Digital Safeguarding for Vulnerable Adults

November 22024

Introduction

People at greater risk on-line

Purpose:

What is Digital Safeguarding?

Understanding who may be vulnerable online

What are the online risks?

Safeguarding against these risks

What is digital safeguarding?

- A good definition of safeguarding is taking proactive steps to prevent harm and abuse from occurring.
- Good safeguarding practice means you'll know what to do if harm or abuse ever takes place: who to contact, what to tell them, and how to help the person who's experienced abuse.
- So what is digital safeguarding? It's the same idea, but in a digital space.
- Digital safeguarding simply means taking steps to stay safe online.

Safeguarding in the Digital Context

- Digital safeguarding is much like safeguarding in any other context.
- Safeguarding, under The Care Act (2014), means protecting children and vulnerable adult's right to live in safety, free from abuse and neglect.
- It is about people and organisations working together to prevent and stop both the risks and experience of abuse or neglect.
- A safeguarding risk involves an allegation or concern that a person has or may have behaved in a way that has harmed themselves or another person or behaved towards a child or adult in a way that indicates they may pose a risk of harm to others.
- In the same way as all safeguarding, online safeguarding involves a whole range of potential risks; and must be looked at in relation to both victim and perpetrator.

Who is vulnerable?

People at greater risk on-line

We are all vulnerable at certain times of our lives, depending on our circumstances and life events.

When thinking of those more at risk than others, this could include a wide range of people:

e.g. those with physical disabilities or illnesses, care leavers, people with mental health difficulties, homeless, minority groups


8 Billion people
4.95 Billion have
Social Media Accounts

Social Engineering

“Social engineering attacks manipulate people into sharing information that they shouldn’t share, downloading software that they shouldn’t download, visiting websites they shouldn’t visit, sending money to criminals or making other mistakes that compromise their personal or organizational security.” - IBM

Phishing, Vishing, Qrishing

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!

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

[Prank]Email Spoofing and Phishing Proof Of Concept

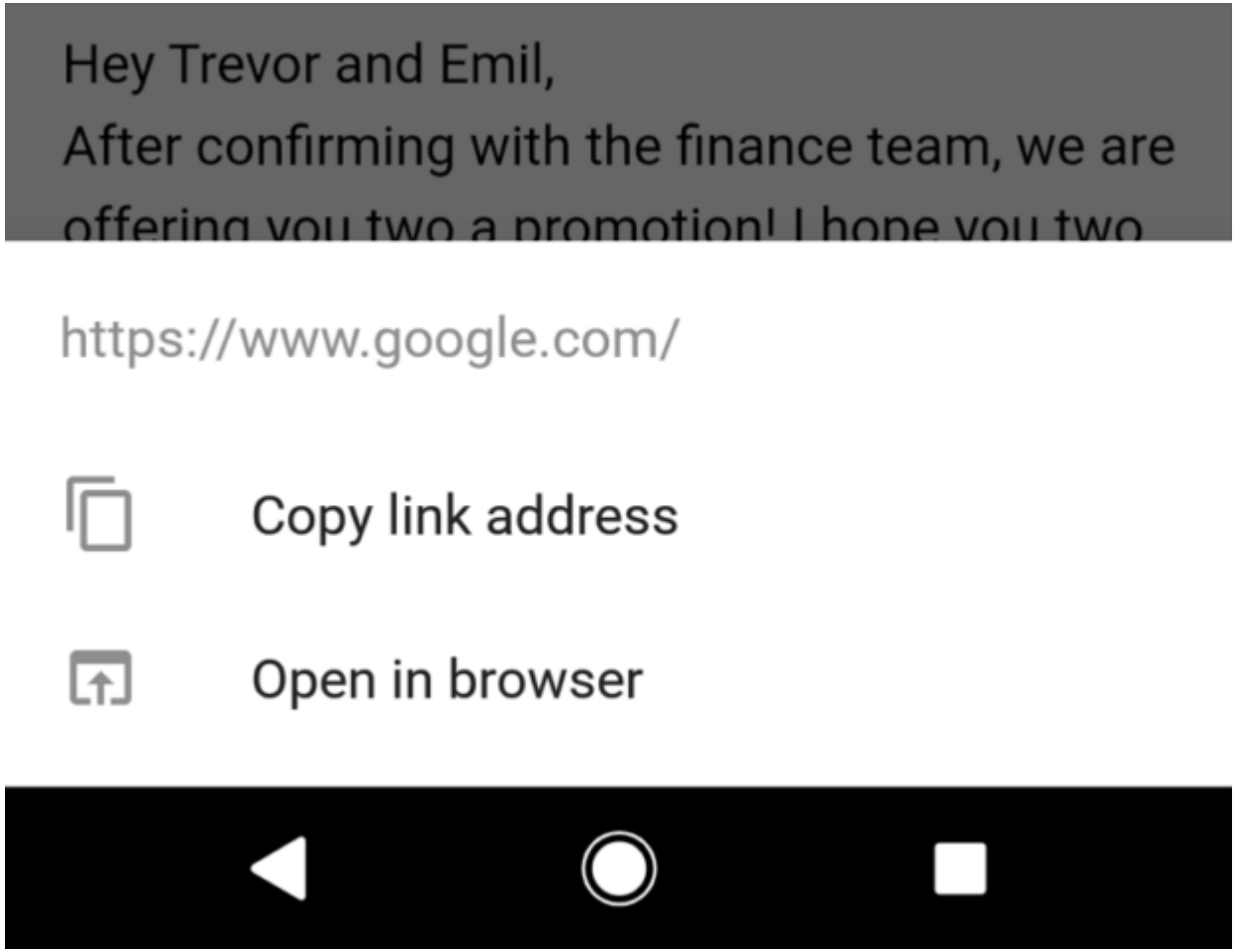
Corey Nachreiner
Trevor Collins, Emil Hozan, + 1

