Cyber Security – Is it time to panic?

Lili Zhang - Business Information Security Officer, Department of Customer Service

Jatinder Bal - Manager Security Awareness, Department of Customer Service

Cyber Awareness
2025 COAT Conference
November 2025

Agenda

Section 1 – Why it's important

Cyber Security Basics

Cyber Threat & Incidents

Victimology

The Cyber Security Logic

What can we do

Section 2 – Basic Cyber Hygiene

Strong Password

Multifactor Authentication

Identification of Phishing

Combat business email compromise

AI use

Section 3 – Where to get help and Q&As

Resources

Q&As

1

Why Cyber Security Is Important

What is Cybersecurity?

DEFINITION

Cybersecurity is the practice of protecting systems, networks, and data from cyber threats.

WHY IT MATTERS

- Prevents data breaches
- Protects privacy
- Prevents financial and reputational damage
- Builds trust

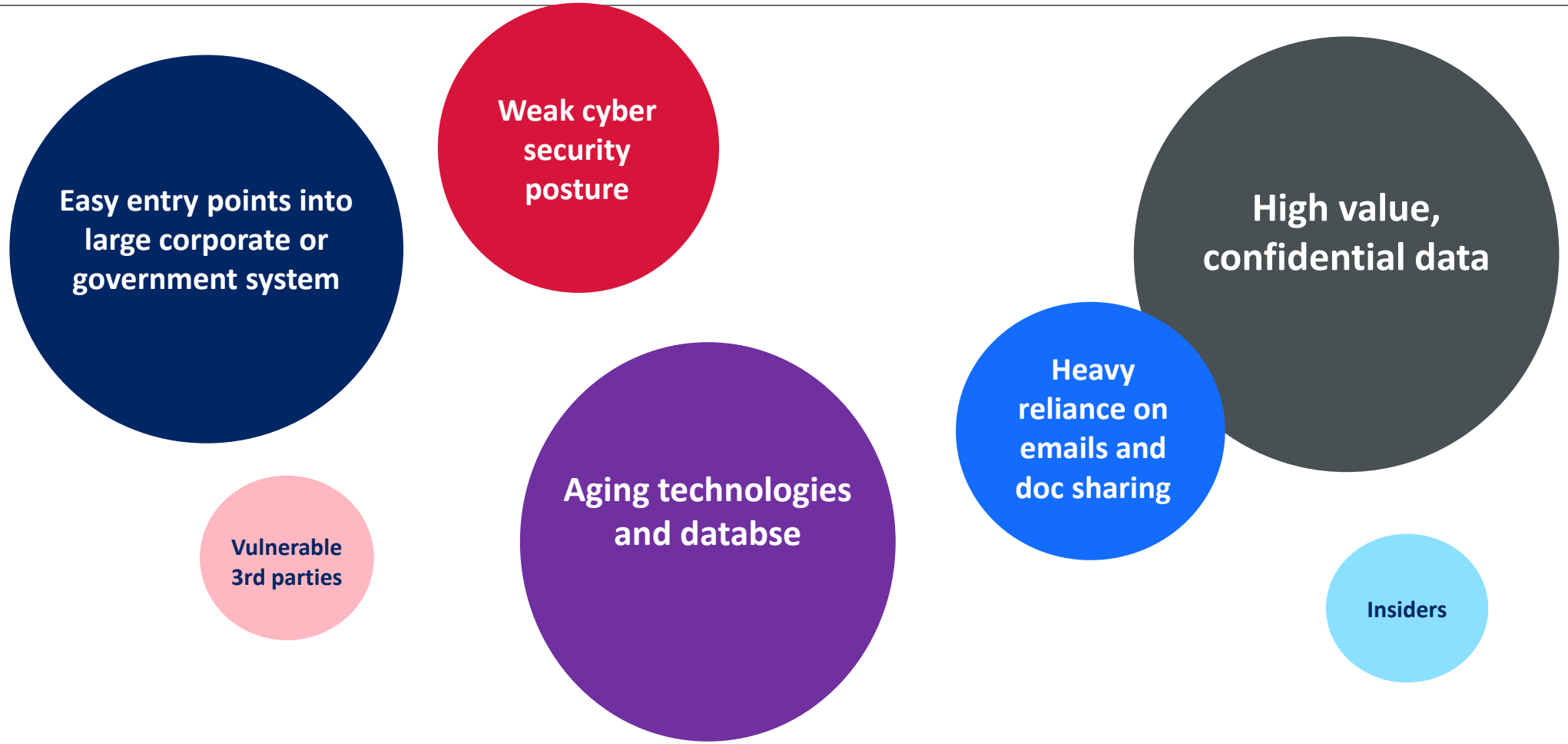
KEY COMPONENTS

Confidentiality – Keeping data private
Integrity – Ensuring data accuracy
Availability – Systems accessible when needed

