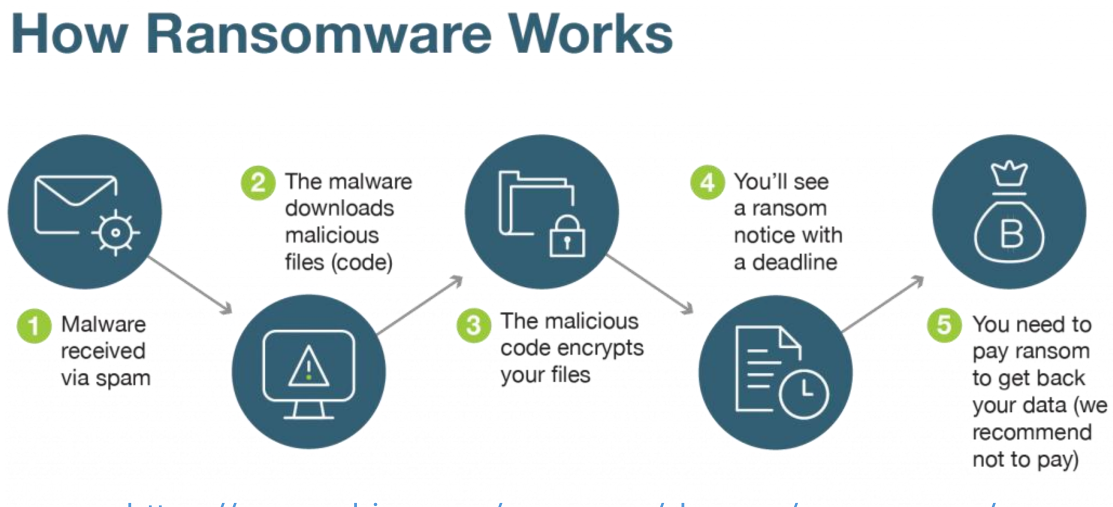
- Infrastructure Intrusions:



Overview: Businesses

There's been an increase in ransomware attacks in the past year

- Attackers install software onto a system to lock it, then demand a fee
- Often done through phishing attacks
    - Emails from attackers pretending to be other people or systems
    - Trick you into entering your login information or to download something
- The systems were insured and recovered
- Not always the case



How Ransomware Works

1 Malware received via spam

2 The malware downloads malicious files (code)

3 The malicious code encrypts your files

4 You'll see a ransom notice with a deadline

5 You need to pay ransom to get back your data (we recommend not to pay)

https://www.yubico.com/resources/glossary/ransomware/

Overview: Businesses

The issues at NWCU and Taylor's Bank were due to:

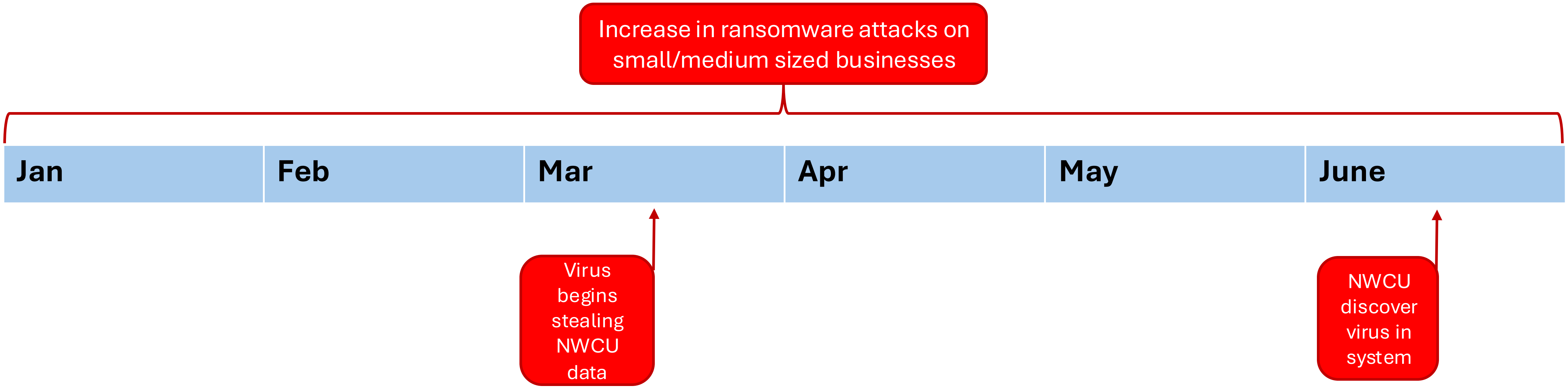
- Lack of risk management and auditing
- Staff not knowing how to spot or respond to attacks
    - Took NWCU three weeks to report their breach after discovery
    - Senior staff at Taylor's Bank fell for spear-phishing attack
        - A form of phishing where the attacker targets a high-level person in an organisation
        - Used bank information collected in the NWCU attack

