HELP TO GROW

CYBER DEFENCES FOR SMEs

Dr Clare Johnson
Capability Lead ITSUS Consulting
www.linkedin.com/in/clare-johnson

ITSUS CONSULTING

Objectives

- Introduction
- Why should you care about cyber security?
- Most common cyber attacks
- Consequences of a successful attack
- Quick wins
- Longer term resilience
- Resources

Join at menti.com | use code 3329 1473

Mentimeter

What is Cyber Security?

All responses to your question will be shown here

Each response can be up to 200 characters long

Turn on voting to let participants vote for their favorites

Menti

H2G Conference

Choose a slide to present

WHAT IS CYBER SECURITY

"Cybersecurity refers to any technologies, practices and policies for preventing cyberattacks or mitigating their impact. Cybersecurity aims to protect computer systems, applications, devices, data, financial assets and people against ransomware and other malware, phishing scams, data theft and other cyberthreats." (IBM)

"Cyber security helps individuals and organisations reduce the risk and impact of cyber attacks". (NCSC)

Join at menti.com | use code 3329 1473

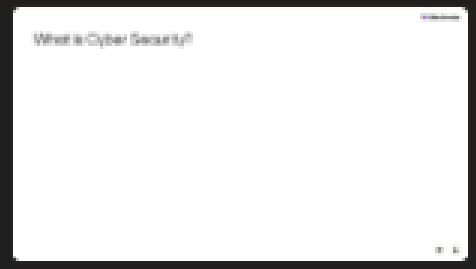
Mentimeter

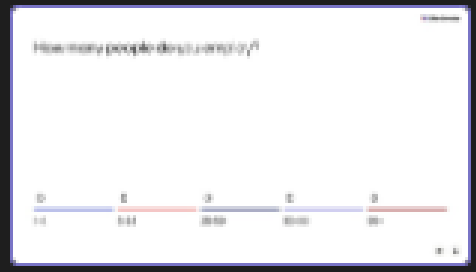
How many people do you employ?

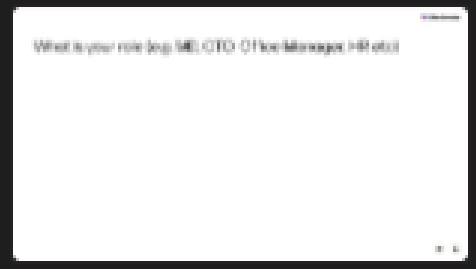
Menti

H2G Conference

Choose a slide to present







ABOUT US

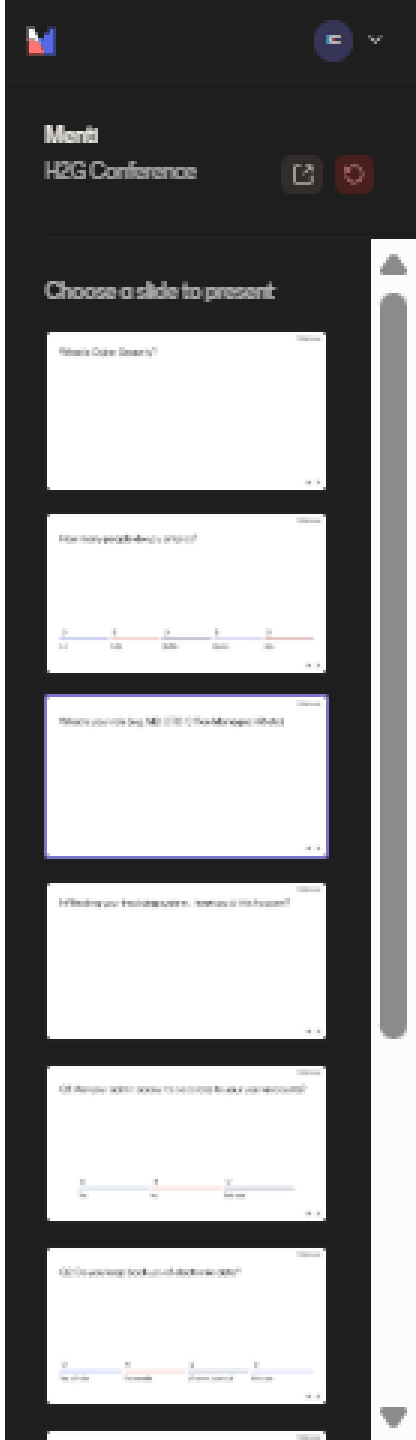
ITSUS is a specialist networks and cyber security SME, providing a wide range of ICT lifecycle services to defence, public and commercial sectors.

- Trading since 2008
- Cyber Essential Plus and ISO 27001 certified
- 26 full time staff
- Based in Cardiff

Join at menti.com | use code 3329 1473

Mentimeter

What is the nature of your business?