COMMON THREATS

- Phishing
- Malware
- Business email compromise
- Social engineering

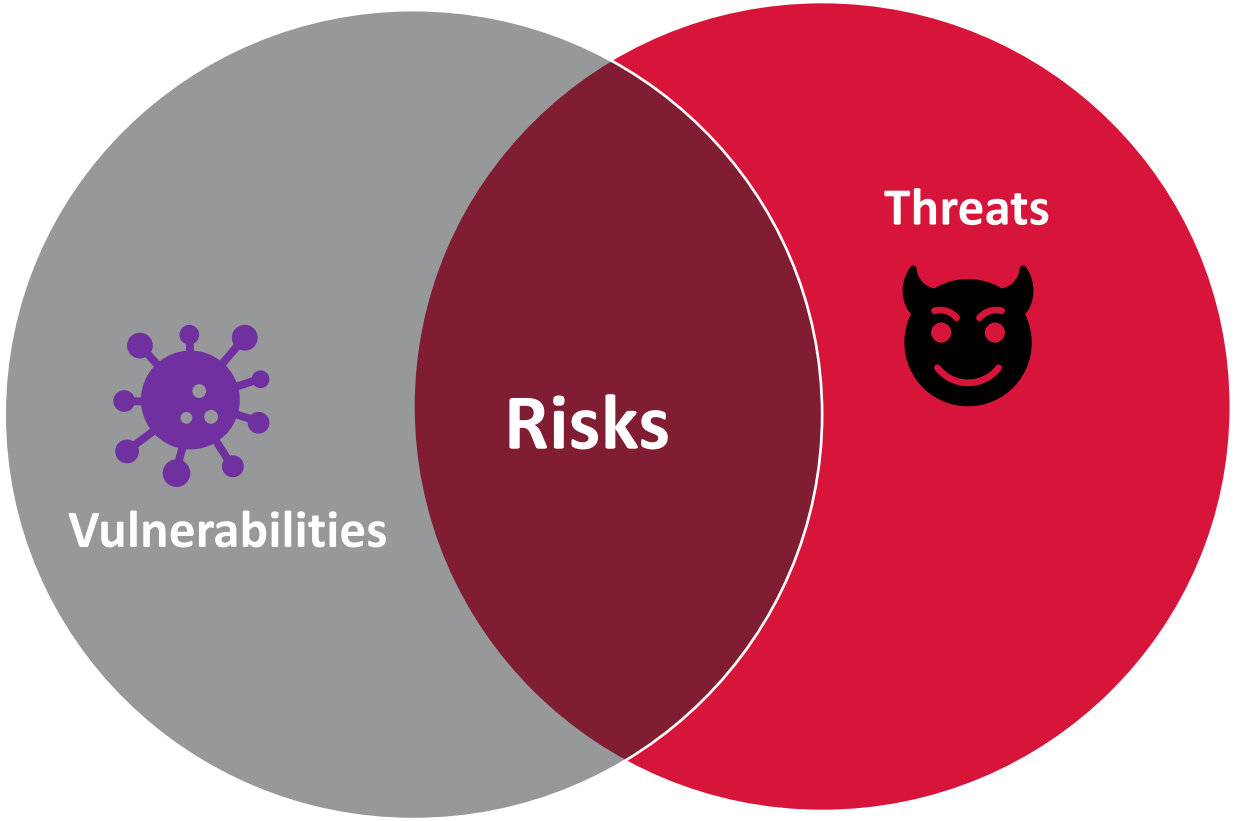
Why is the justice and legal industry an attractive target?



The Logic of Cyber Security

Weak spots that make you susceptible to attack. E.g.

- Weak passwords,
- Unpatched systems,
- Oversharing on social
- No data backup



External forces that can exploit weakness. E.g.

- Phishing,
- Ransomware,
- Data theft,
- Business email compromise
- Hacking attempts

What can you do?

UNDERSTAND YOUR ASSETS

KNOW YOUR SYSTEMS AND THIRD PARTIES

PRACTICE CYBER HYGIENE AND RISK ASSESSMENTS

2

Cyber Hygiene

Afternoon Brain Teaser

Can you remember these 4 words?

‘Tis the Season…to be cyber-aware!

~~Is it time to panic?~~

No, it’s time to prepare!

Spoiler Alert!

It all starts with Intel

It all starts with Intel

Attackers look for easy targets

- Don’t be the least secure house on the street

What can attackers see about you?

Make it difficult to find information about you:

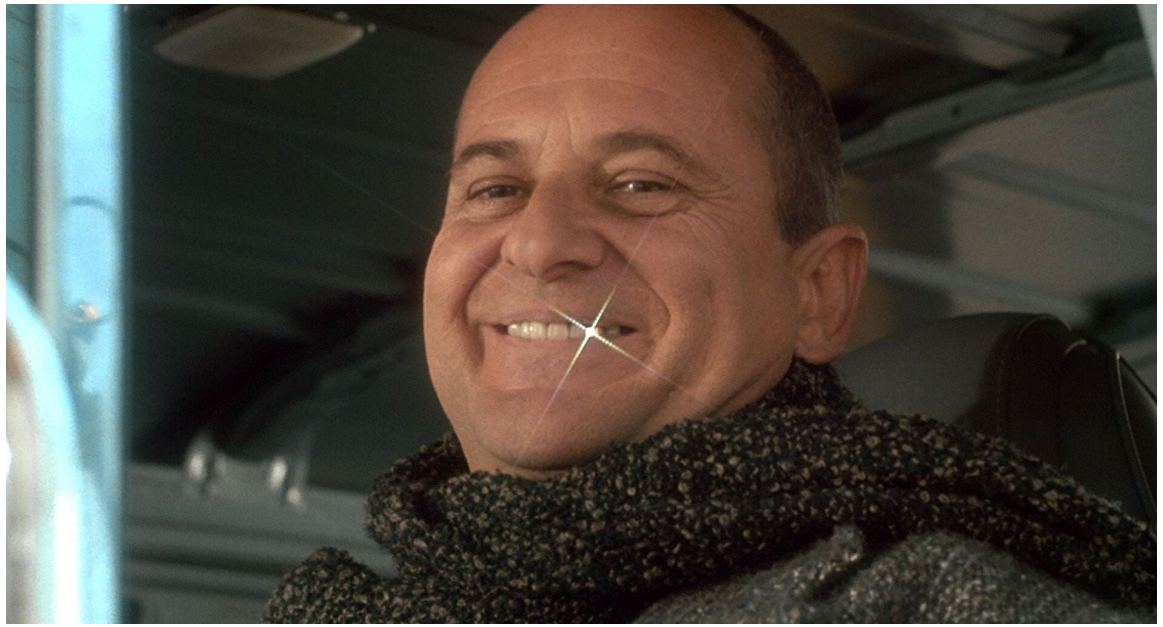
- Perform a ‘vanity search’
- Lock down your social media profiles
- Review your connections
- Consider reducing your digital footprint