Taylor's Bank's systems went down the day after they started investigating

Resulted in:

- Customers withdrawing money
- Impacted the stock market
- Other bank systems going down

Timeline: 2024



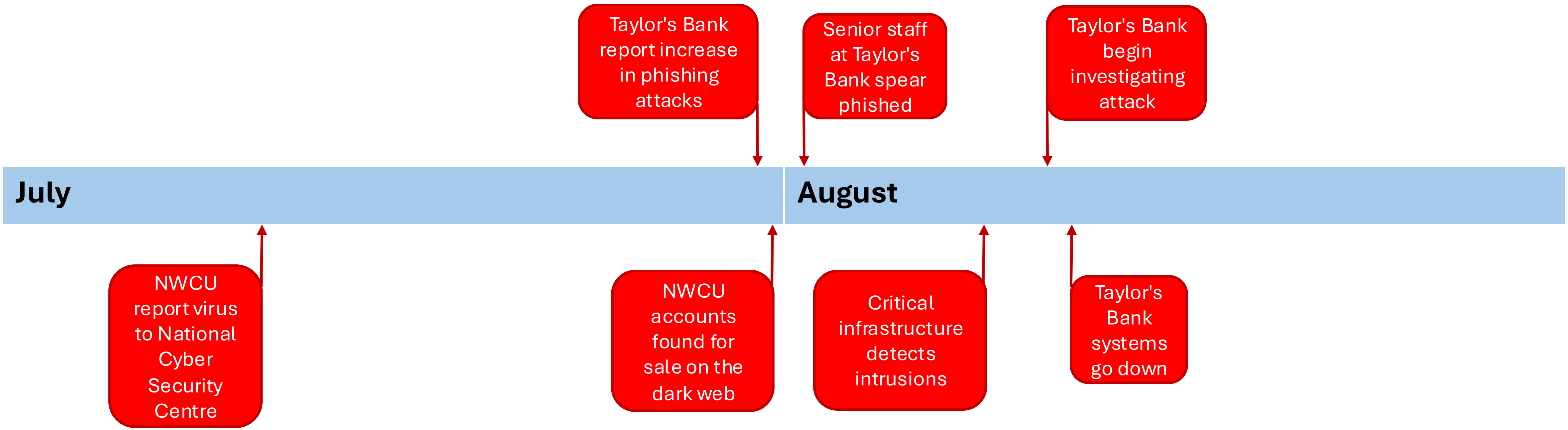
Increase in ransomware attacks on small/medium sized businesses

Jan | Feb | Mar | Apr | May | June

Virus begins stealing NWCU data

NWCU discover virus in system

Timeline: 2024



July

NWCU report virus to National Cyber Security Centre

Taylor's Bank report increase in phishing attacks

NWCU accounts found for sale on the dark web

August

Senior staff at Taylor's Bank spear phished

Critical infrastructure detects intrusions

Taylor's Bank begin investigating attack

Taylor's Bank systems go down

Possible Threat Actors

https://intellectualpoint.com/understanding-threat-actors-101/

Possible Threat Actors – Motive and Gain

https://www.thebluediamondgallery.com/handwriting/m/motive.html

Possible Threat Actors: Money

Cyber criminals

Insiders (Accidental and Malicious)

https://stock.adobe.com/uk/images/pile-of-money-and-a-bag-of-coins-wealth-concept-vector-illustration/430081855