NO ONE WOULD WANT TO ATTACK ME!

But…

Who are your customers?

Who is in your supply chain?

How would a successful cyber attack affect your business?

43% of businesses and 30% of charities had some form of cyber attack in 12 months

Join at menti.com | use code 3329 1473

Mentimeter

Accessing your invoicing system... how could this happen?

All responses to your question will be shown here

Each response can be up to 200 characters long

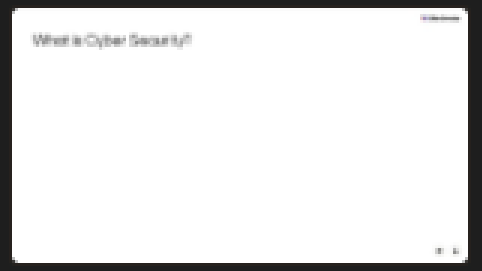
Turn on voting to let participants vote for their favorites

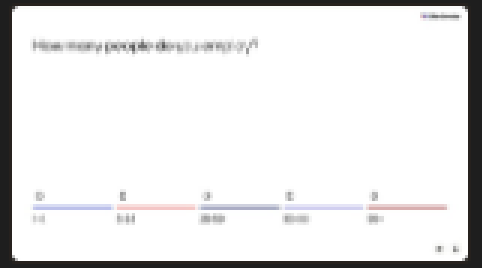
IC

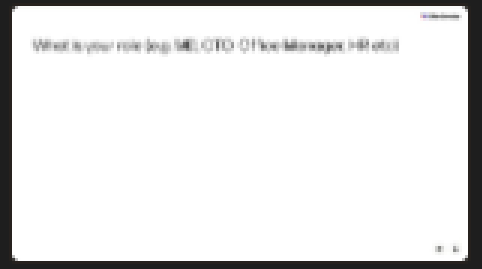
Menti

H2G Conference

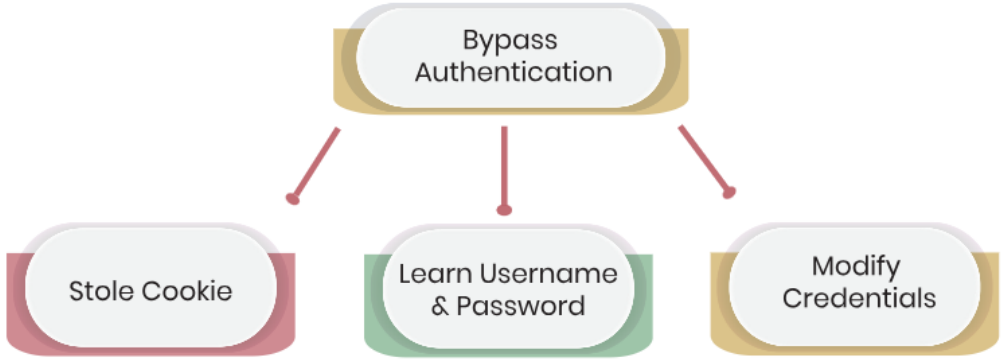
Choose a slide to present







Threat Modelling



Phishing email → Credential theft → Remote access → Privilege escalation → Invoicing data

TYPES OF BREACHES OR ATTACKS

Type of breach / attack	Proportion of attacks reported
Phishing attacks	85%
Impersonation	34%
Devices targeted by other malware	18%
Takeovers (web / social media / email)	7%
Hacking / attempted hacking of bank accounts	6%
Devices targeted with ransomware	6%
Other (DNS, Unauthorised access / listening / other)	9%