Social Engineering

"The practice of manipulating people into revealing confidential information or performing actions that compromise security"

- Phishing Emails
- Smishing/Vishing (mobiles)
- Quishing (QR Codes)
- Tailgating (Physical security)

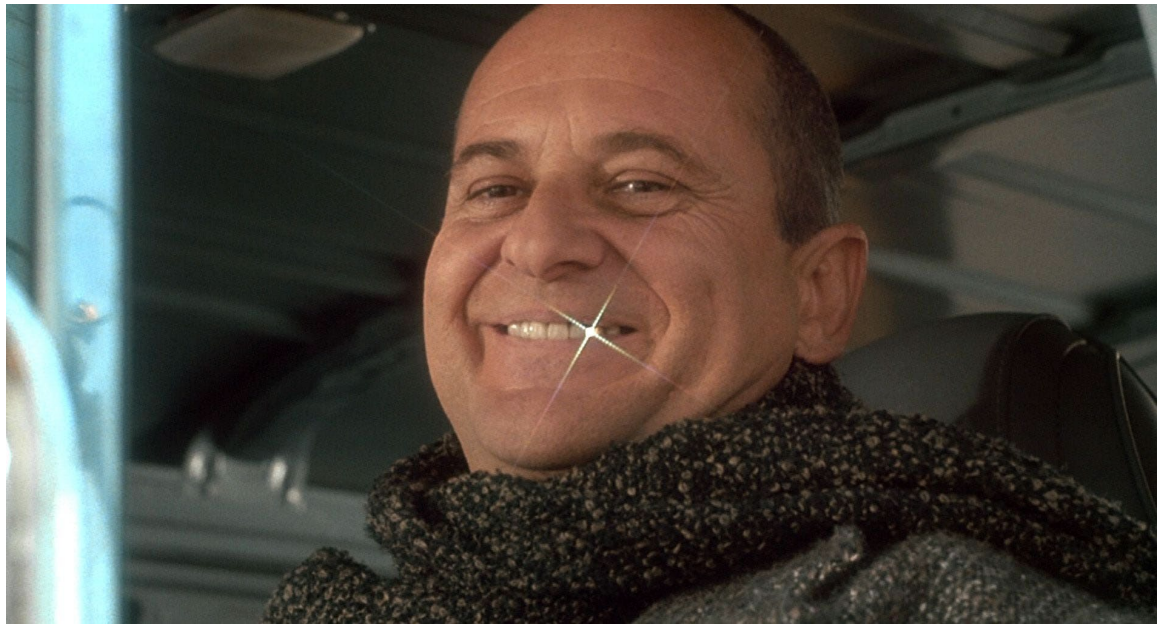
How to spot a phish



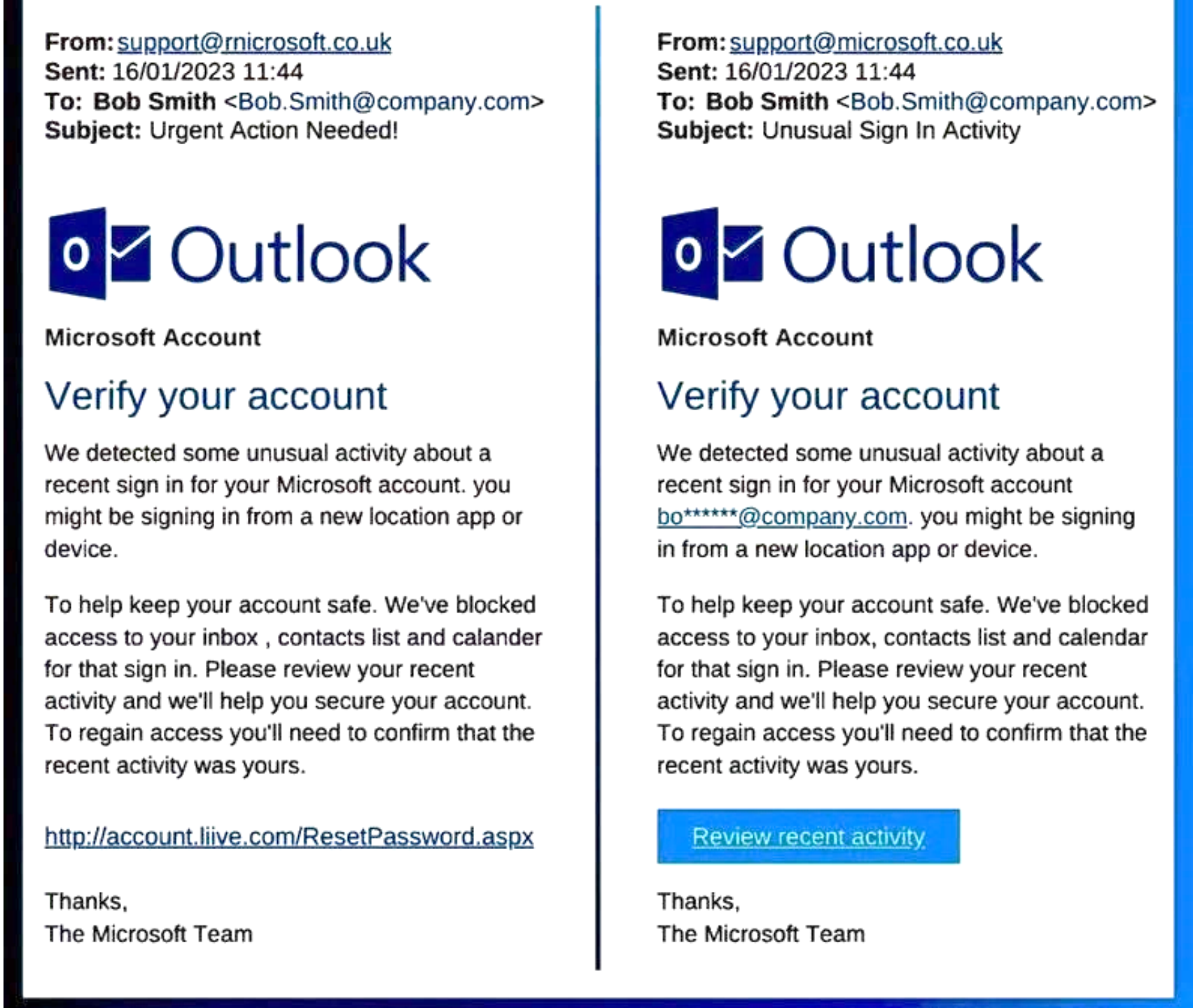
How to spot a phish

Look out for these red flags:

- Sender Email Address
- Suspicious Links
- Sense of Urgency
- Grammatical Mistakes



Can you spot the difference?



From: support@rnicrosoft.co.uk
Sent: 16/01/2023 11:44
To: **Bob Smith** <Bob.Smith@company.com>
Subject: Urgent Action Needed!

Outlook

Microsoft Account

Verify your account

We detected some unusual activity about a recent sign in for your Microsoft account. you might be signing in from a new location app or device.

