caIT

Cybersecurity Essentials

cyber securITy_ IT consulting & training_ cyber awareness_

Technology is Amazing

WiTWA
If you can see her
OPTUS STADIUM
witwa.org.au
@witwa

2021
AUSTRALIAN WOMEN
IN SECURITY AWARDS
IT SECURITY
CHAMPION
FINALIST

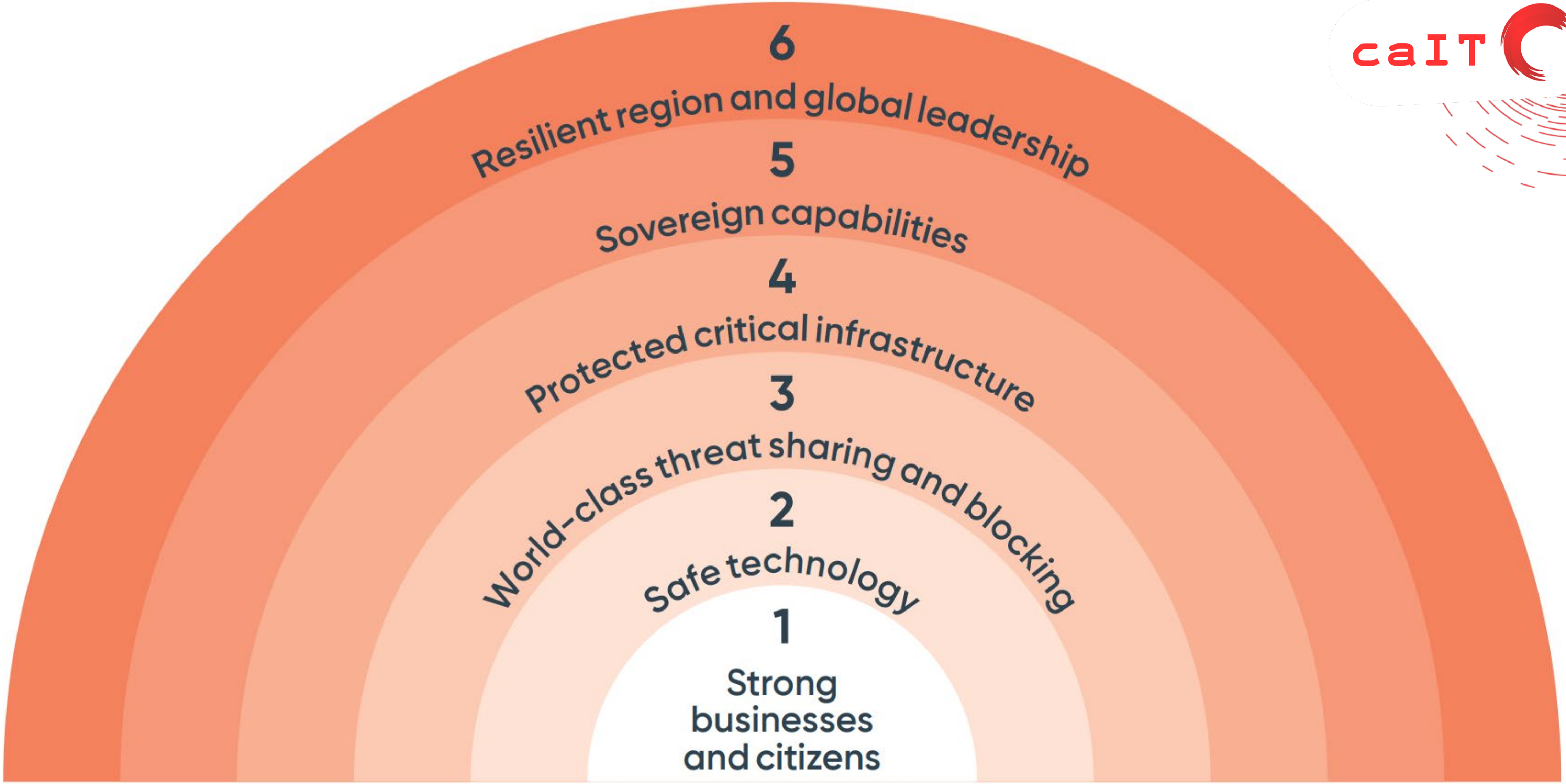
EDITH COWAN
WORLD REA
University
2022 | ECU

"Most hacked nation"

In the last quarter of 2022

client_no:
medicare_no:
app_surname:
app_given:
app_birth_dte:
app_sex:
home_suburb:
home_addr_1:
medibank
medibank

OPTUS
OPTUS
yes
PLAN



6

Resilient region and global leadership

5

Sovereign capabilities

4

Protected critical infrastructure

3

World-class threat sharing and blocking

2

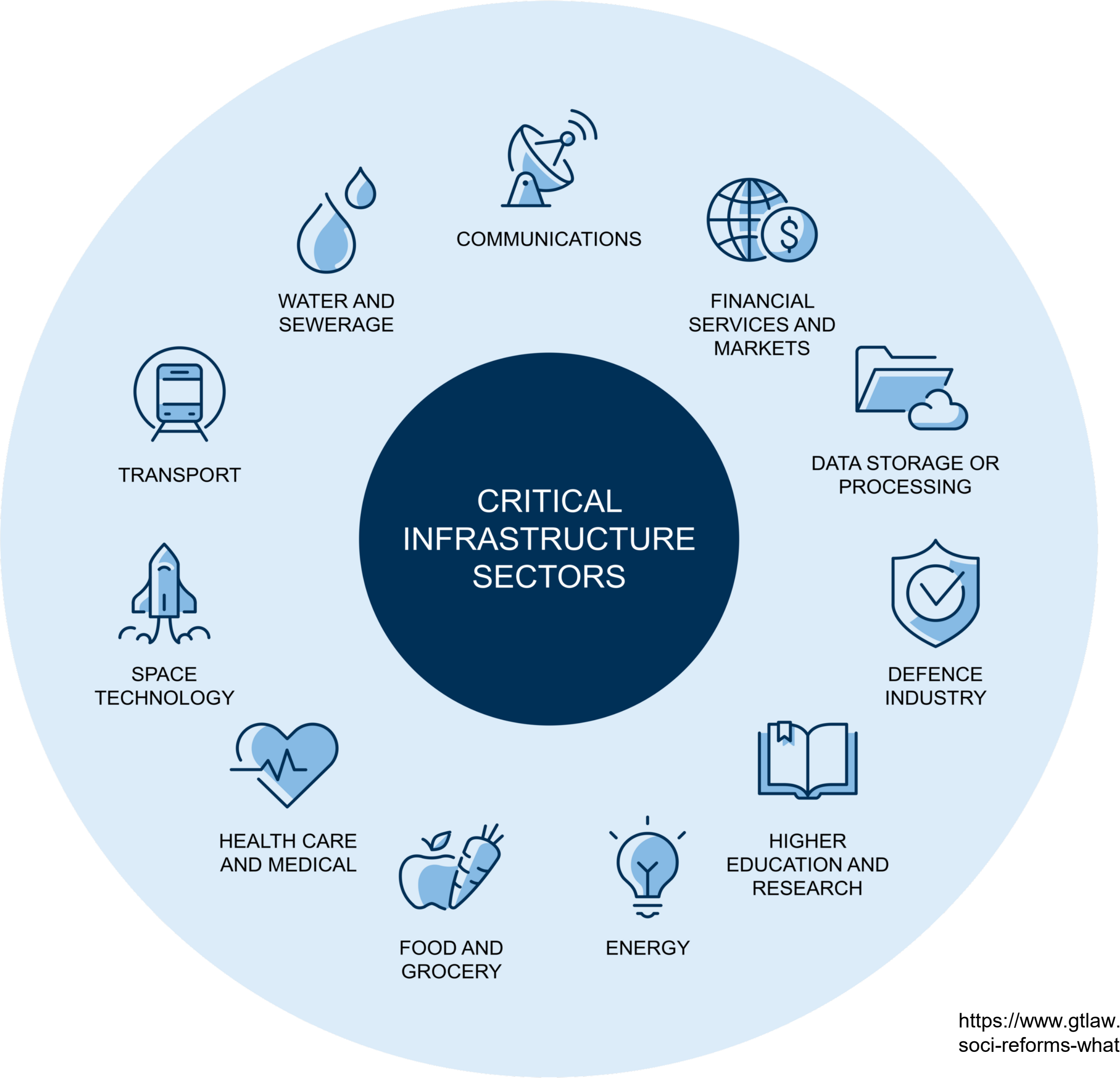
Safe technology

1

Strong businesses and citizens

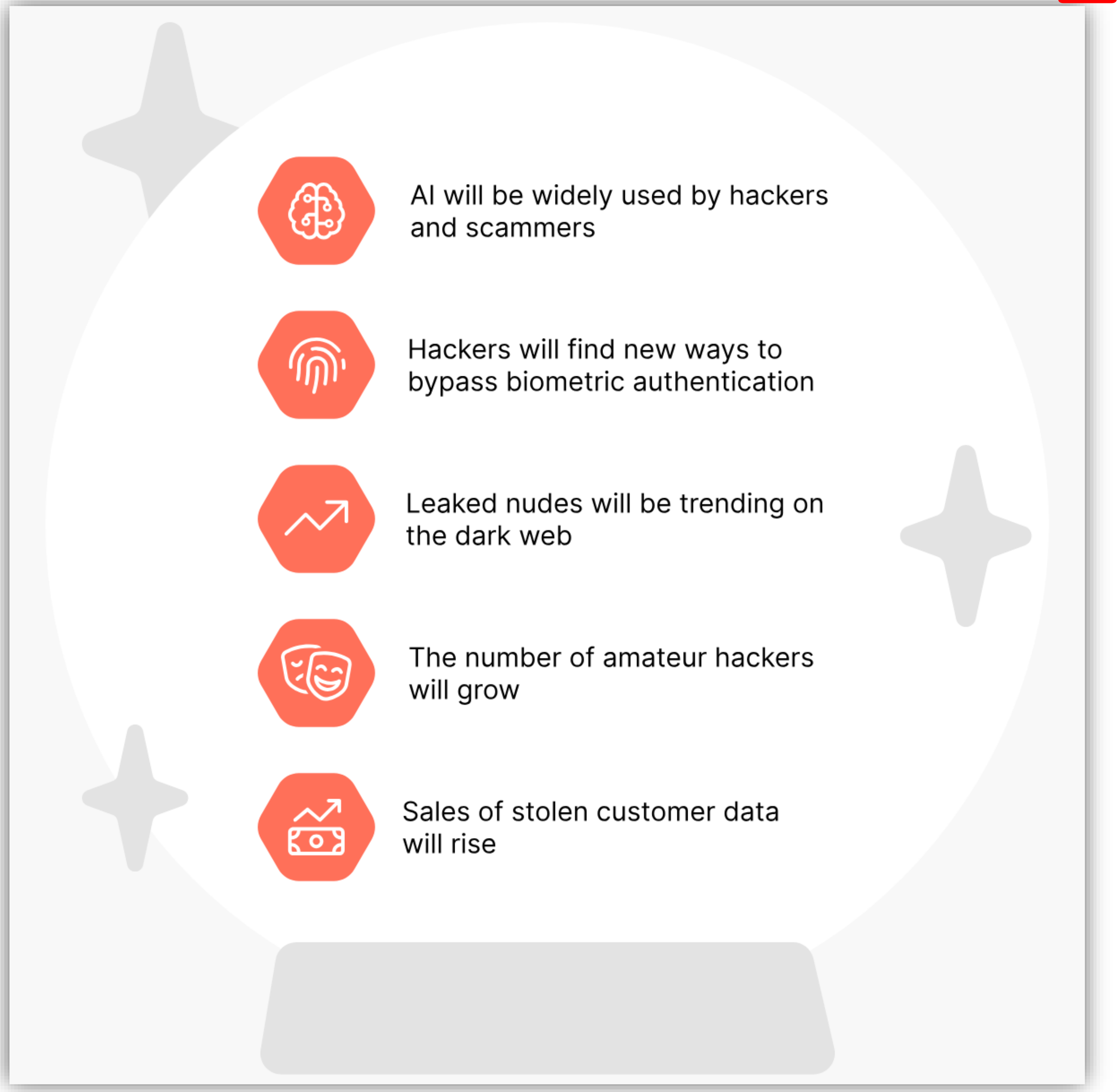
https://www.homeaffairs.gov.au/cyber-security-subsite/files/2023-cyber-security-strategy.pdf

Security Legislation Amendment (Critical Infrastructure) Act 2021 (SOCI Bill)



https://www.gtlaw.com.au/knowledge/security-critical-infrastructure-act-soci-reforms-what-your-business-needs-know