Possible Threat Actors: Confusion and panic

Cyber Terrorist

Nation State

https://www.istockphoto.com/photos/stock-market-down

Unlikely Threat Actors

Hacktivist

Thrill Seeker

https://www.stockvault.net/free-photos/hacktivists

Which Threat Actors are responsible?

https://intellectualpoint.com/understanding-threat-actors-101/

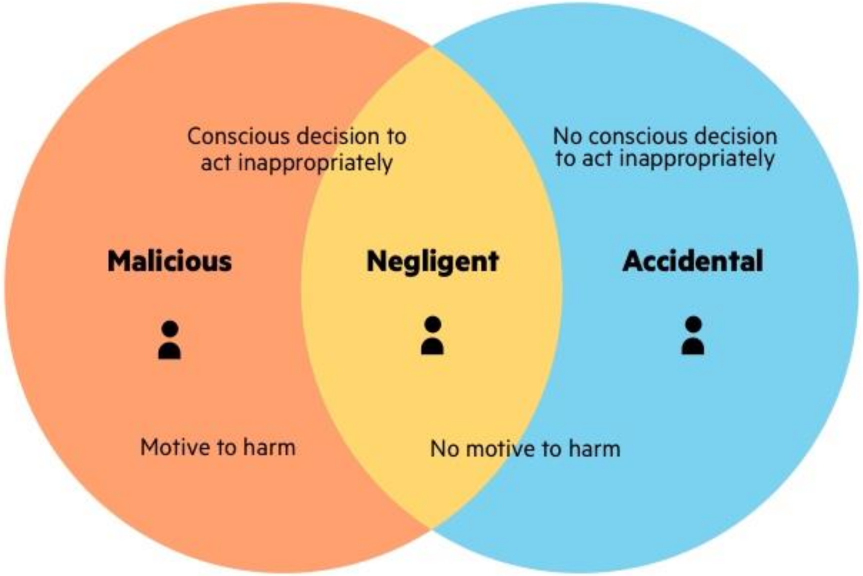
Main Threat Actors – Insiders

Accidental Insiders

- Due to Human error
- Unintentional

Malicious Insiders

- Purposeful attack
- Intentional


Conscious decision to act inappropriately
No conscious decision to act inappropriately
Malicious
Negligent
Accidental
Motive to harm
No motive to harm

https://www.imperva.com/learn/application-security/insider-threats/

Main Threat Actors – Cyber criminals

Large Financial Gain

Cyber Criminals vs Insiders

Possible large-scale attack

https://www.alamy.com/stock-photo-disguised-computer-hacker-56934520.html

<u>Steps for businesses</u>

Steps for Protection: Businesses

Risk analysis

- Identify and rank risks with a risk matrix
- Can prioritise risks by their likelihood and severity

Severity

		1	2	3	4	5
	5	🟨	🟨	🟥	🟥	🟥
	4	🟨	🟨	🟨	🟥	🟥
Likelihood	3	🟩	🟨	🟨	🟨	🟥
	2	🟩	🟩	🟨	🟨	🟨
	1	🟩	🟩	🟩	🟨	🟨

Steps for Protection: Businesses

Model threats with STRIDE

- Create diagrams of your system
- Identify threats with STRIDE processes
- Review the risk matrix, plan responses
  - Avoidance, mitigation, transfer, acceptance
- Validate
  - User and unit testing
  - Plan to review the model in the future

	Threat	Property Violated	Threat Definition
S	Spoofing	Authentication	Impersonating a person or system (e.g., an online bank)
T	Tampering	Integrity	Modifying something without authorisation
R	Repudiation	Non-repudiation	Claiming to not have done something that you did
I	Information Disclosure	Confidentiality	Sharing information with people who are not authorised to see it
D	Denial of service	Availability	Preventing other users from accessing a service
E	Elevation of privilege	Authorisation	Giving yourself or someone else a level of access they are not authorised to have

Response	Definition
Avoidance	Avoid the risk by removing whatever is causing the risk
Mitigation	Create plans to handle threats and lessen their impacts
Transfer	Pay a 3rd party to handle the risk for you
Acceptance	The risk is unlikely and would have little impact, therefore it can be tolerated

Steps for Protection: Businesses

Must create a security policy:

- Clear rules for employees to follow
  - Unambiguous wording
  - Define key terms
  - Explain the consequences of breaching the policy

- Helps to maintain and protect information systems

- Protects and informs employees
  - Helps them understand their responsibilities
  - Increase their personal security with password policies

- Helps your business meets legal requirements
  - Helps you to comply with regulations such as GDPR, which breaching would result in heavy fines

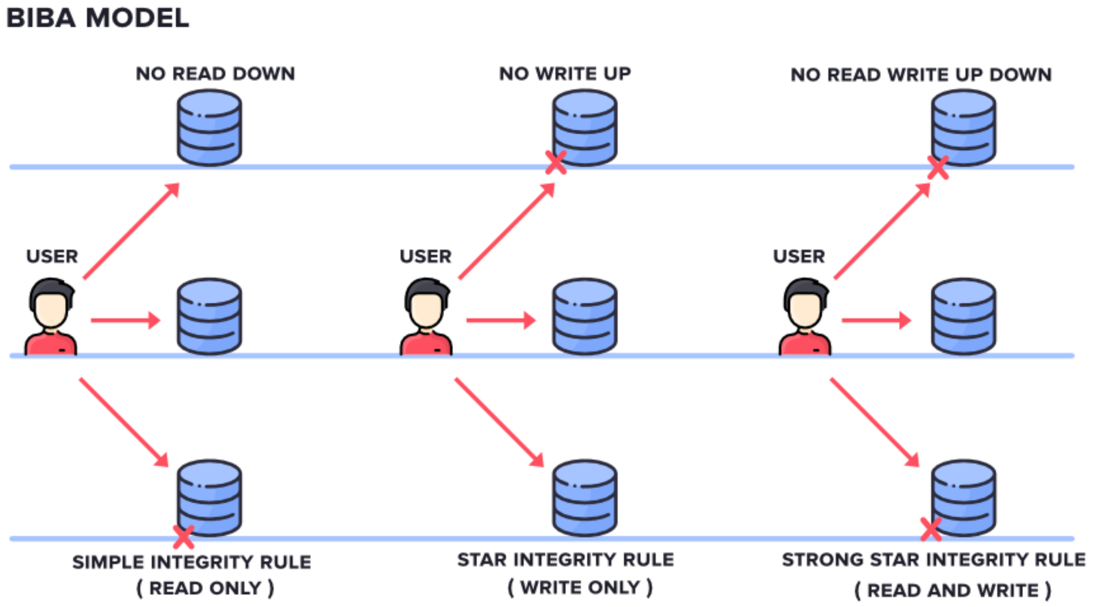
- Should be regularly updated

Steps for Protection: Businesses

There are existing data models for security policies

The Biba model:

- Identify your system's critical data
- Organise the data into levels of integrity
- Decide what access levels different employees should have
    - Users are not allowed to write to data at a higher level of integrity
- Protects integrity of data
    - Employees cannot alter data without permissions
    - Reduces insider threat



https://www.geeksforgeeks.org/introduction-to-classic-security-models/

Steps for Protection: Businesses

Initial cyber security training and refresher courses for staff

- Must know from the beginning of their employment how to identify and respond to threats
- Should have their knowledge regularly tested and updated as new threats are developed

Use MFA to make staff prove their identies before accessing the system

- Multiple security checks when signing in to prevent unauthorised access to the system

Use firewalls and anti-virus software to regularly scan your systems for threats

- Reduce the risk of malicious software entering your system
- Helps you detect anything malicious as soon as possible

Creates backups that can be used to restore your system

- Ensures that if your system goes down, it will be available again as soon as possible

Filter staff emails for spam

- Reduce the risk of phishing attacks by storing anything suspicious in the spam folder

Should keep logs of the activity in your systems

- Record what has been done, who did it, and at what time

Should have access control levels for staff

- Only have a necessary level of access to the system for their job
- Access privileges should be immediately revoked when they leave their role

Steps for public

Steps for Protection: Public - Overview

Overview: Due to rising cyber-crime, the public faces increasing cyber threats. This can harm for public so it's important to follow these steps to stay safe.