To help keep your account safe. We've blocked access to your inbox , contacts list and calander for that sign in. Please review your recent activity and we'll help you secure your account. To regain access you'll need to confirm that the recent activity was yours.

http://account.liive.com/ResetPassword.aspx

Thanks,
The Microsoft Team

From: support@microsoft.co.uk
Sent: 16/01/2023 11:44
To: **Bob Smith** <Bob.Smith@company.com>
Subject: Unusual Sign In Activity

Outlook

Microsoft Account

Verify your account

We detected some unusual activity about a recent sign in for your Microsoft account bo******@company.com. you might be signing in from a new location app or device.

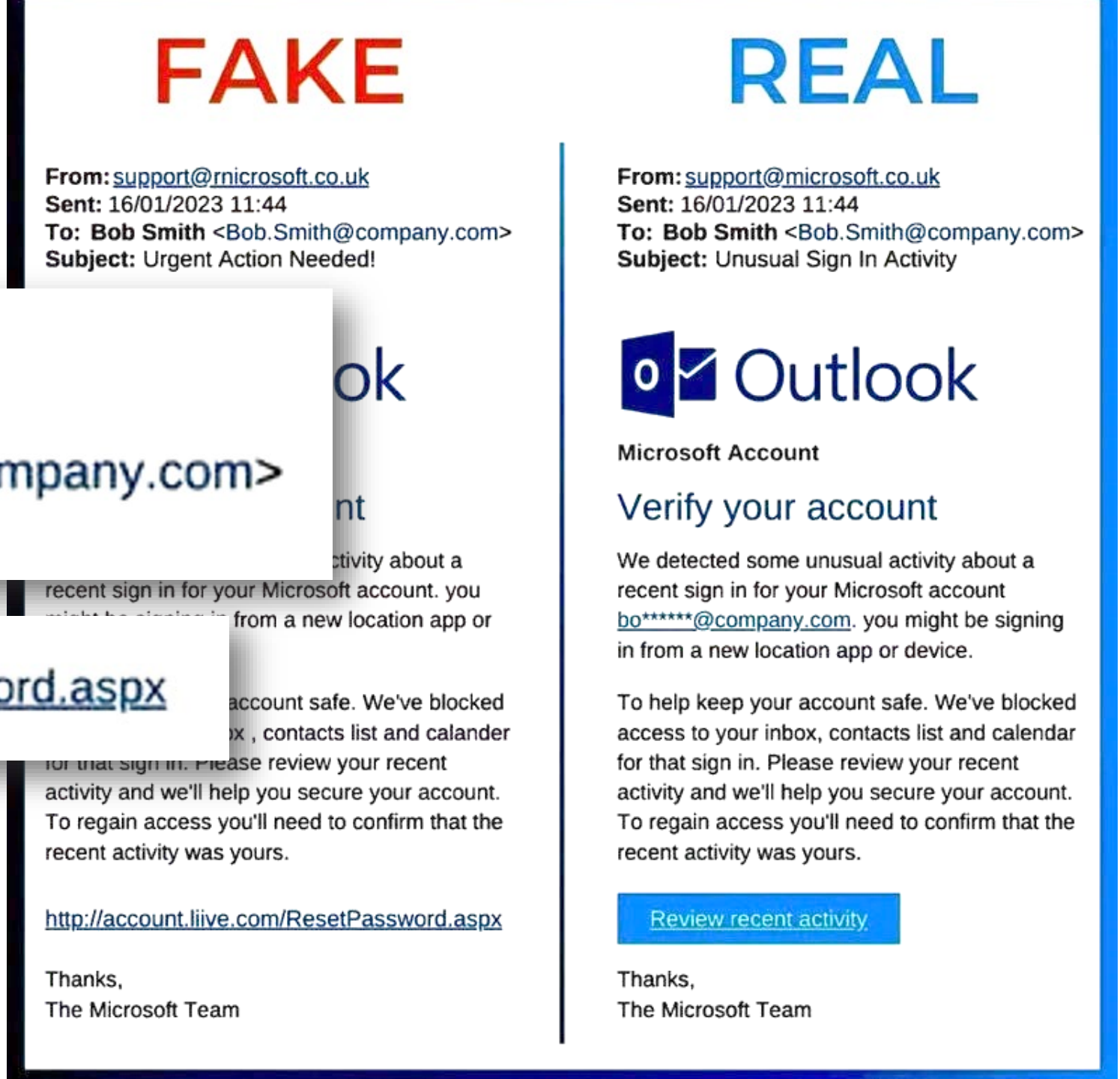
To help keep your account safe. We've blocked access to your inbox, contacts list and calendar for that sign in. Please review your recent activity and we'll help you secure your account. To regain access you'll need to confirm that the recent activity was yours.