2024 Cybersecurity Predictions

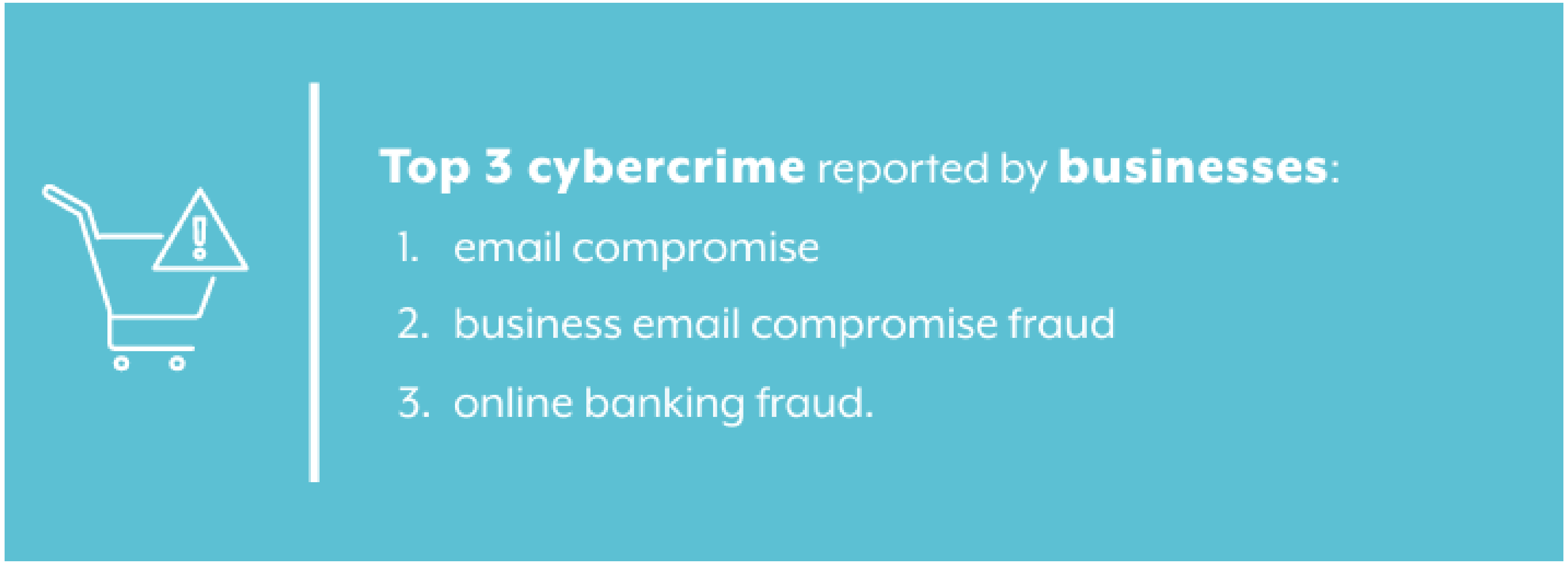


- AI will be widely used by hackers and scammers
- Hackers will find new ways to bypass biometric authentication
- Leaked nudes will be trending on the dark web
- The number of amateur hackers will grow
- Sales of stolen customer data will rise

https://nordvpn.com/blog/cybersecurity-predictions-for-2024/

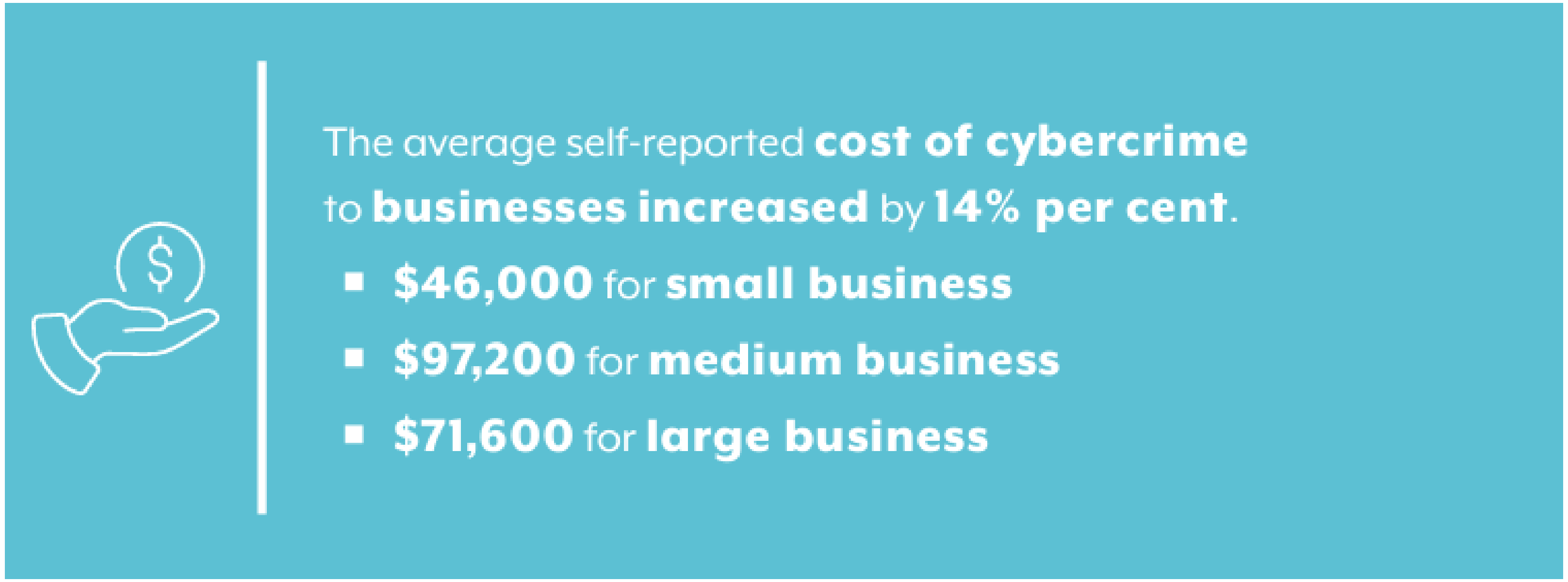
Why Small Businesses are a Target_

1. **Limited Cybersecurity Resources**: Small businesses often lack the budget and resources to invest in robust cybersecurity measures, making them an easier target for cybercriminals than larger organisations.
2. **Valuable Data**: Despite their size, small businesses hold valuable data such as customer information, payment details, and proprietary business information that can be lucrative for cybercriminals.
3. **Less Awareness and Training**: Employees in small businesses may not receive adequate training on cybersecurity practices, leading to vulnerabilities such as falling for phishing scams or using weak passwords.
4. **Third-Party Vulnerabilities**: Small businesses often work with larger companies and can be targeted as a way to gain access to more extensive networks and sensitive information through these connections.
5. **Underestimating the Threat**: Many small business owners believe they are too small to be targeted, leading to complacency and insufficient protective measures, which cybercriminals exploit.



Top 3 cybercrime reported by **businesses**:

1. email compromise
2. business email compromise fraud
3. online banking fraud.



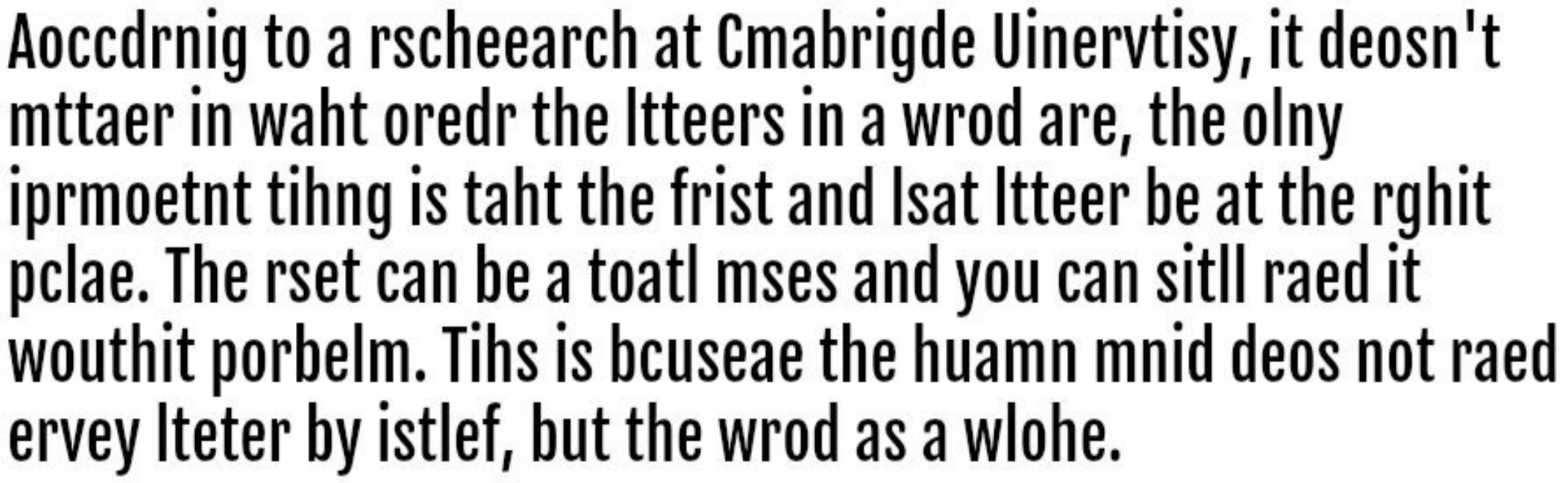
The average self-reported **cost of cybercrime** to **businesses increased** by **14% per cent**.

- **$46,000** for **small business**
- **$97,200** for **medium business**
- **$71,600** for **large business**

https://www.cyber.gov.au/about-us/view-all-content/reports-and-statistics/asd-cyber-threat-report-july-2022-june-2023

What is the number 1 way hackers get into businesses?

PHISHING



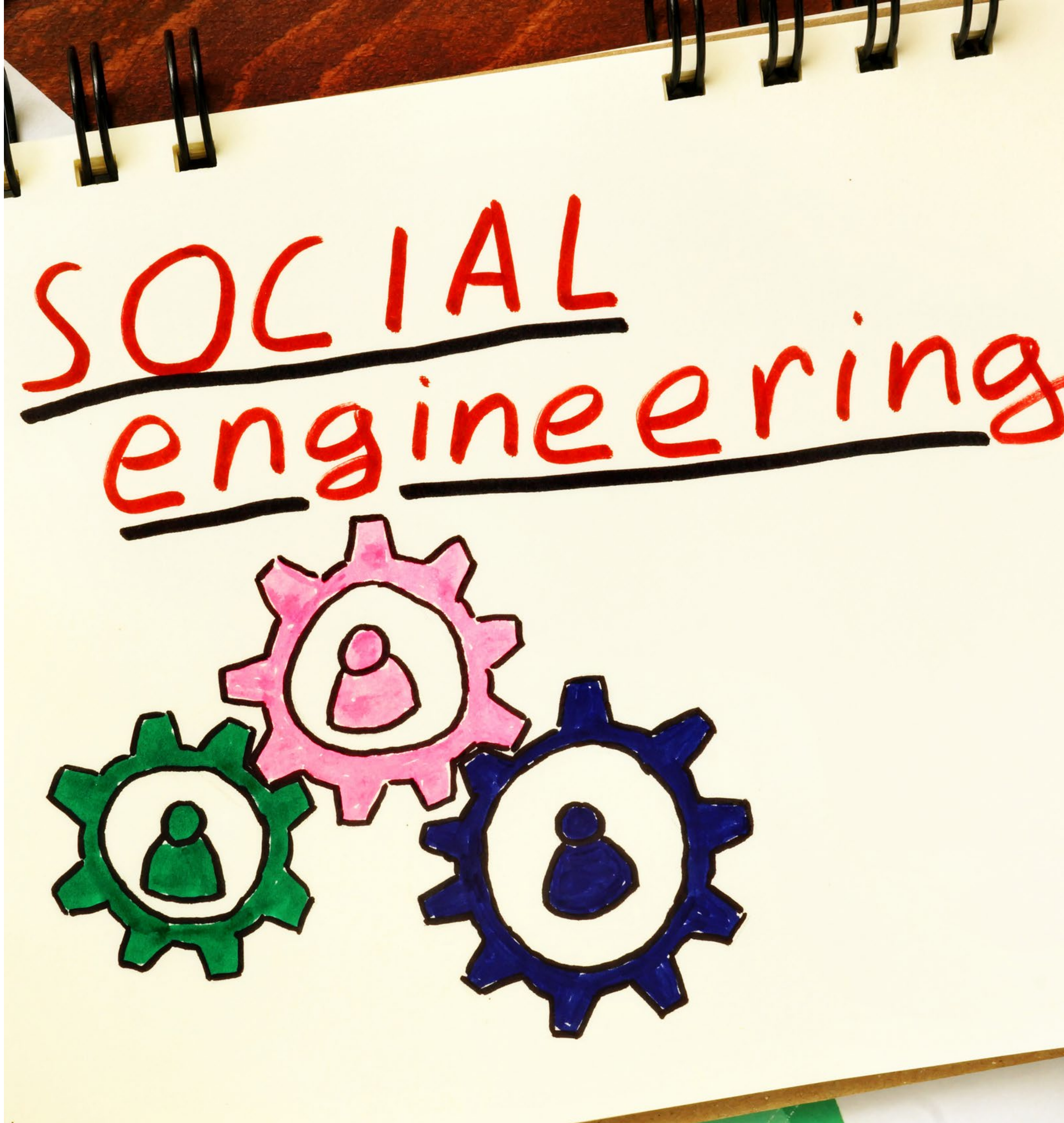
Aoccdrnig to a rscheearch at Cmabrigde Uinervtisy, it deosn't mttaer in waht oredr the ltteers in a wrod are, the olny iprmoetnt tihng is taht the frist and lsat ltteer be at the rghit pclae. The rset can be a toatl mses and you can sitll raed it wouthit porbelm. Tihs is bcuseae the huamn mnid deos not raed ervey lteter by istlef, but the wrod as a wlohe.