11:11 AM

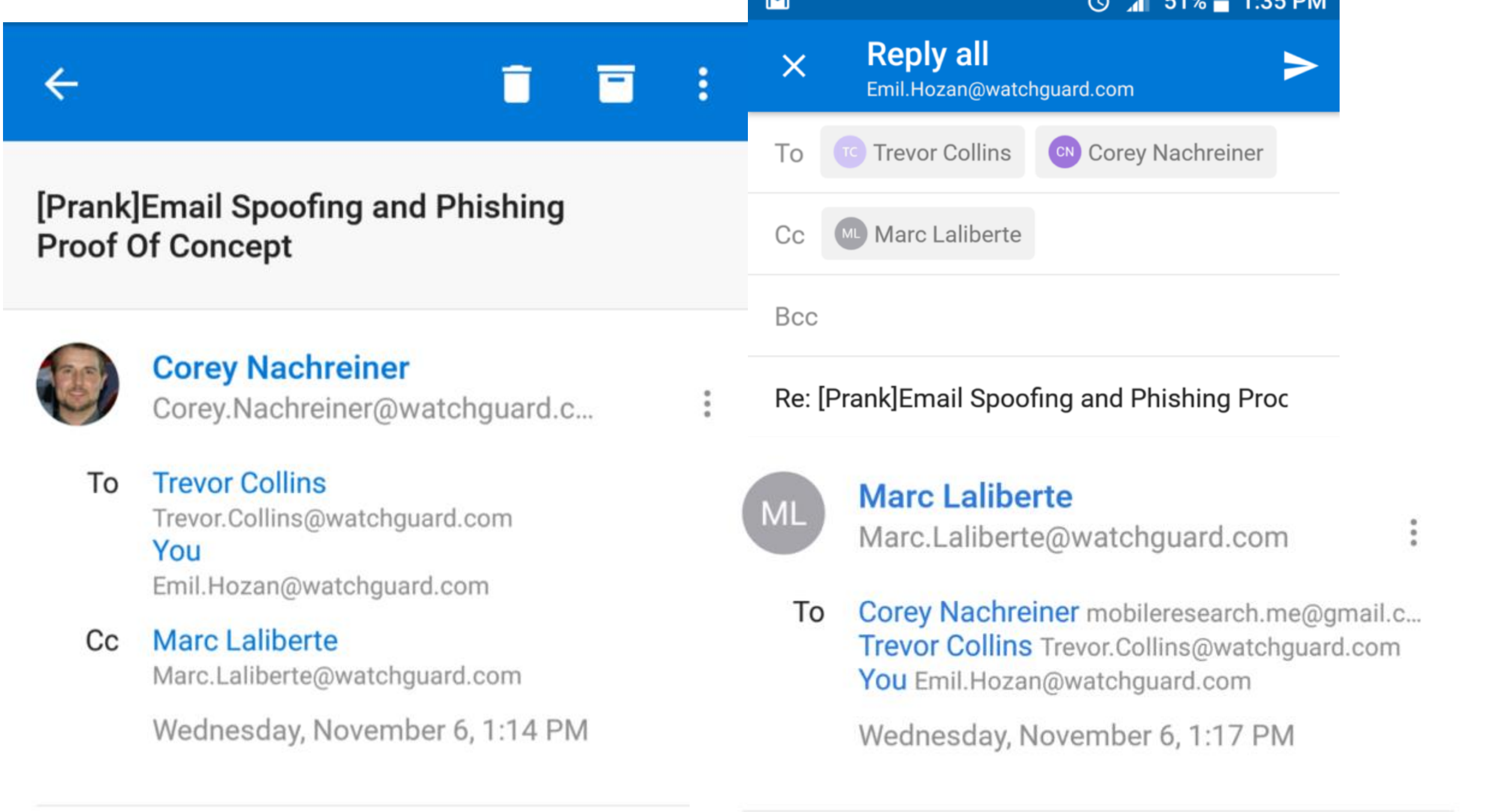
Hey Trevor and Emil,

After confirming with the finance team, we are offering you two a promotion! I hope you two excited about this opportunity! Click on the following link to log into our HR tool to accept the invite.