Review recent activity

Thanks,
The Microsoft Team

From: support@rnicrosoft.co.uk
Sent: 16/01/2023 11:44
To: **Bob Smith** <Bob.Smith@company.com>
Subject: Urgent Action Needed!

http://account.liive.com/ResetPassword.aspx



Scenario 1: **Phishing**

From: Evan Carr <evan.carr@servicenswgov.com>
To: Ally Lange <ally.Lange@service.nsw.gov.au>
Subject: Re: Proposed Proposal Document
Attachment: proposal.pdf.exe 253 KB

Email is not legitimate NSW Government address

Generic subject line

Attachment has a generic title and misleading file type

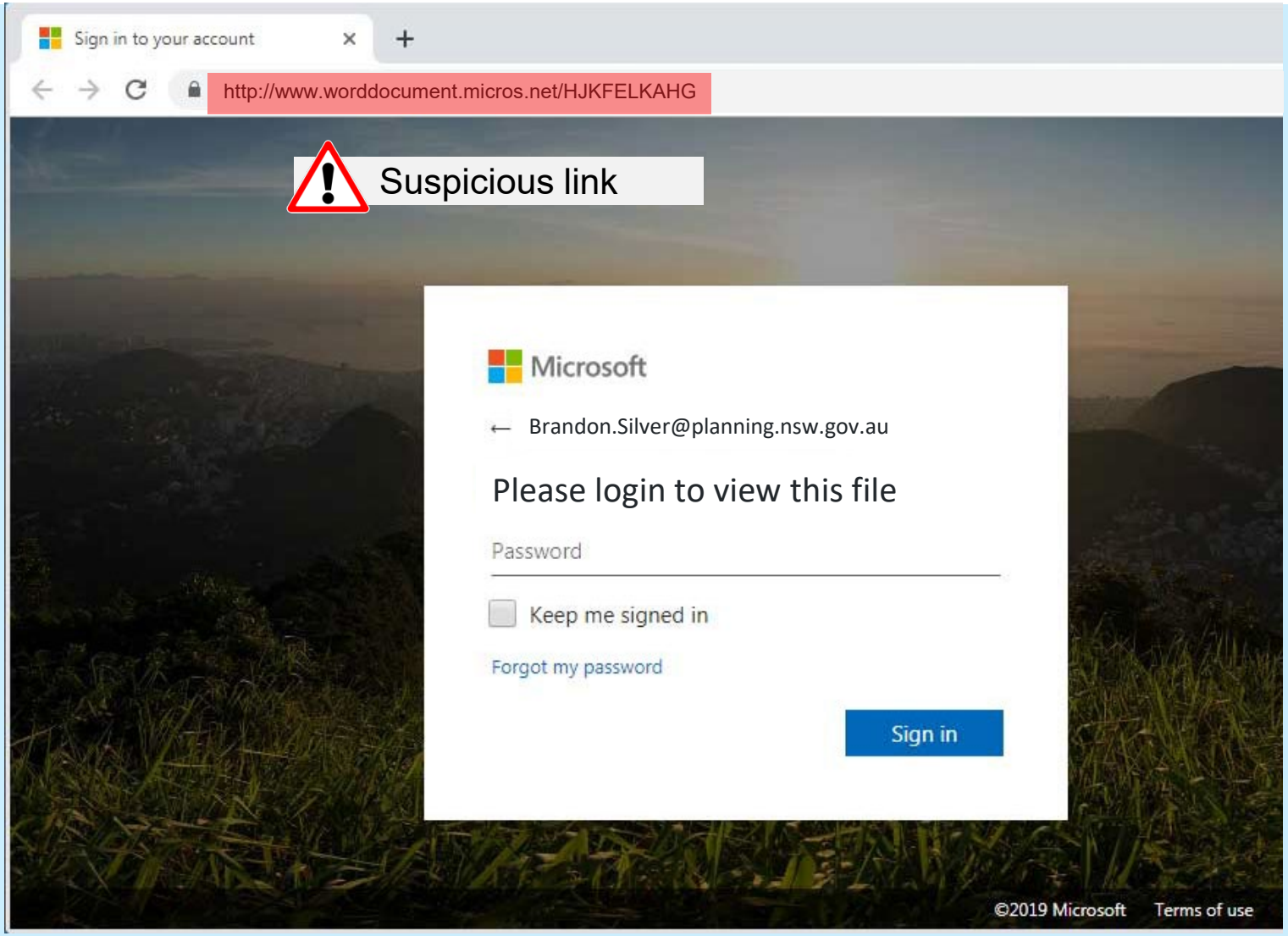
Poor spelling and grammar

Hello,
Please find attachedthe Request for Proposal Document for the Davidson marketing centre.
Please provide a proposal and your avalability for the attached scope of work.
Should you have any questions, please do not hesitate to contact our office.
Benjamin would like a response by 2PM EST on Friday 20th July 2023.