Social Engineering

Social engineering involves the **manipulation of individuals** into performing actions or releasing confidential information for the purpose of **information gathering, fraud, and system access**.

ChatGPT:
“Hack This Email!”

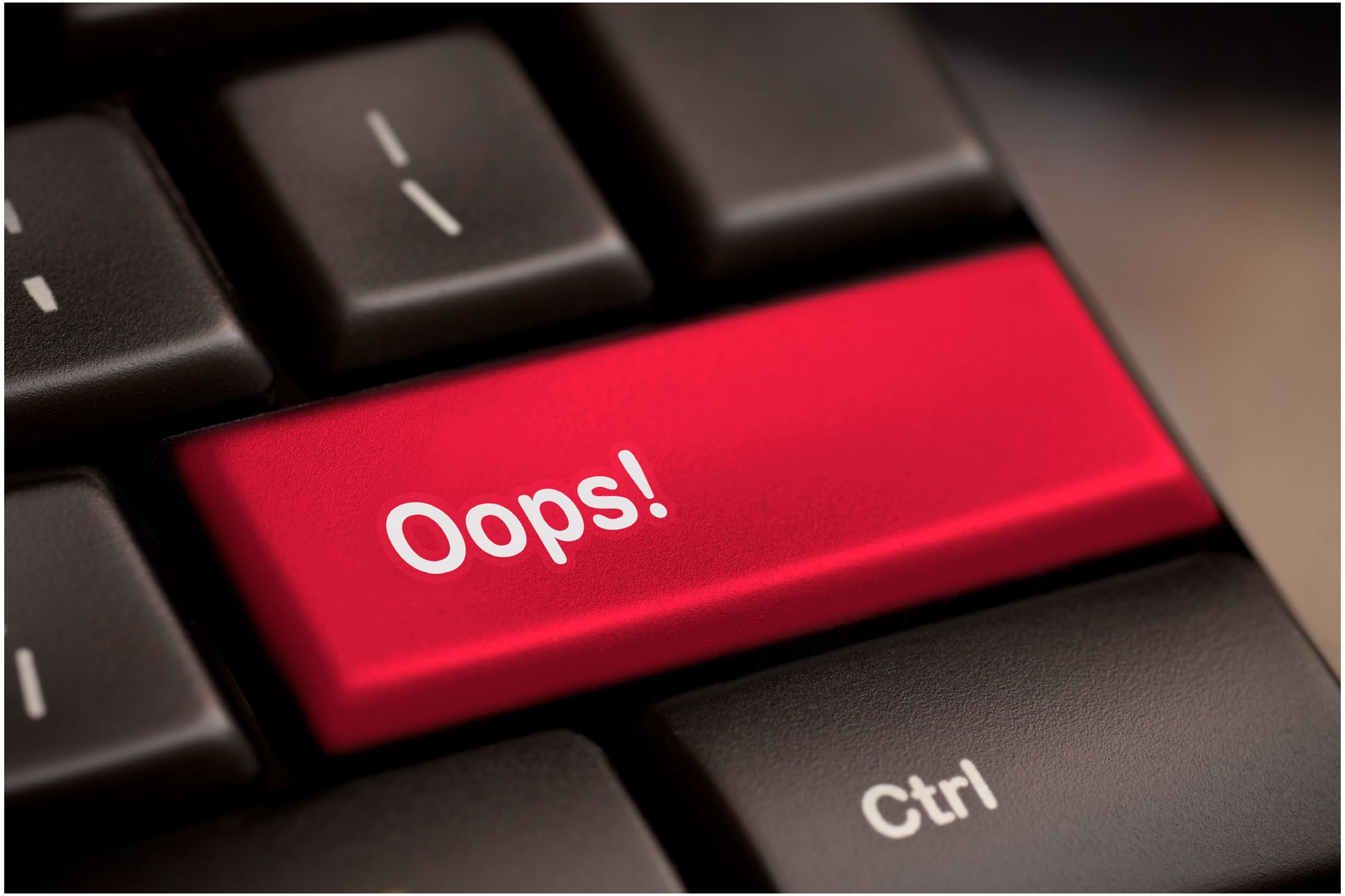
- Fear
- Greed
- Curiosity
- Helpfulness
- Urgency



We all have off days…..

And hackers use this to their advantage

And before you know it…



How to spot a Phish

Learn how to spot a Phishing Email

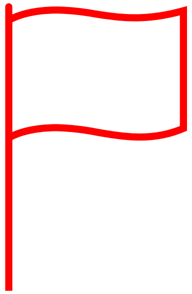
Trigger	Check
A sense of emotion	Look for ‘urgency’ in request
An *unusual* request	Confirm request with sender
Context relevant event	“Was I expecting this email?”
Poor template or signature block	Email reflect normal behaviour?
Unknown sender domain	Confirm identity
Poor grammar	Be detail oriented
Unusual or obscure link	Hover over links
http:// vs https:// link	

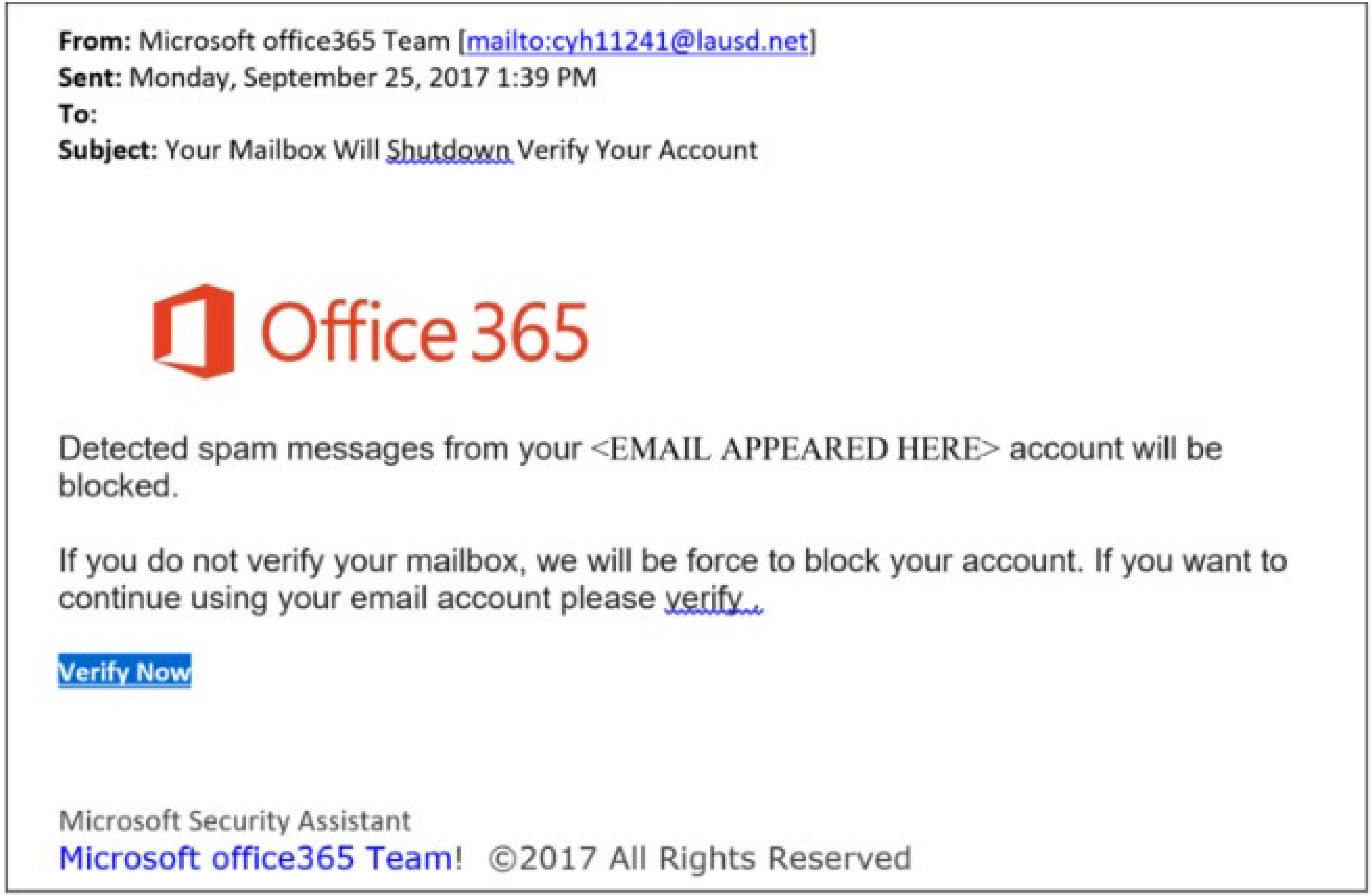
Phishing_

Three questions to ask when opening emails:

1. Do I know the sender?
2. What type of language are they using?
3. What are they asking me to do?

The red flags





From: Microsoft office365 Team [mailto:cyh11241@lausd.net]
Sent: Monday, September 25, 2017 1:39 PM
To:
Subject: Your Mailbox Will Shutdown Verify Your Account

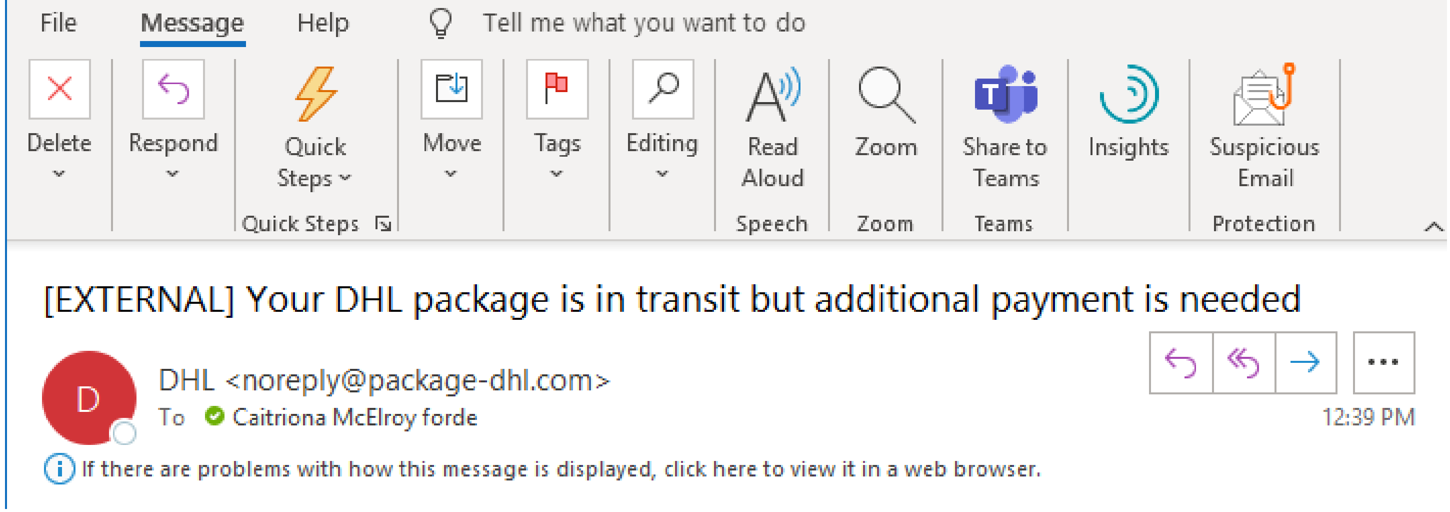
Office 365

Detected spam messages from your <EMAIL APPEARED HERE> account will be blocked.

If you do not verify your mailbox, we will be force to block your account. If you want to continue using your email account please verify .