Threats the public may face:

- Phishing – A threat where hackers will create fake websites or emails to steal personal or organisation information
- Social Engineering - Manipulates peoples trust to get sensitive data or access secure systems
- Disruption of Critical Infrastructure – Intrusions may disrupt essential services like the rail network and the power grid
- Data Breaches – Gaining unauthorised access to sensitive data such as customer information
- Malware Infection – This is harmful software such as viruses, ransomware, and spyware

Steps for Protection: Public – Secure Passwords

Why it's important:

Strong passwords help prevent unauthorised access to your sensitive information such as banking accounts, and emails.

Strong Passwords:

- Ih0peYouGiv3M3FullMarks!
- Wo9@z£Ro9K#dV4z

Weak Passwords:

- Password123
- Tom2004

Recommended tools to use:

Password Managers:

- Generates very secure passwords for you
- Securely stores your passwords for multiple accounts
  - Nord Pass
  - Bit Defender
  - Dashline

2FA (two factor authentication)

5 | TIPS ON CREATING A SAFE PASSWORD

☑ Length
- Password should be 12-16 characters

☑ Complexity
- Use a variation of both uppercase and lowercase letters, special character (?!)

☑ Unpredictability
- Don't use names dates or other common phrases that are guessable

☑ Randomness:
- Avoid patterns and sequences (ABCD, 5678)