Cheers, C.N.



Pri ual but doesn't require to be sent via secure methods.



Private: Information that contains a small amount of sensitive data which is essential to communicate with an individual but doesn't require to be sent via secure methods.

2FA, 2SV, MFA,

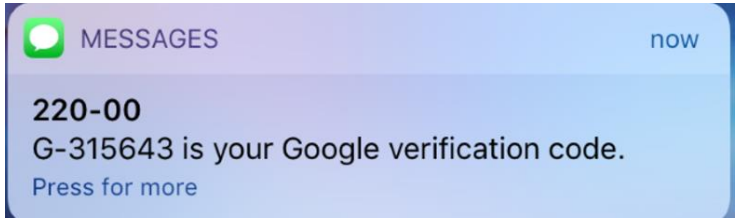
- What's the difference? Why?
- 2SV –password + code (Google, One Time Password)
- 2FA –password + push notification(SMS, App, Fingerprint, company ID, RSA tokens)

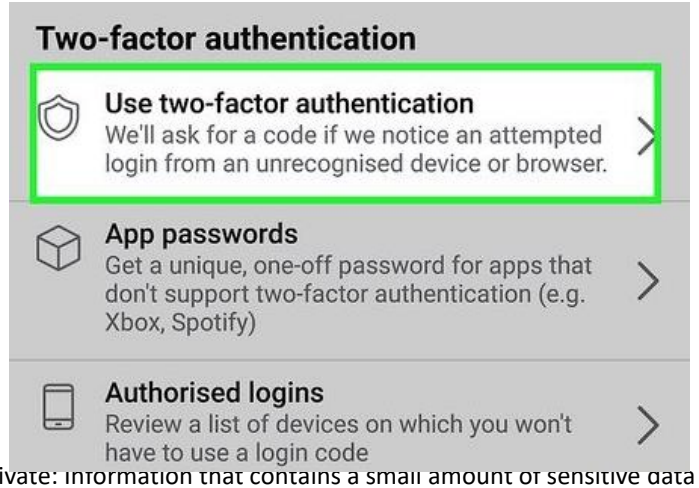
Both are classed as Multi-Factor Authentication