Verify Now

Microsoft Security Assistant
Microsoft office365 Team! ©2017 All Rights Reserved

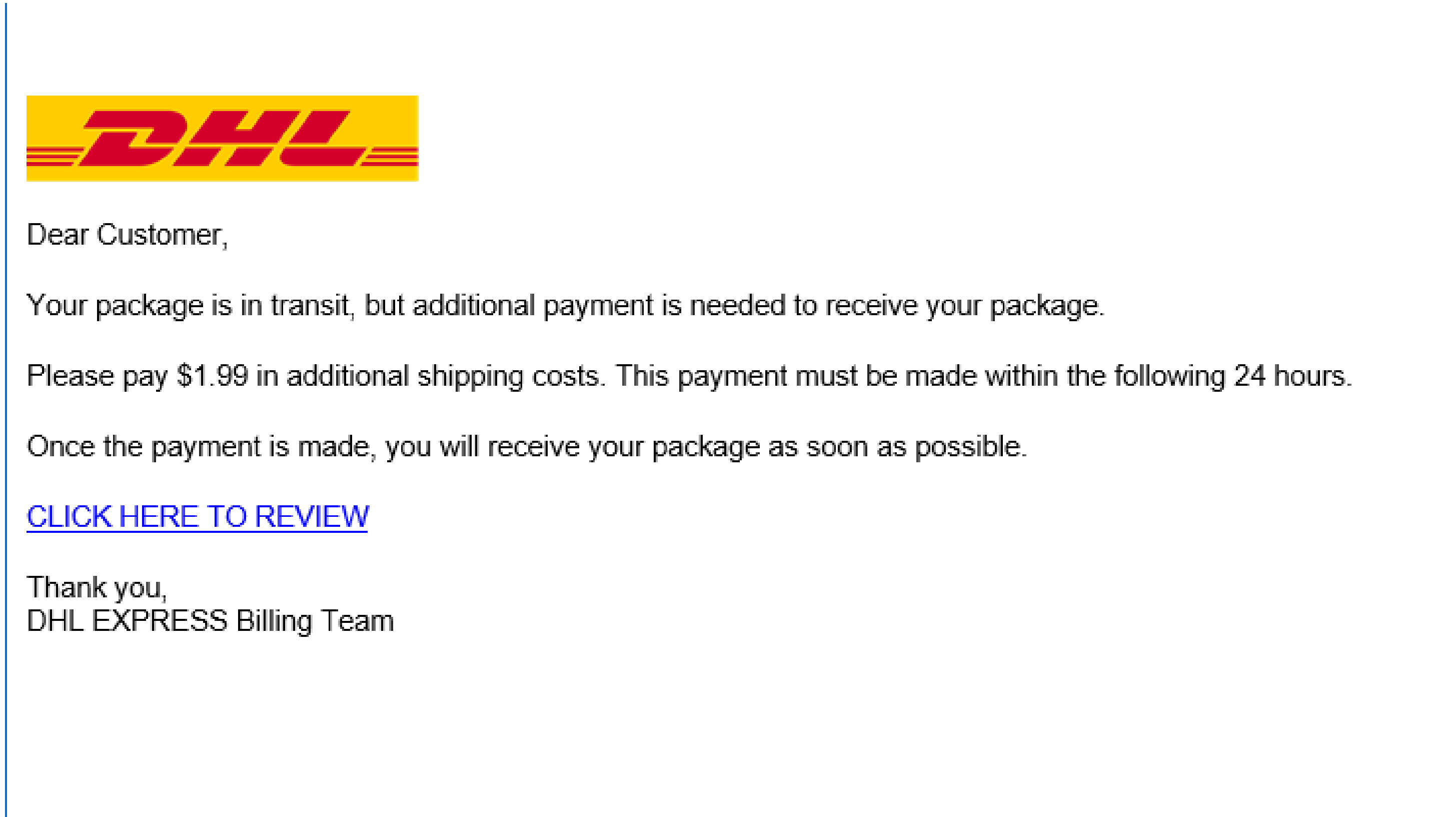


[EXTERNAL] Your DHL package is in transit but additional payment is needed

DHL <noreply@package-dhl.com>
To Caitriona McElroy forde

12:39 PM

If there are problems with how this message is displayed, click here to view it in a web browser.



Dear Customer,

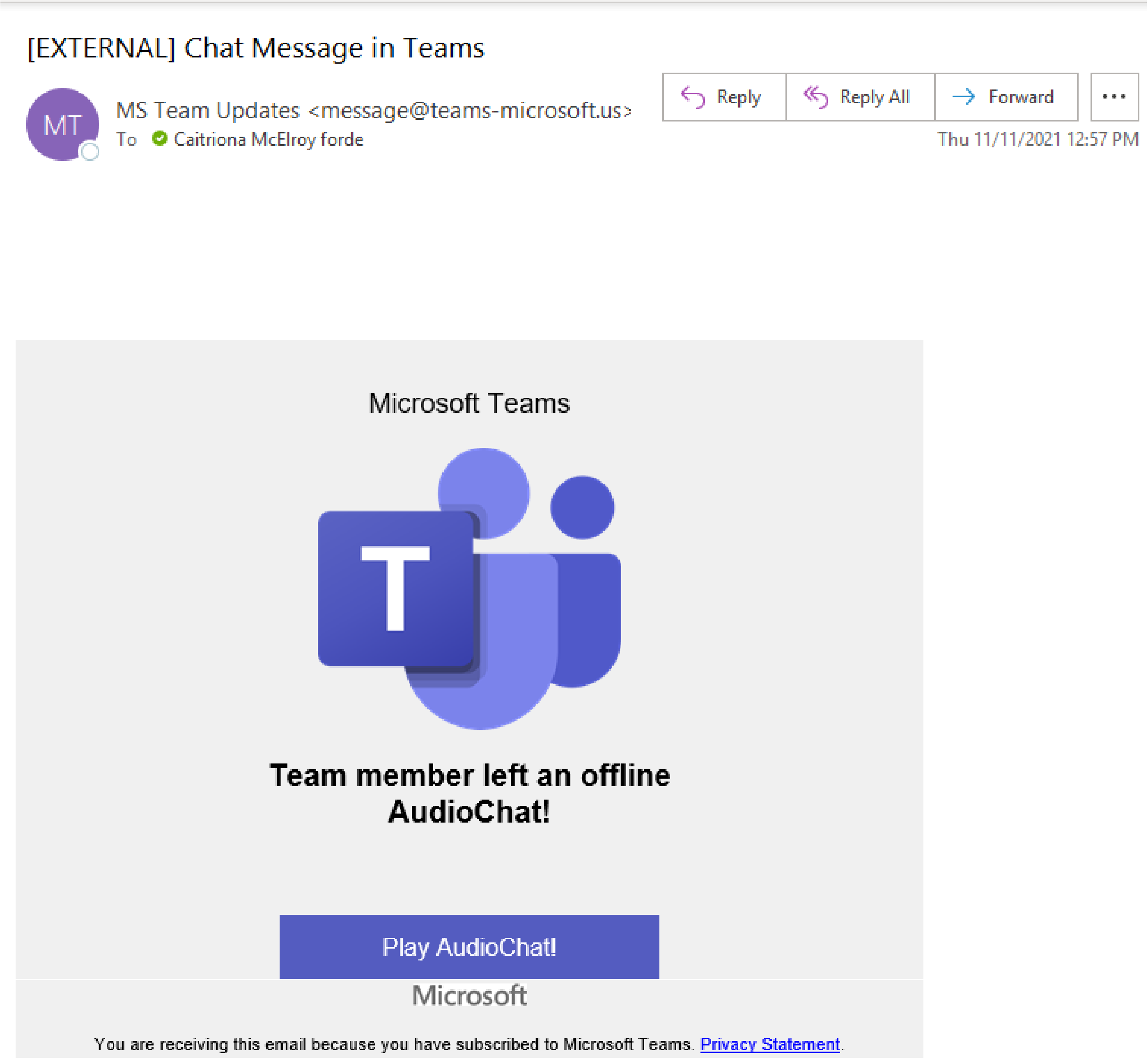
Your package is in transit, but additional payment is needed to receive your package.

Please pay $1.99 in additional shipping costs. This payment must be made within the following 24 hours.

Once the payment is made, you will receive your package as soon as possible.

CLICK HERE TO REVIEW

Thank you,
DHL EXPRESS Billing Team



[EXTERNAL] Chat Message in Teams

MS Team Updates <message@teams-microsoft.us>

To Caitriona McElroy forde

Thu 11/11/2021 12:57 PM

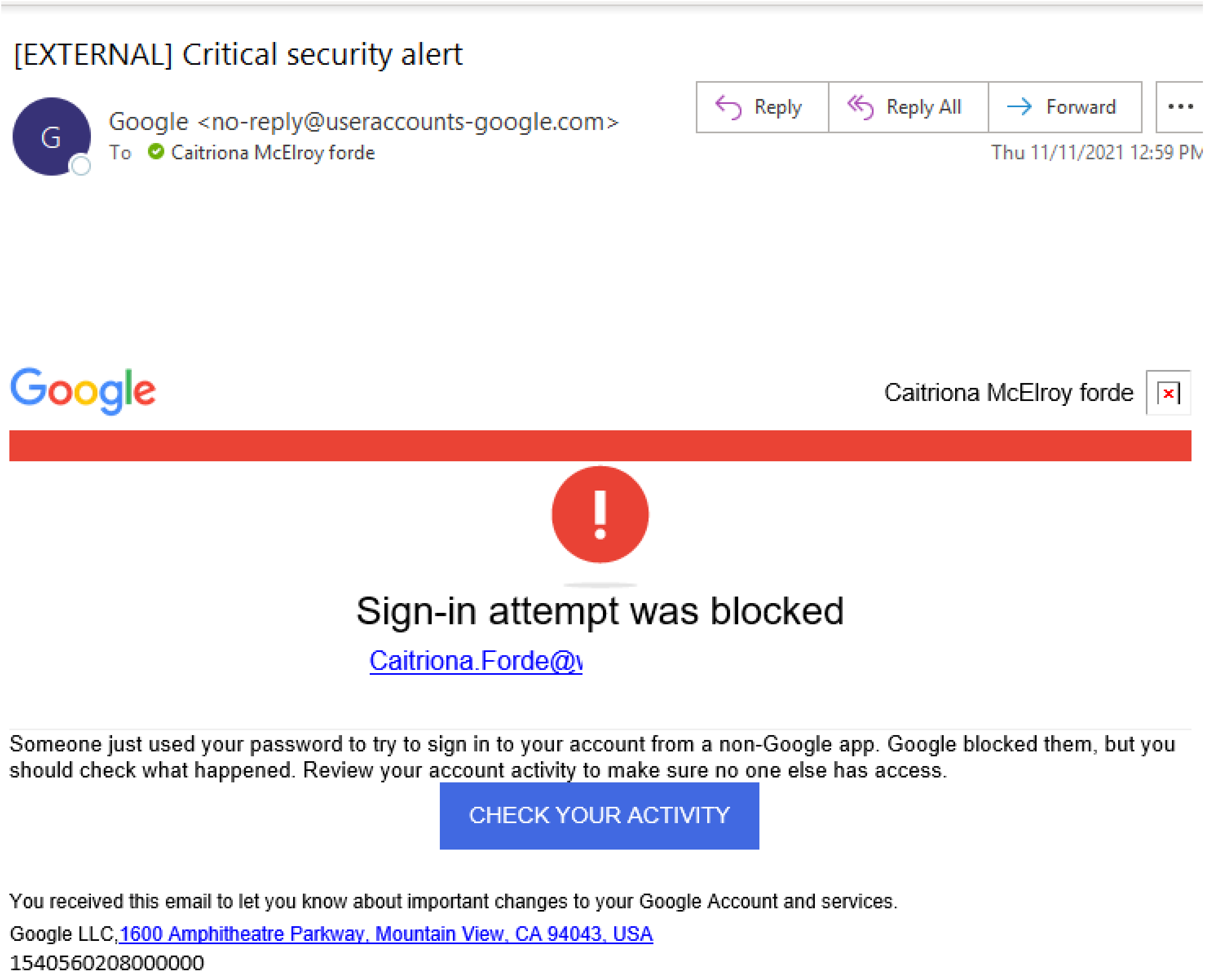
Microsoft Teams

Team member left an offline AudioChat!

Play AudioChat!

Microsoft

You are receiving this email because you have subscribed to Microsoft Teams. Privacy Statement.