☑ Uniqueness:
- Avoid using the same password for everything

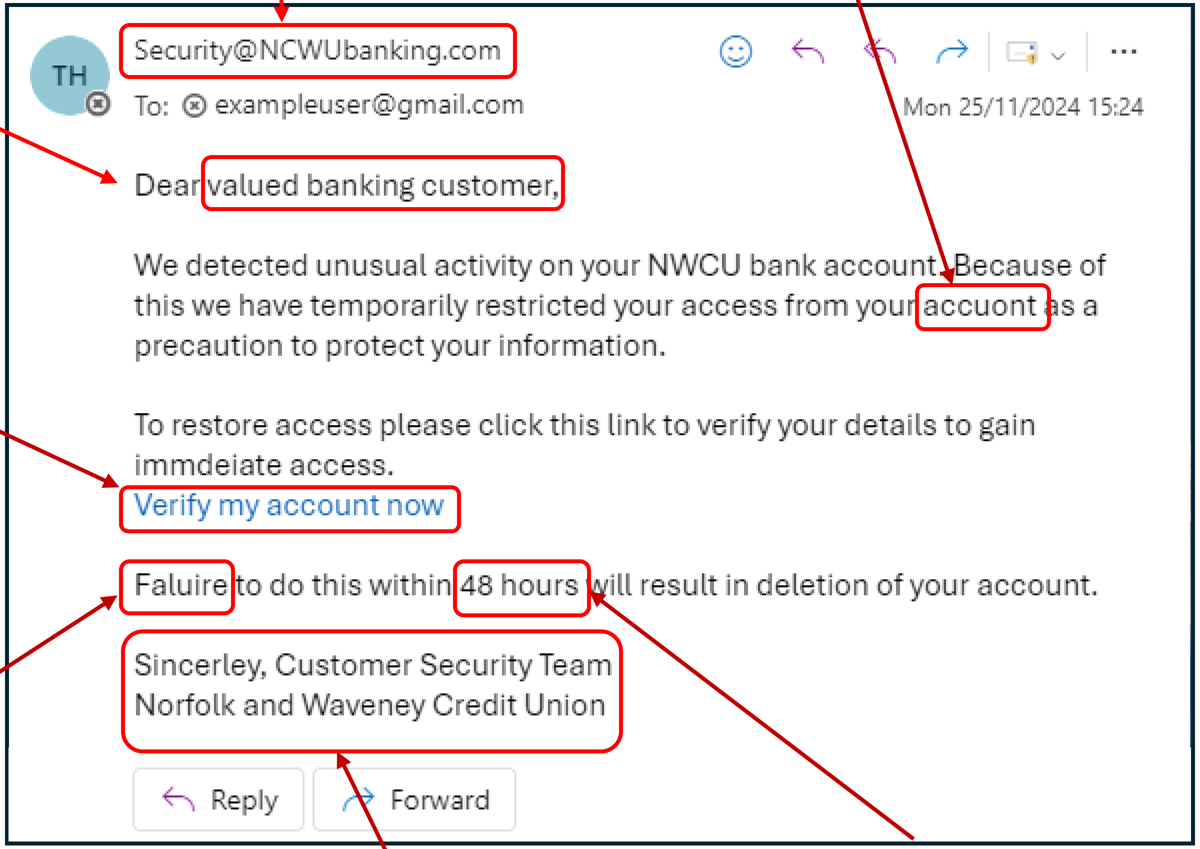
Steps for Protection: Public - Phishing

What is Phishing? Phishing is a cyber-attack where hackers will impersonate a person or organization to trick you into giving sensitive information. Around 30% of adults have experienced a phishing attack in 2024 (statista.com)

Example: A hacker sends an email pretending to be a bank with a link to a fake login screen where the website will extract your inputted details

What to do if you suspect you've been sent one:

- Report the email
  - UK Government Phishing reporting service
  - Action Fraud
  - Email providers like Gmail have an inbuilt option



Security@NCWUbanking.com

To: exampleuser@gmail.com

Mon 25/11/2024 15:24

Dear valued banking customer,

We detected unusual activity on your NWCU bank account. Because of this we have temporarily restricted your access from your accuont as a precaution to protect your information.

To restore access please click this link to verify your details to gain immdeiate access.

Verify my account now

Faluire to do this within 48 hours will result in deletion of your account.