Not the usual business process

Cheers,
Evan Carr Industrial Planning Specialist
Level 19, McKell Building, 2–24 Rawson Place, Haymarket, Sydney NSW 2000
T 02 8973 7475 **E** Evan.Carr@service.nsw.gov.au
service.nsw.gov.au **1300 420 596**

Scenario 2: **Credential harvesting**



Scenario 3: **Business email compromise**

From: Susan Fry [mailto:sfry@yourcompany.com]
Sent: Tuesday, January 9, 2018 9:25 AM
To: Hamil, James <james.hamil@yourcompany.com.
Subject: Please handle ASAP

– External email. Forward any suspicious emails to bad@yourcompany.com –

Hi James,

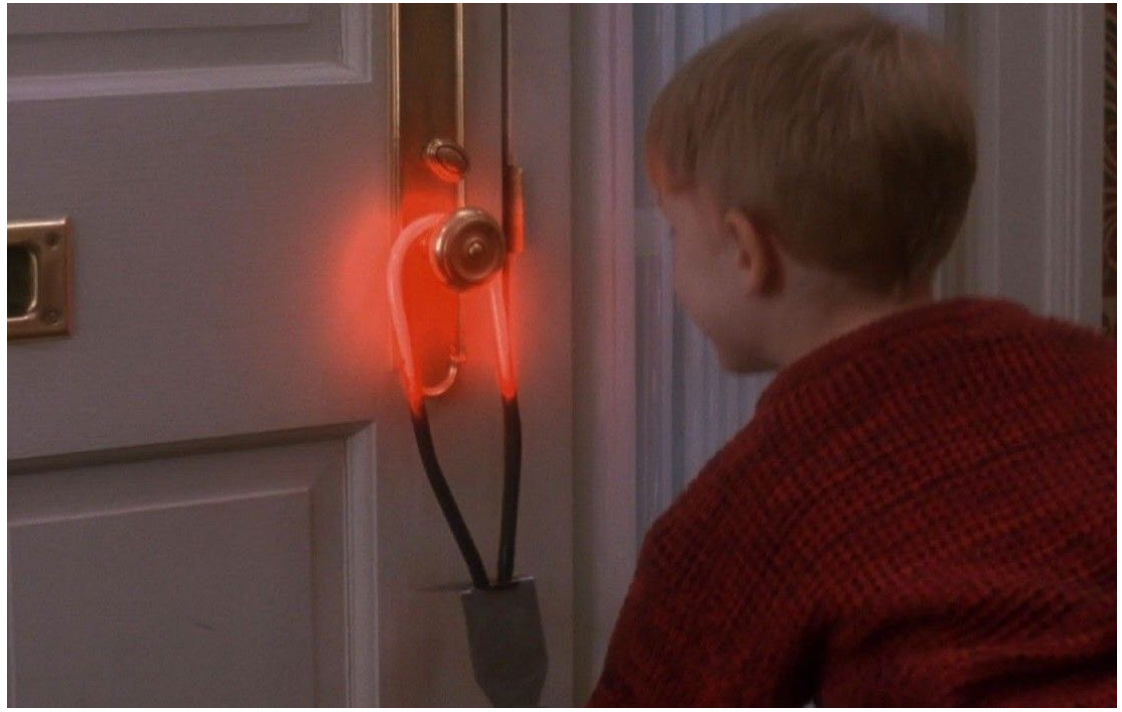
I'm currently tied up in a meeting for the next six hours, but we have a vendor saying we're late on paying an invoice. Can you handle the attached ASAP? I can't take calls, so just email me if you have questions.

Susan Fry
Chief Operating Officer
sfry@yourcompany.com

Sent from my iPhone, please excuse typos

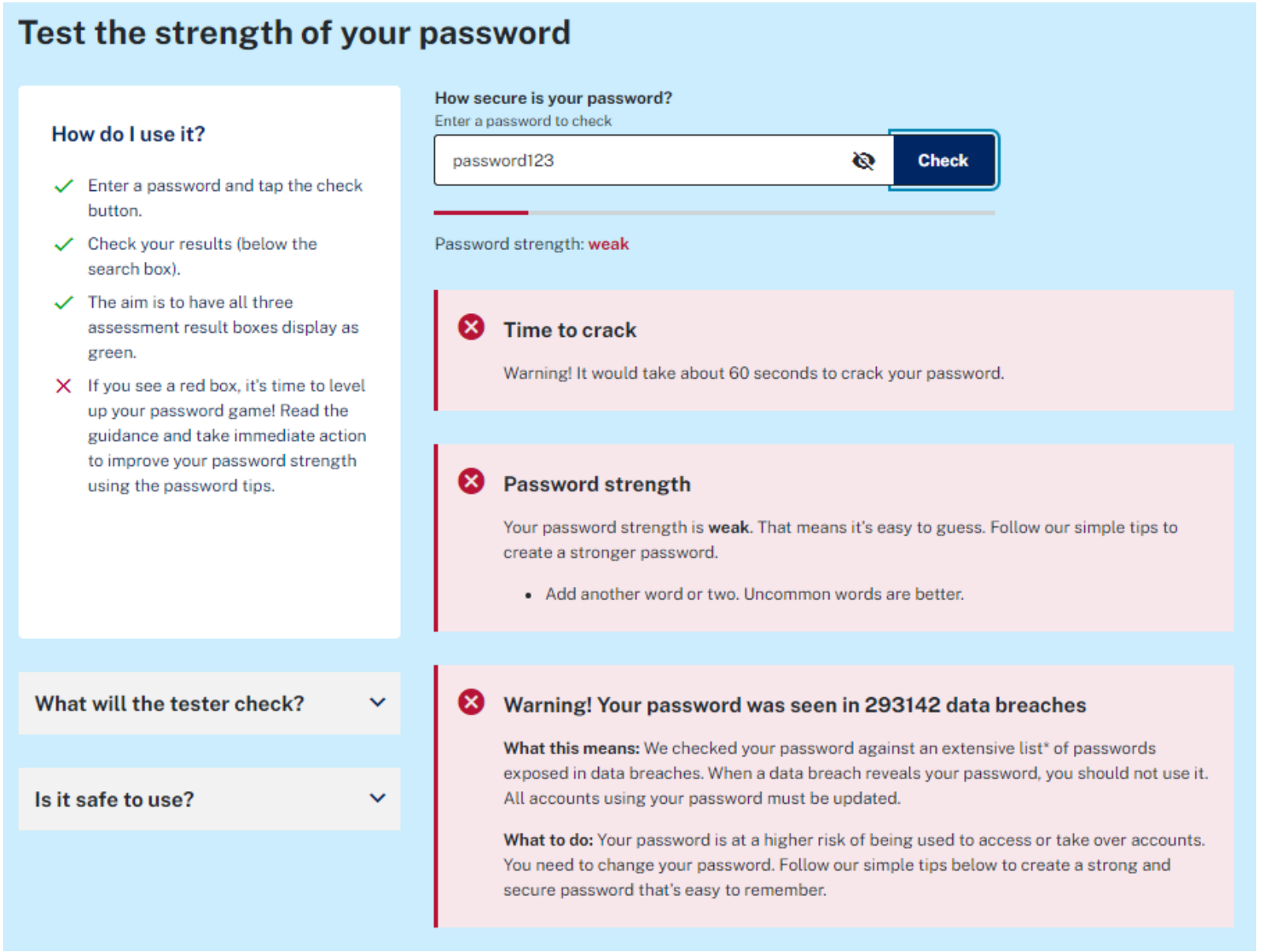
Make it hard for them to get in!