[EXTERNAL] Critical security alert

Google <no-reply@useraccounts-google.com>
To Caitriona McElroy forde

Thu 11/11/2021 12:59 PM

Google

Caitriona McElroy forde

Sign-in attempt was blocked

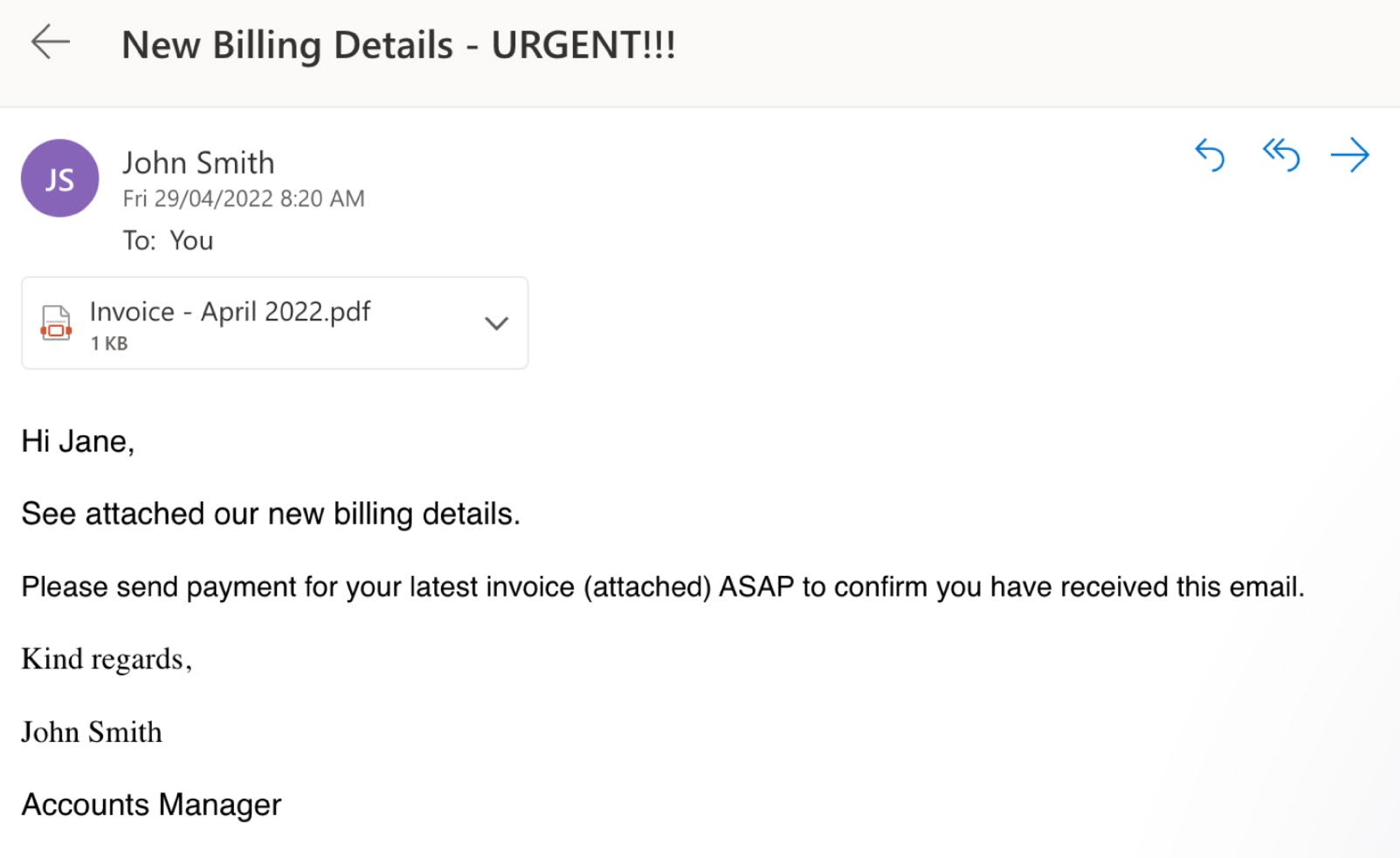
Caitriona.Forde@v

Someone just used your password to try to sign in to your account from a non-Google app. Google blocked them, but you should check what happened. Review your account activity to make sure no one else has access.

CHECK YOUR ACTIVITY

You received this email to let you know about important changes to your Google Account and services.

Google LLC,1600 Amphitheatre Parkway, Mountain View, CA 94043, USA
1540560208000000



New Billing Details - URGENT!!!

John Smith
Fri 29/04/2022 8:20 AM
To: You

Invoice - April 2022.pdf
1 KB

Hi Jane,

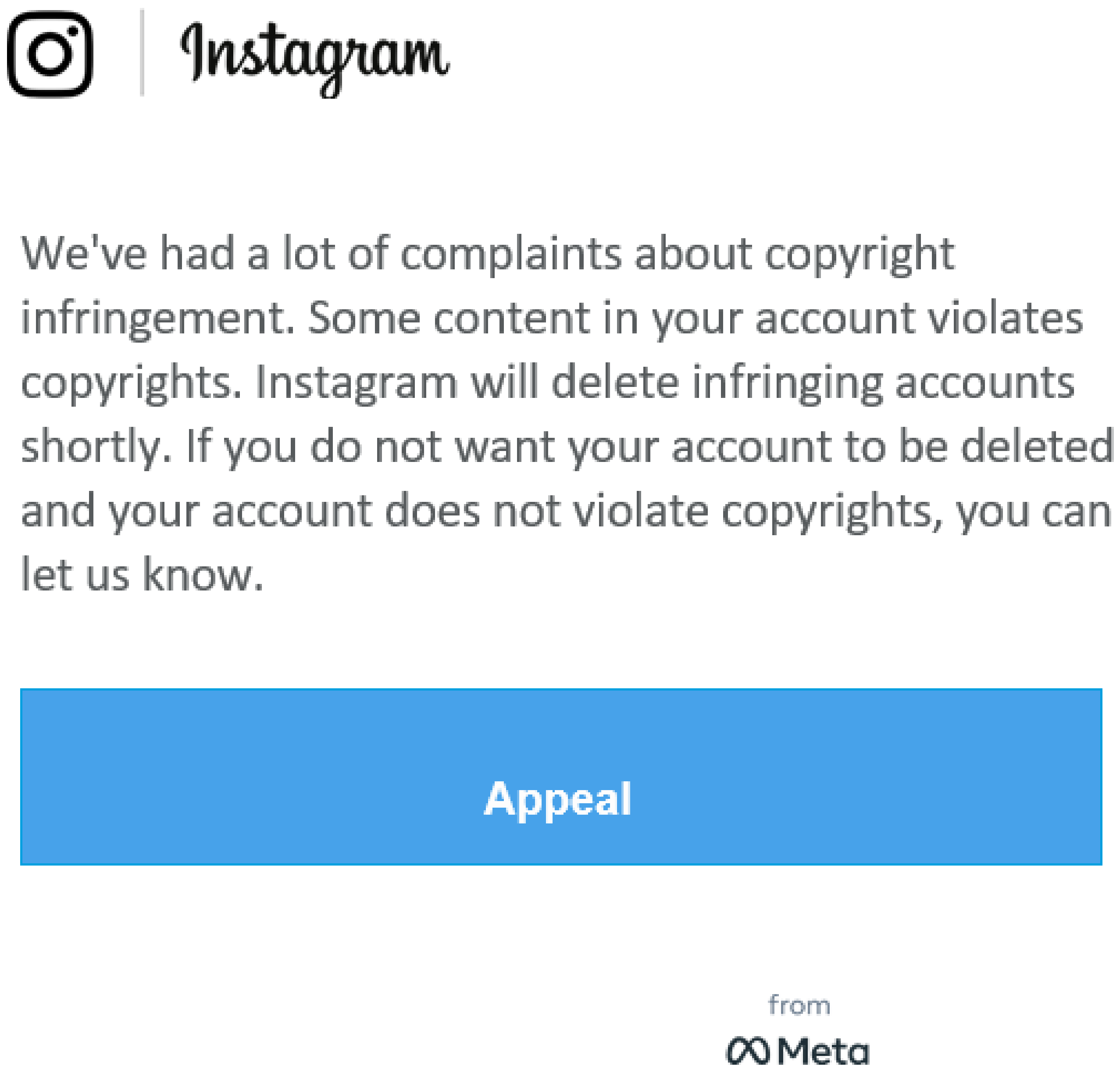
See attached our new billing details.

Please send payment for your latest invoice (attached) ASAP to confirm you have received this email.

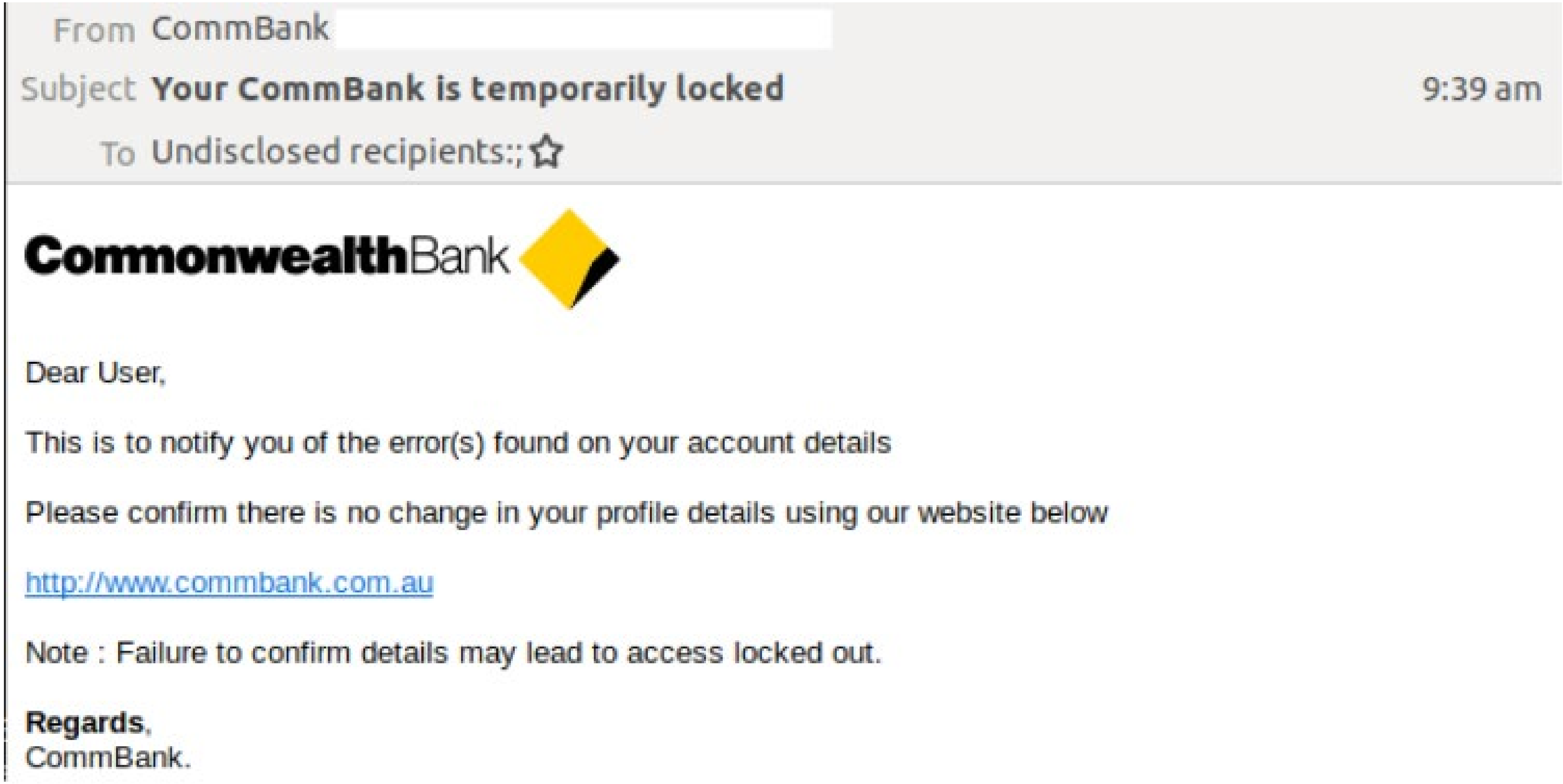
Kind regards,

John Smith

Accounts Manager



We've had a lot of complaints about copyright infringement. Some content in your account violates copyrights. Instagram will delete infringing accounts shortly. If you do not want your account to be deleted and your account does not violate copyrights, you can let us know.



From CommBank [redacted]

Subject **Your CommBank is temporarily locked** 9:39 am

To Undisclosed recipients:; ☆

CommonwealthBank

Dear User,

This is to notify you of the error(s) found on your account details

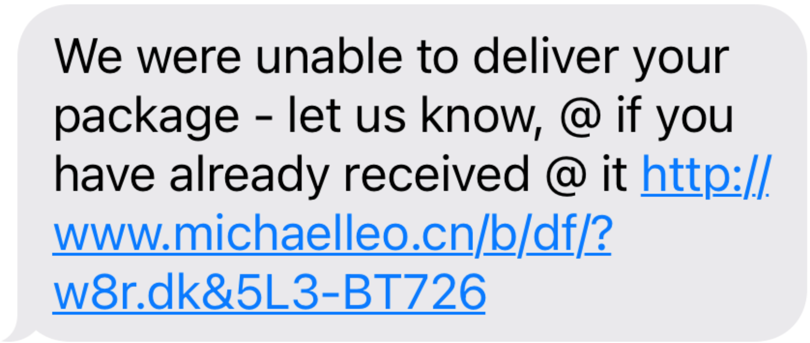
Please confirm there is no change in your profile details using our website below

http://www.commbank.com.au

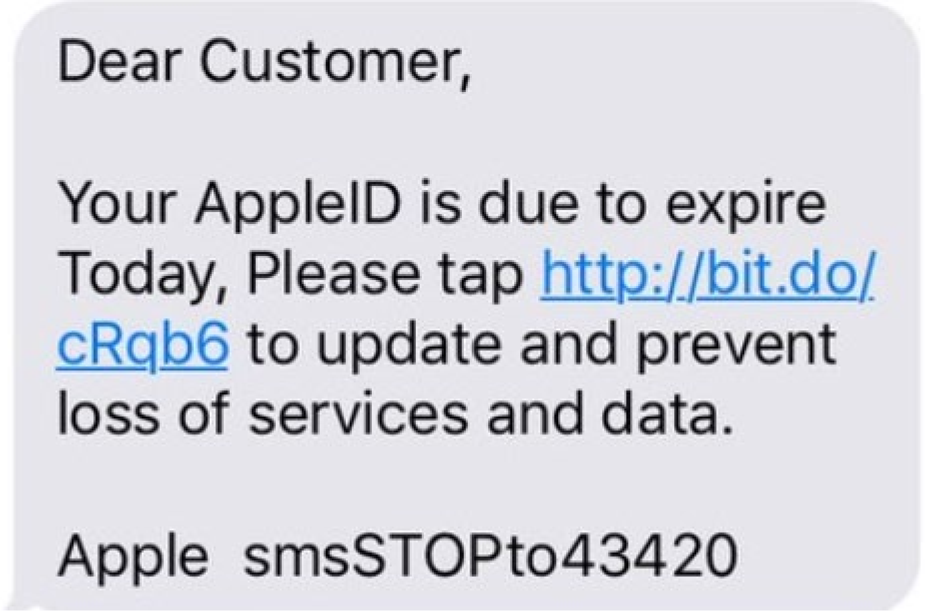
Note : Failure to confirm details may lead to access locked out.