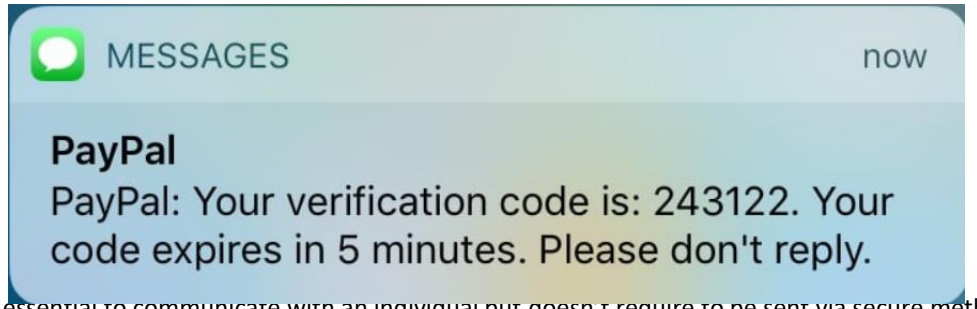
2 Step Verification

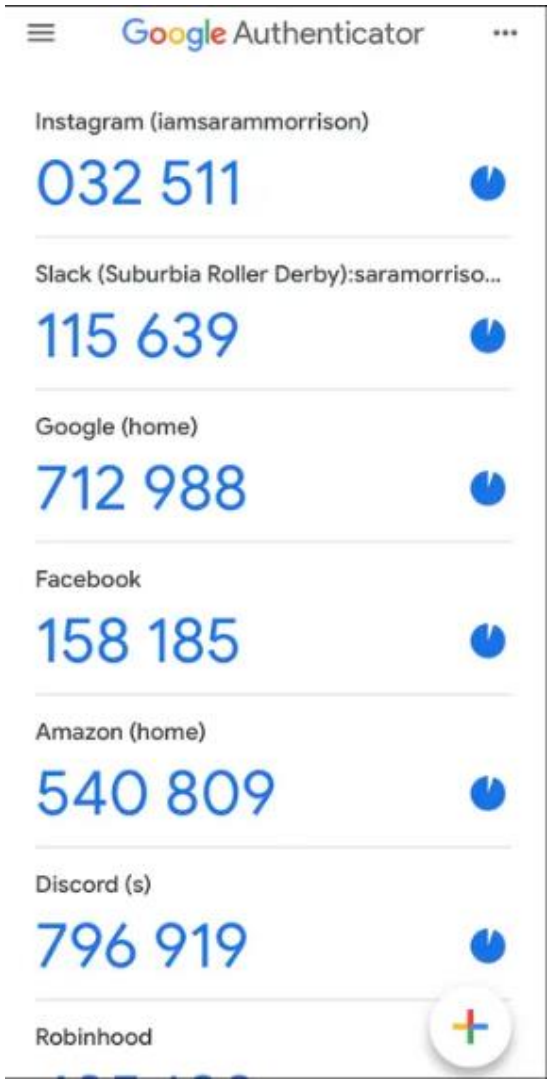
Essential

- Multi Factor Authentication (MFA)
- Two Step Verification (2SV)
- Two Factor Authentication (2FA)





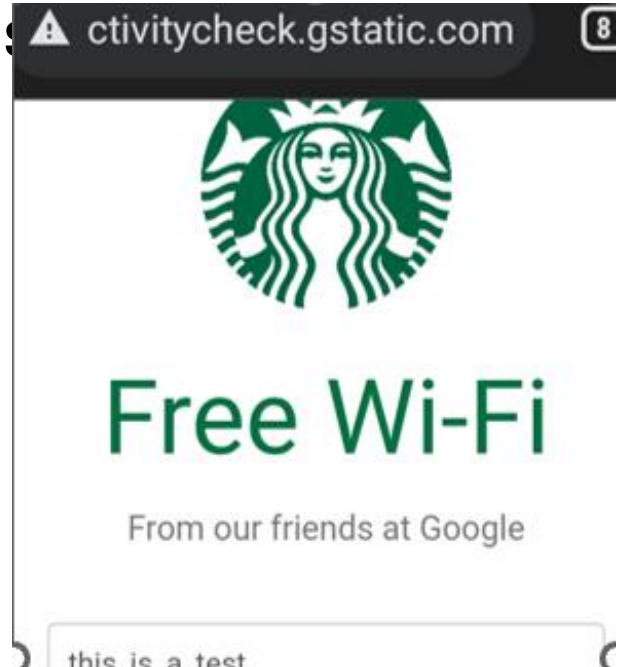




WI-FI

- **Avoid using public Wi-Fi where possible**

- **Look for a padlock or similar in the URL (bar at the top). Ensure URL contains HTTPS instead of just HTTP. HTTPS sites can still be malicious but most unsafe sites HTTP.**



Private: Information that contains a small amount of sensitive data which is essential to communicate with an individual but doesn't require to be sent via secure methods.

Ok now what?

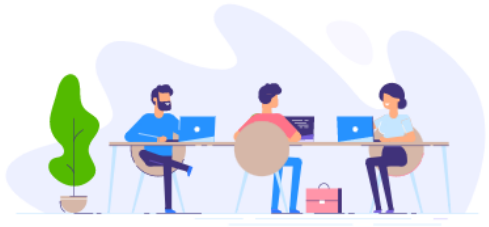
- How long is my password/s?
- How many online accounts do I have?
- Have I recently changed my password?
- Have I activated 2SV?
- Have I secured my email account properly?
- How much do I share online?
- Have I check my social media security?
- Can I spot phishing or scam emails, texts, calls better now?

Private: Information that contains a small amount of sensitive data which is essential to communicate with an individual but doesn't require to be sent via secure methods.

NCSC Cyber Aware Action Plan

Free Cyber Action Plan

Answer a few simple questions to get a free personalised action plan that lists what you or your organisation can do right now to protect against cyber attack.



Small organisations

I'm self employed or work in an organisation with up to 50 employees.

Start now

For individuals & families

I want to improve my personal cyber security.

Start now

Reporting

Action Fraud

National Fraud & Cyber Crime Reporting Centre

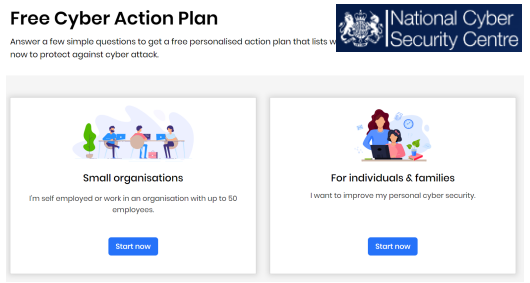
0300 123 2040

Reporting

- **SMS – 7726**
- **159 – Secure Banking**
- **Email – report@phishing.gov.uk**
- **Google – "Free Cyber Action Plan"**

As of 31/03/24

- Over 30.75 million reports
- Removal of 176,100 scams
- Across 321,400 URLs



Private: Information that contains a small amount of sensitive data which is essential to communicate with an individual but doesn't require to be sent via secure methods.