Make it hard for them to get in!



TIME IT TAKES FOR A HACKER TO CRACK YOUR PASSWORD

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	INSTANTLY	INSTANTLY	INSTANTLY	INSTANTLY	INSTANTLY
5	INSTANTLY	INSTANTLY	INSTANTLY	INSTANTLY	INSTANTLY
6	INSTANTLY	INSTANTLY	INSTANTLY	1 SEC	5 SECS
7	INSTANTLY	INSTANTLY	25 SECS	1 MIN	6 MINS
8	INSTANTLY	5 SECS	22 MINS	1 HOUR	8 HOURS
9	INSTANTLY	2 MINS	19 HOURS	3 DAYS	3 WEEKS
10	INSTANTLY	58 MINS	1 MONTH	7 MONTHS	5 YEARS
11	2 SECS	1 DAY	5 YEARS	41 YEARS	400 YEARS
12	25 SECS	3 WEEK	300 YEARS	2K YEARS	34K YEARS
13	4 MINS	1 YEAR	16K YEARS	100K YEARS	2M YEARS
14	41 MINS	51 YEARS	800K YEARS	9M YEARS	200M YEARS
15	6 HOURS	1K YEARS	43M YEARS	600M YEARS	15BN YEARS
16	2 DAYS	34K YEARS	2BN YEARS	37BN YEARS	1TN YEARS
17	4 WEEK	800K YEARS	100BN YEARS	2TN YEARS	93TN YEARS
18	9 MONTHS	23M YEARS	6TN YEARS	100 TN YEARS	7QD YEARS

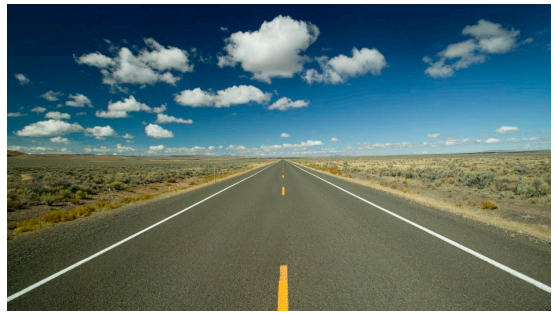


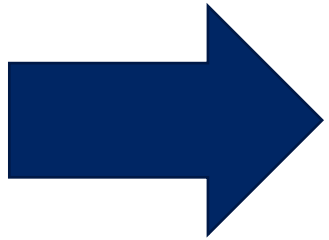
https://www.nsw.gov.au/id-support-nsw/be-prepared/passwords

Do you remember those 4 words?

Use a Passphrase

Use four random words, then add numbers & symbols:





Trumpet + Clown + Horse + Road = 1ClownHorseRo@dTrumpet

Multi-factor authentication (MFA)
A second line of defence

Something you **have** (e.g. bank card)

Something you **know** (e.g. pin number)

Something you **are** (e.g. biometrics)

Somewhere you are (e.g. IP address)

Something you **do** (e.g. the way you type)

Multi-factor authentication (MFA)
A second line of defence

Something you **have** (e.g. bank card)

Something you **know** (e.g. pin number)

Something you **are** (e.g. biometrics)

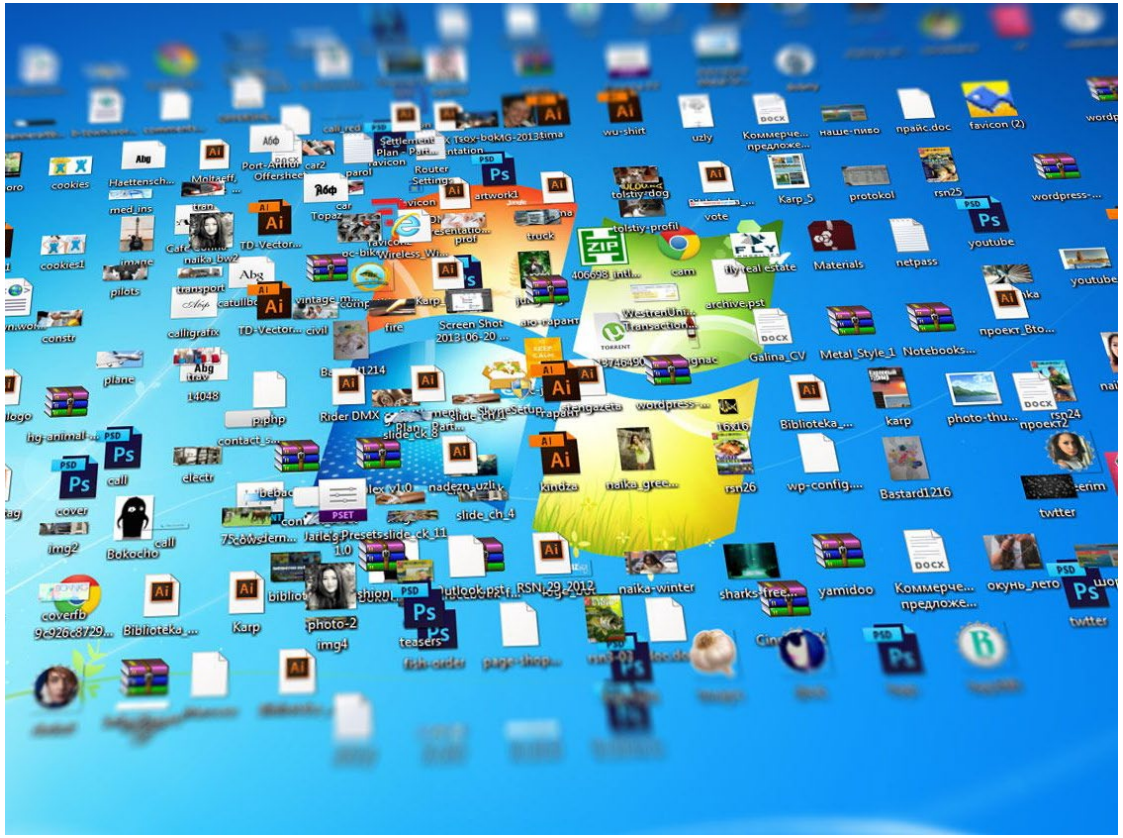
Somewhere you are (e.g. IP address)