Sincerley, Customer Security Team
Norfolk and Waveney Credit Union

Suspicious email address. Doesn't match the banks name

Spelling errors

Not addressing the recipient

Suspicious link/ unclear link

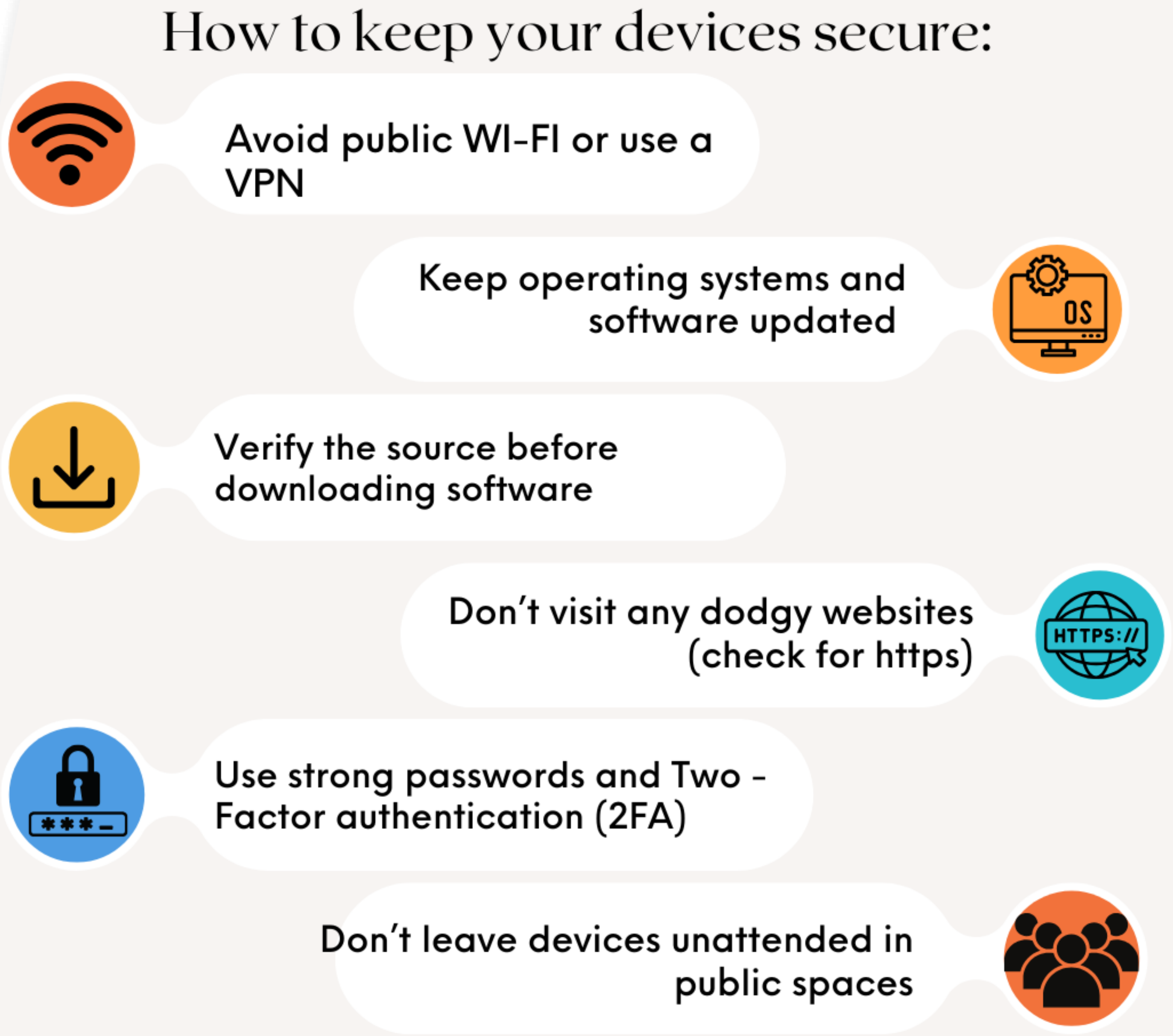
Spelling errors

Claims to be the Customer security teams however there is no direct contact info

Threatens account deletion in 48 hours to pressure the victim

Steps for Protection: Public - Keeping devices secure

- Making sure are personal devices are secure is important to protecting our data and accounts from hackers



How to keep your devices secure:

Avoid public WI-FI or use a VPN

Keep operating systems and software updated

Verify the source before downloading software

Don't visit any dodgy websites (check for https)

Use strong passwords and Two - Factor authentication (2FA)

Don't leave devices unattended in public spaces

Steps for Protection: Public - Monitoring

Monitor bank accounts

Use tools to check for data breaches

NWCU account details sold on the dark web

Change password if your data has been leaked

Steps for Protection: Public - Conclusion

Free Online Resources and Information

IT Governance Phishing Resources | IT Governance UK

National Cyber Security Centre (NCSC) Phishing: Spot and report scam emails, texts, websites and... - NCSC.GOV.UK

Key points to remember:

- Use Strong passwords (12+ chars, symbols and numbers) and 2FA
- Learn about phishing
- Keep devices updated with the latest software
- Change your password if you have an NWCU account

Conclusion

Today we've discussed:

- An overview of what has happened
- The possible threat actors involved
- Steps for businesses to protect themselves
- Steps for the public to protect themselves

References

Visualisations:

- https://www.yubico.com/resources/glossary/ransomware/
- https://www.geeksforgeeks.org/introduction-to-classic-security-models/
- https://intellectualpoint.com/understanding-threat-actors-101/
- https://www.thebluediamondgallery.com/handwriting/m/motive.html
- https://stock.adobe.com/uk/images/pile-of-money-and-a-bag-of-coins-wealth-concept-vector-illustration/430081855
- https://www.alamy.com/stock-photo-man-in-panic-49949308.html
- https://www.stockvault.net/free-photos/hacktivists
- https://www.alamy.com/stock-photo-disguised-computer-hacker-56934520.html
- https://www.streamnetworks.co.uk/can-we-be-more-prepared-for-outages
- https://www.indusface.com/learning/what-is-a-ddos-attack/
- https://www.imperva.com/learn/application-security/insider-threats/

References – DDOS Slide/Intrusion

- https://thenounproject.com/icon/evil-computer-98569/ - malicious computer
- https://www.veryicon.com/icons/miscellaneous/smart-icon-library/internet-61.html - internet symbol
- https://www.iconpacks.net/free-icon/computer-956.html - computer symbol
- https://www.veryicon.com/icons/miscellaneous/open-ncloud/the-server-4.html - server icon
- https://www.vecteezy.com/png/44448989-round-red-cross-mark - red cross
- https://www.veryicon.com/icons/miscellaneous/intellectual-property/power-grid.html - power
- https://en.m.wikipedia.org/wiki/File:National_Rail_logo.svg - rail
- https://www.vexels.com/png-svg/preview/129025/water-tap-symbol-svg - water

Thank you for listening