Regards,
CommBank.

Smishing_



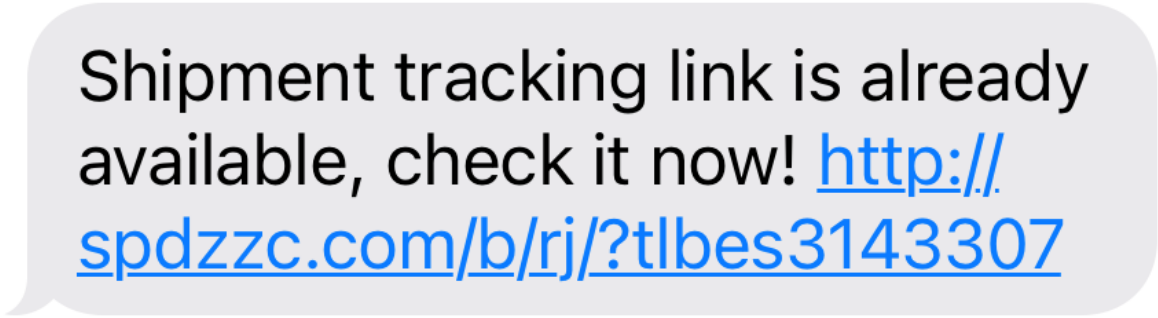
We were unable to deliver your package - let us know, @ if you have already received @ it http://www.michaelleo.cn/b/df/?w8r.dk&5L3-BT726



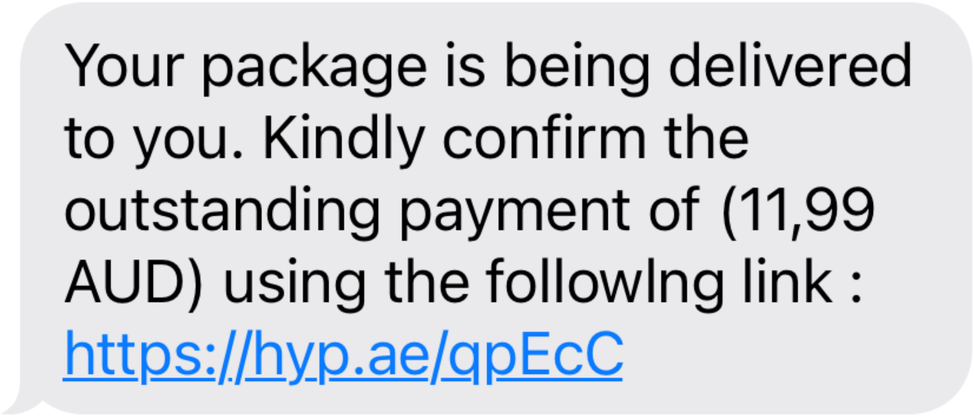
Dear Customer,

Your AppleID is due to expire Today, Please tap http://bit.do/cRqb6 to update and prevent loss of services and data.

Apple smsSTOPto43420



Shipment tracking link is already available, check it now! http://spdzzc.com/b/rj/?tlbes3143307



Your package is being delivered to you. Kindly confirm the outstanding payment of (11,99 AUD) using the followlng link : https://hyp.ae/qpEcC

Data Breaches

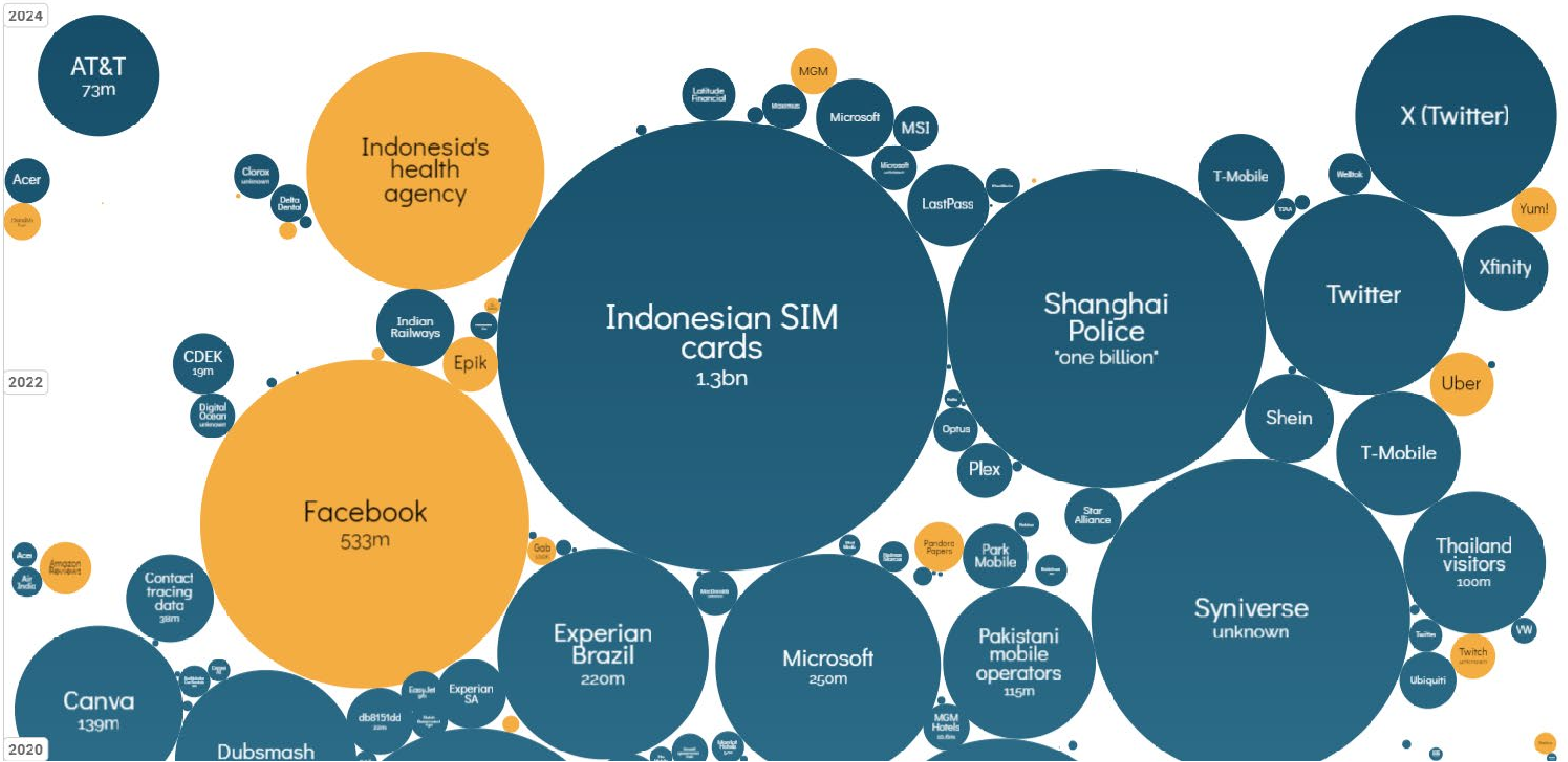
World's Biggest Data Breaches & Hacks

interesting story

Selected events over 30,000 records stolen

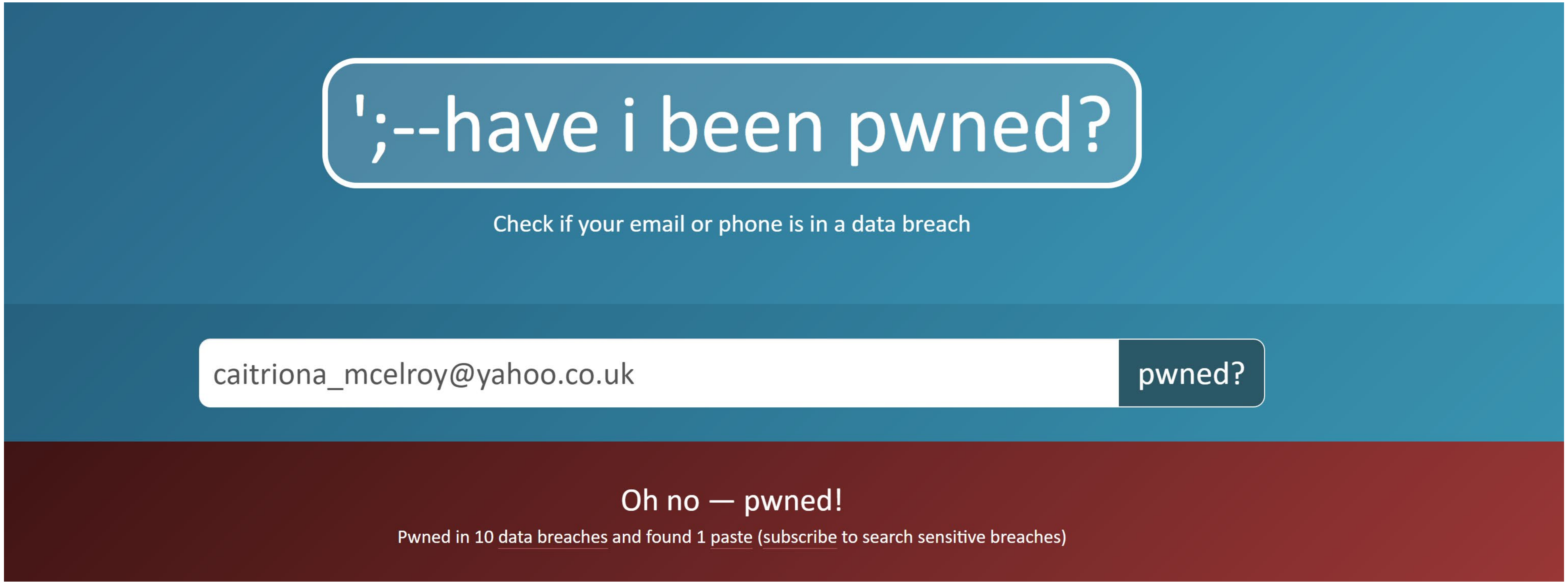
UPDATED: Jan 2024

size: records lost   filter   search...



Protecting yourself_

Have you become a victim?



Check if your email or phone is in a data breach

caitriona_mcelroy@yahoo.co.uk

Oh no — pwned!

Pwned in 10 data breaches and found 1 paste (subscribe to search sensitive breaches)

https://haveibeenpwned.com

Passwords V's Passphrase

Monday2020?
Password2021!
W3sternAus?21
W3lcome2020#

I love Pizza for lunch

I don't like pineapple
on my pizza

Bus no211 is the best

Why length V's Complexity?

Password/Passphrase	Brute Force Attack	Dictionary Attack
password123	Instantly	Instantly
Spaghetti95!	48 hrs	30 mins
5paghetti95!	24 hrs	1 hrs
A&d8j+1	2.5 hrs	2.5 hrs
I don't like pineapple on my pizza	1 Year	40 days

The top 10 most common passwords:

1.123456111111

2.123123

3.12345

4.1234567890

5.qwerty

6.123456789

7.picture1

8.password

9.12345678

10.senha

A password is like a toothbrush
Choose a good one
Don't share it with anyone
Change it occasionally

Password Management

[illegible] lives, we

Look familiar?