Something you **do** (e.g. the way you type)

Once they’re in, make it difficult

Once they’re in, make it difficult

- Don’t leave sensitive files laying around
- Clean up your downloads/desktop
- Assess your access to files and devices



Your own personal ‘computer Kevin’

Anti-virus

All devices should be running anti-virus where possible

Keep anti-virus updated to detect new threats

Software updates

Enable automatic updates where possible

Updates should occur for all Internet of Things (IoT) devices, not just smartphones and PCs

Always have a back-up Plan

- Always have a secure back-up
- Set recovery access

Home Alone 7 (2025)

- The child now has **high-tech gadgets**: a plasma blaster in one hand and a glowing energy shield in the other.
- **Defensive drones** hover around, projecting laser tripwires across the room.
- A **turret-like device** on the floor emits intersecting beams, creating a security grid.
- The intruders remain in the doorway, but now face a much more advanced defence system.

Using AI Securely

- Beware of free AI platforms
- Protect sensitive data
- Verify outputs
- Turn off learning/memory

Plot Twist! – Call for Help

reddit

r/AskReddit • 4y ago
External_Set_1766

In home alone why didn't kevin just phone the police?

Timetothrowww • 4y ago

It'd be a pretty short movie

6 Award Share ···

Resources and support

Learn the basics:
https://www.cyber.gov.au/learn-basics

For business and government: https://www.cyber.gov.au/business-government

Getting help on cybercrime:
https://www.cyber.gov.au/report-and-recover/where-get-help

Report a scam:
https://www.scamwatch.gov.au/report-a-scam

Recap

Reduce your digital footprint

Beware of Phishing

Always use strong passwords and MFA

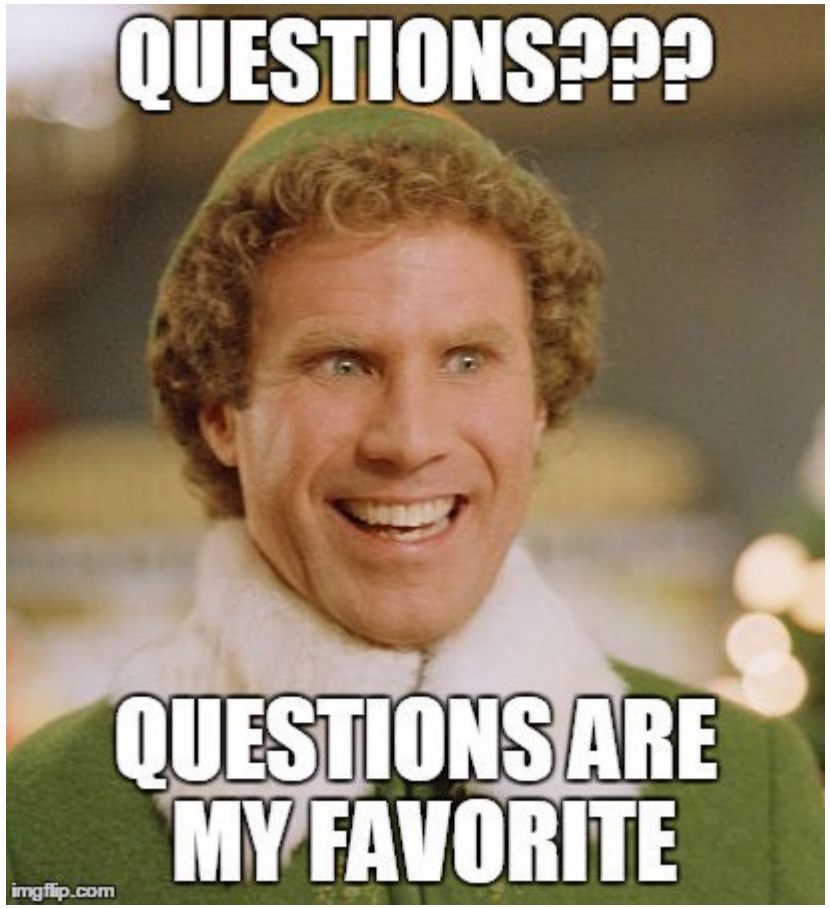
Protect your sensitive information

Always install software updates and anti-virus

Backup your data

Use AI with caution

Report any suspicious activity


QUESTIONS???
QUESTIONS ARE MY FAVORITE
imgflip.com