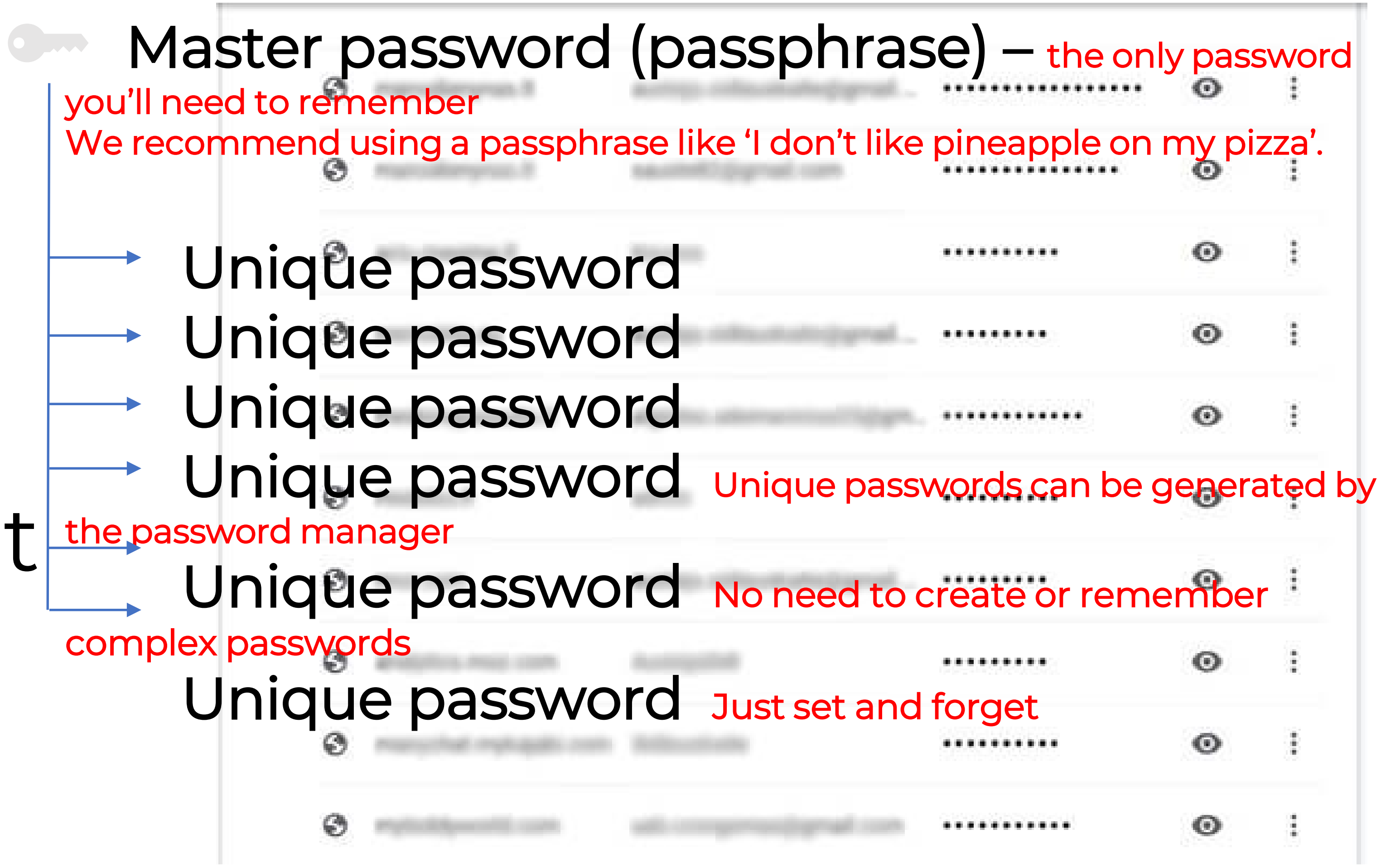
[illegible]

browser, it may

[illegible], it

[illegible] your computer

[illegible] can access all your saved passwords.



Master password (passphrase) – the only password you'll need to remember

We recommend using a passphrase like 'I don't like pineapple on my pizza'.

Unique password

Unique password

Unique password

Unique password

Unique passwords can be generated by the password manager

Unique password

No need to create or remember complex passwords

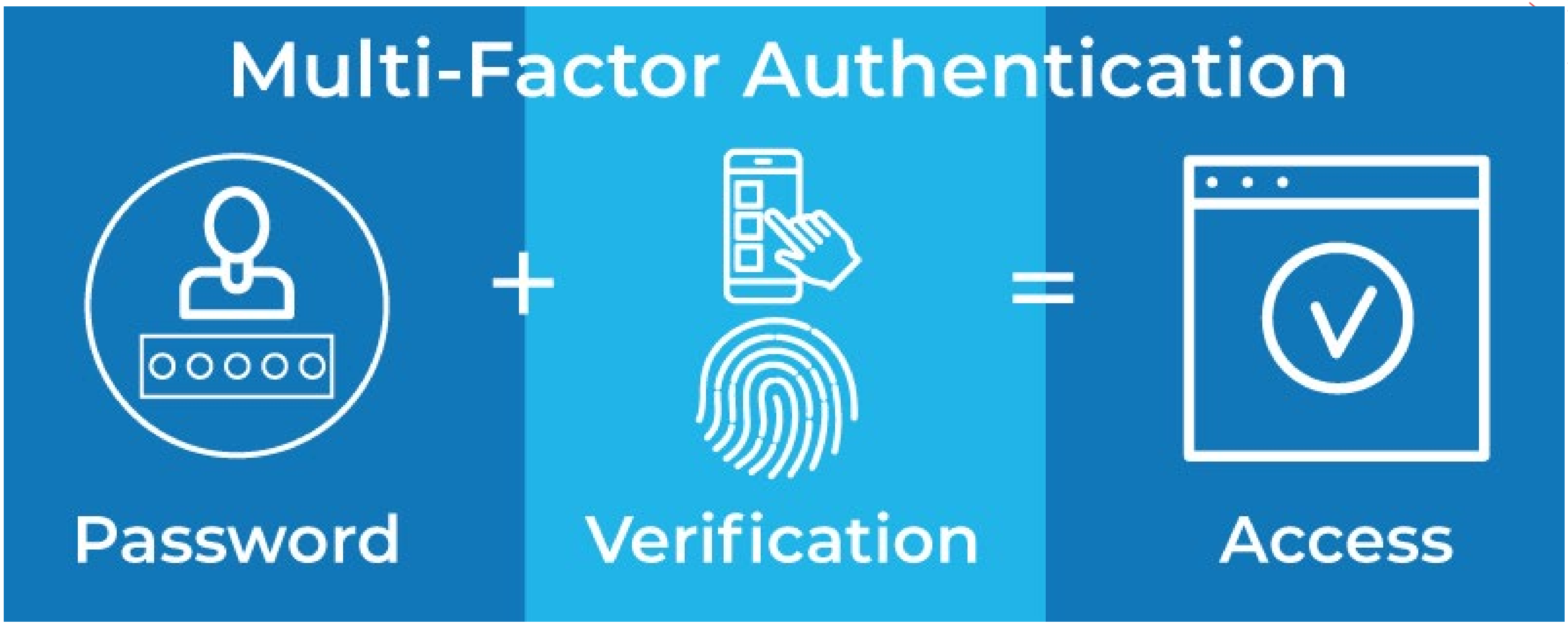
Unique password

Just set and forget

“Multi-Factor Authentication Can Prevent 90% of Attacks”

https://www.infosecurity-magazine.com/news/tech-execs-mfa-prevent-90-of/

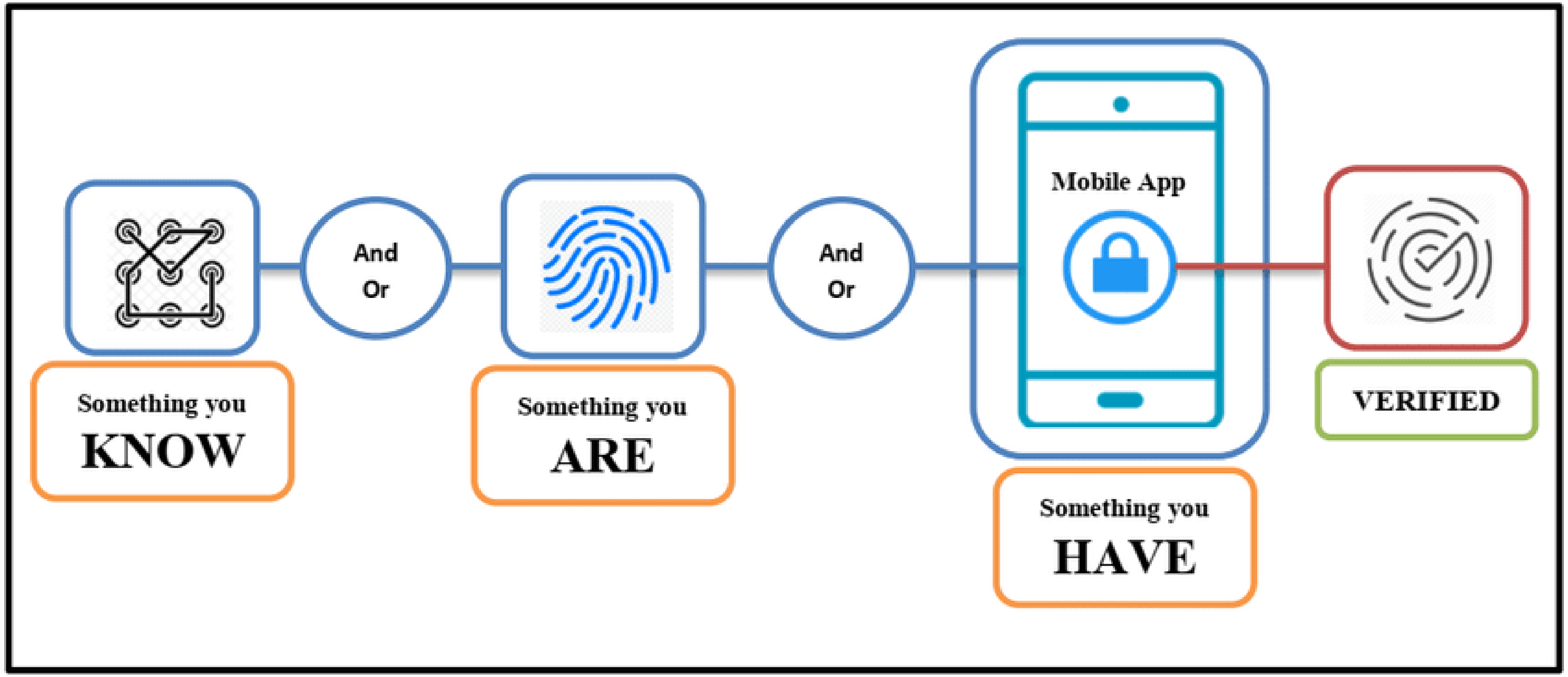
Multi-factor Authentication_



https://edafio.com/blog/why-multi-factor-authentication-mfa-is-a-must/

Multi-factor Authentication_

Multi-factor means using a combination of the following:



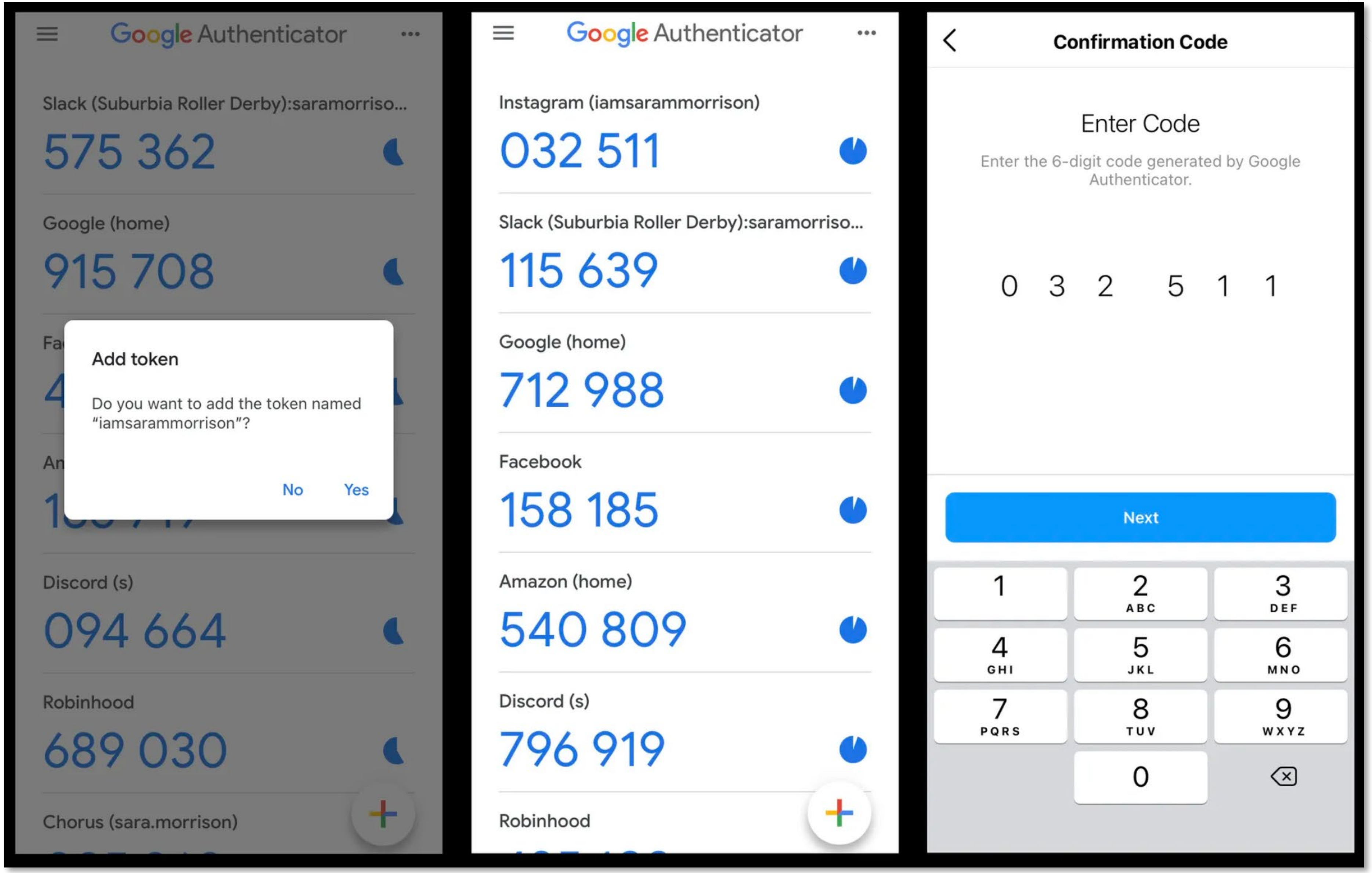
https://www.researchgate.net/figure/Multi-factor-authentication_fig2_335709093

Multi-factor Authentication_

Set it up for:

- Social media accounts
- Online banking
- Email accounts & mailboxes– Office 365
- Online databases
- Accounting Software
- CRM/Customer Database
- Domain name and hosting accounts
- Any online platform you save data

Multi-factor Authentication_



Google Authenticator

Slack (Suburbia Roller Derby):saramorriso...

575 362

Google (home)

915 708

Fa

Add token

Do you want to add the token named “iamsarammorrison”?

No Yes

An

Discord (s)

094 664

Robinhood

689 030

Chorus (sara.morrison)

Google Authenticator

Instagram (iamsarammorrison)

032 511

Slack (Suburbia Roller Derby):saramorriso...

115 639

Google (home)

712 988

Facebook

158 185

Amazon (home)

540 809

Discord (s)

796 919

Robinhood

Confirmation Code

Enter Code

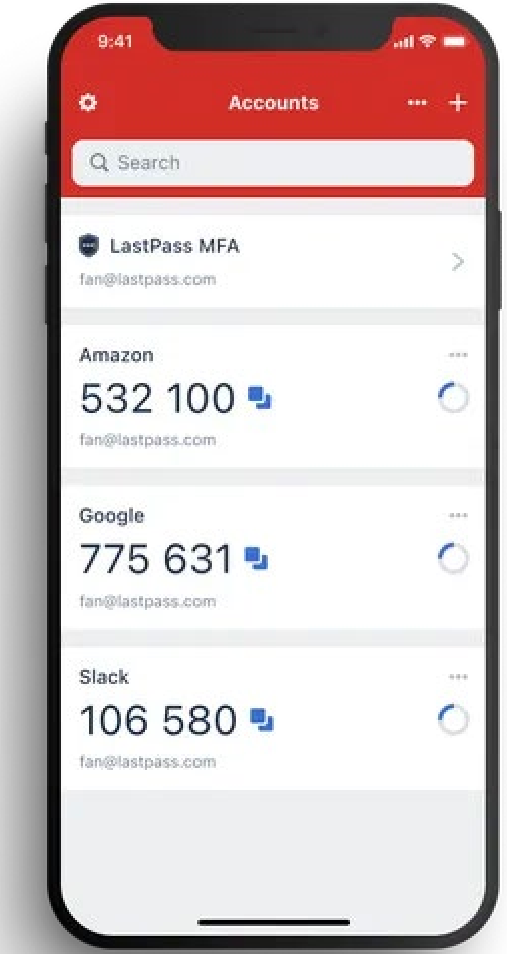
Enter the 6-digit code generated by Google Authenticator.

0 3 2 5 1 1

Next

https://www.vox.com/recode/22419794/authenticator-apps-and-you-authy-google-authenticator

Multi-factor Authentication_



9:41

Accounts

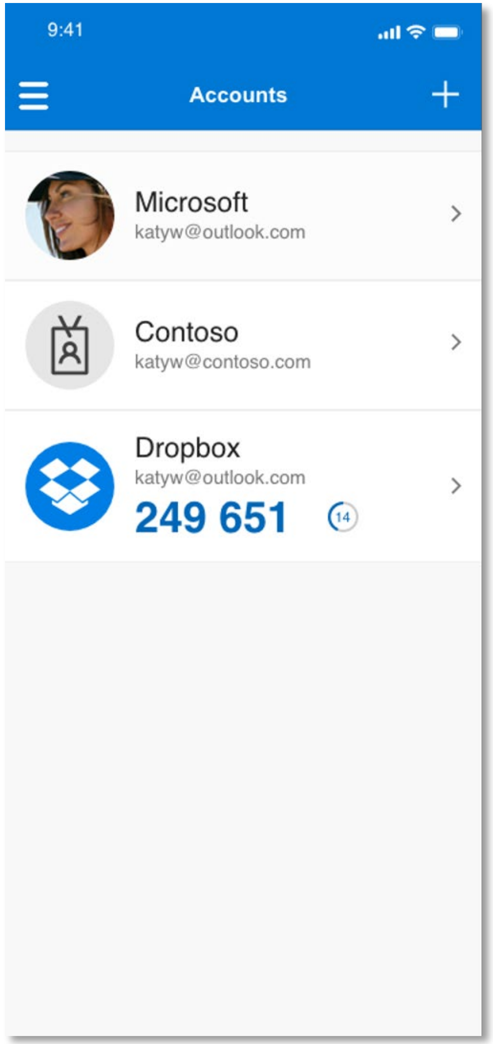
Search

LastPass MFA
fan@lastpass.com

Amazon
532 100
fan@lastpass.com

Google
775 631
fan@lastpass.com

Slack
106 580
fan@lastpass.com



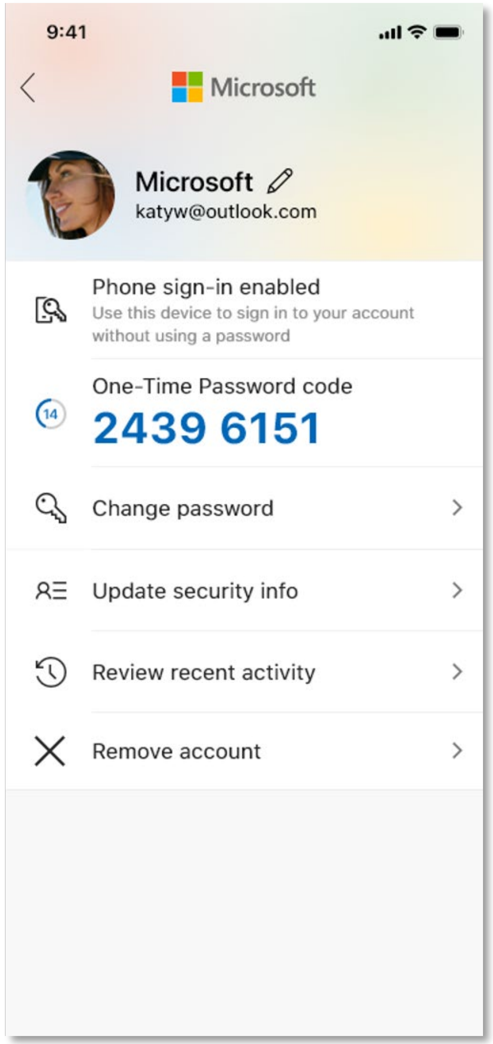
9:41

Accounts

Microsoft
katyw@outlook.com

Contoso
katyw@contoso.com

Dropbox
katyw@outlook.com
249 651 14



9:41

Microsoft

Microsoft
katyw@outlook.com

Phone sign-in enabled
Use this device to sign in to your account without using a password

One-Time Password code
14 2439 6151

Change password

Update security info

Review recent activity

Remove account

Case Studies

Case Study 1
LinkedIn

- Social Engineering – Convincing email pretending to be from event organisers
- Phishing – Email with link to click
- Ransomware

Case Study 2
Real Estate Company

- Phishing – Email for credential harvesting (Microsoft 365)
- Social Engineering – Convincing the buyer they were speaking with the sales agent
- Business Email Compromise – Targeting companies who deal with large financial transactions and trust accounts

Case Study 3
Not for Profit

- Business Email Compromise – CEO mailbox compromised while overseas.
- Sent email from CEO to finance team to pay urgent invoice of $25K

Actions to take _

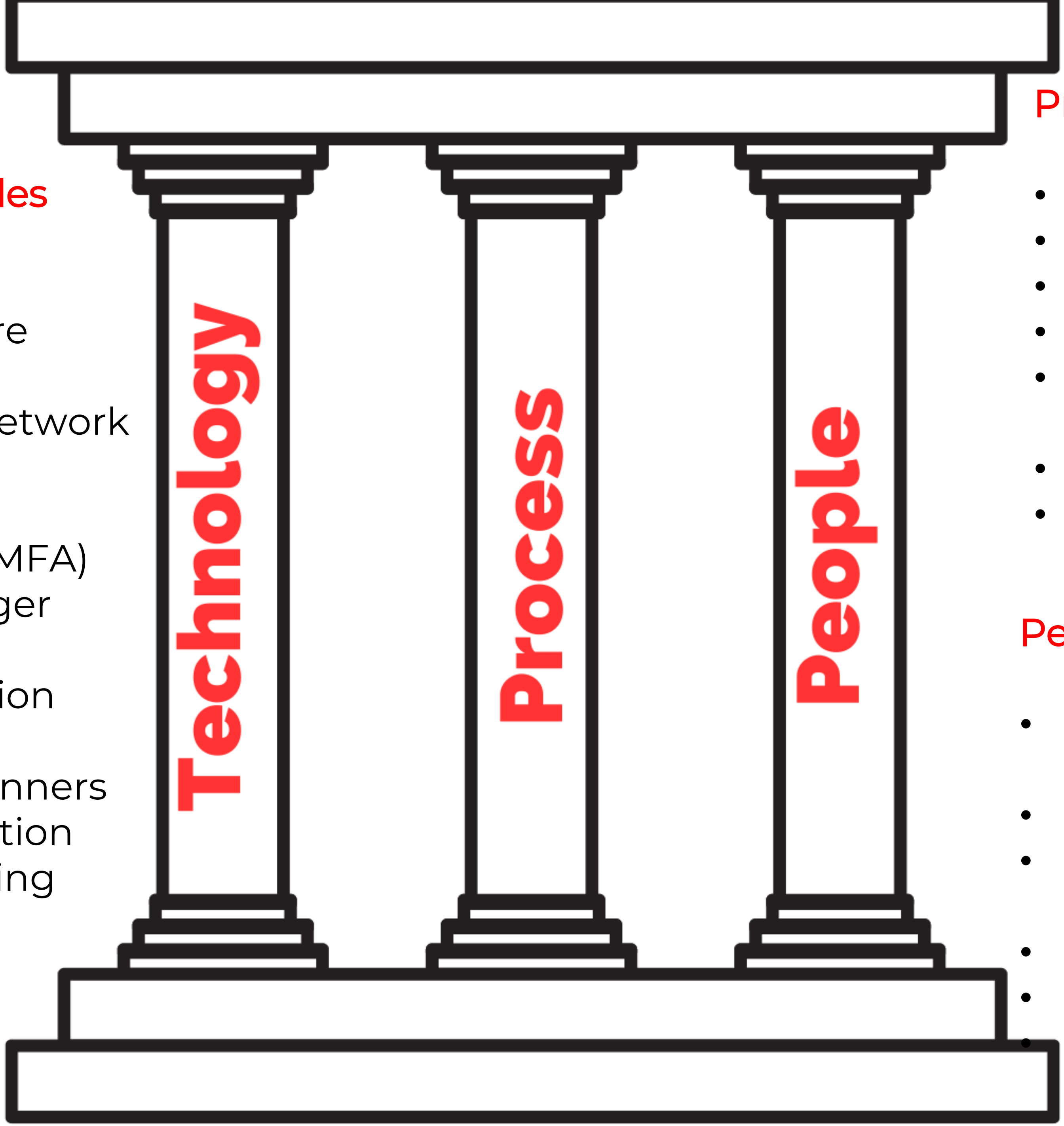
- Turn off your computer and disconnect from Internet/Network
- Get professional help
- Change all passwords
- Inform bank
- Run virus scans
- Inform authorities

Main takeaways…

- Don't click links or open attachments in emails that look suspicious
- Password hygiene is essential – Implement a password manager
- Multi-factor Authentication on everything
- **Backup your important data (Crown Jewels)**
- Regular software updates on all devices
- **Train your team**

Technology examples

- Firewall
- Antivirus software
- Spam Filter
- Virtual Private Network (VPN)
- Multi-factor authentication (MFA)
- Password Manager
- Encryption
- Intrusion Detection System (IDS)
- Vulnerability scanners
- Endpoint Protection
- Penetration testing



Process examples

- Finance & HR
- Incident response plan
- Access control
- Security risk assessment
- Security policy and procedu documentation
- Change management proc
- Business continuity and disaster recovery plan

People examples

- Regular training and awareness sessions
- Background checks
- Limit access to sensitive information
- Use secure collaboration too
- Monitor user activity
- Create a security culture

Leaving thought…

1 in 55

*Odd's of you having a car accident

1 in 4

*Odd's of a cyber attack

https://www.varonis.com/blog/likelihood-of-a-cyber-attack