NB – Businesses may be affected by more than one type of attack

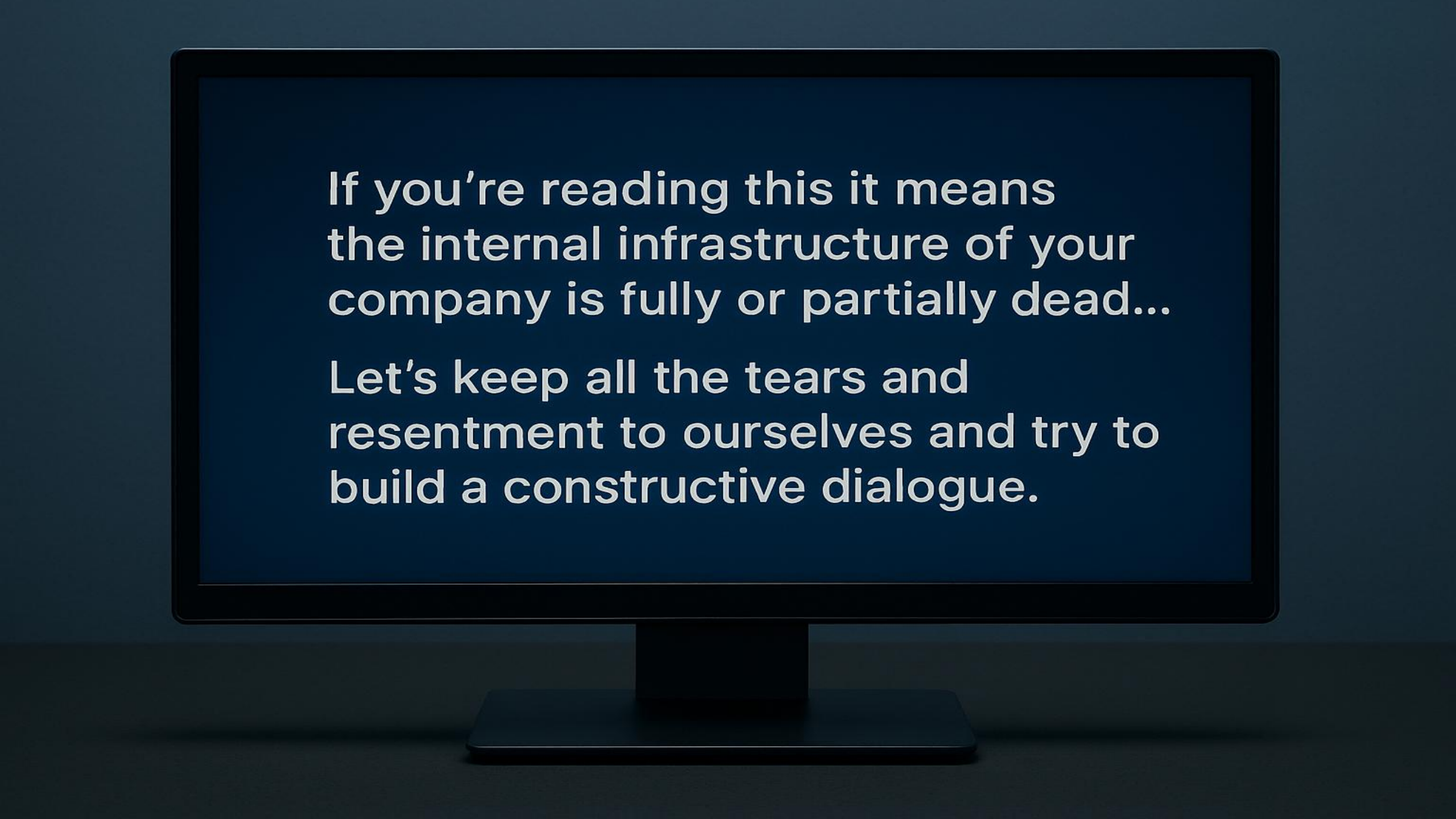
Source: Cyber Security Breaches Survey 2025, DSIT

THE CONSEQUENCES OF A SUCCESSFUL ATTACK

Consequences of a successful cyber attack:

- System downtime causing revenue loss
- Lost customers
- Reputational damage
- ICO fines

DSIT estimate that approximately 612,000 UK business identified a cyber breach or attack in the 12 months preceding the report


If you’re reading this it means
the internal infrastructure of your
company is fully or partially dead...
Let’s keep all the tears and
resentment to ourselves and try to
build a constructive dialogue.

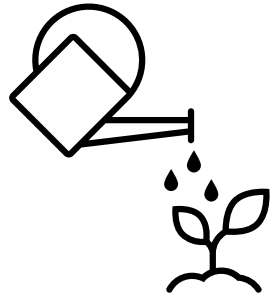
Quick Wins

People

Process

Technology

- Cyber Aware campaign – NCSC https://www.ncsc.gov.uk/cyberaware/home
- **Free Cyber Action Plan** – NCSC https://www.ncsc.gov.uk/cyberaware/actionplan
- 10 Steps to Cyber Security – NCSC https://www.ncsc.gov.uk/collection/10-steps
- Check your cyber security – NCSC https://checkcybersecurity.service.ncsc.gov.uk/



NCSC Cyber Action Plan

Cyber Aware

National Cyber Security Centre

Your result

Based on the answers you've provided, we've identified the following actions that we strongly recommend to protect your business online.

Print / Download

Protect your email and social media accounts

URGENT

Change your password on your work email

If a cyber criminal gets access to your work email account, they could:

- read your personal and business emails, and access private information about you
- reset the passwords on your other accounts
- send emails to your business or client contacts pretending to be you

You should use strong and separate passwords for each one of your work email accounts so that if one account is hacked, a cyber criminal won't be able to access the others using the same password.

Tips on how to create and remember strong passwords:

URGENT

Turn on 2-step verification (2SV) for all your important work accounts

2SV asks for another way to prove your identity when you sign in to a service, such as a code that is sent to your phone. You then need to enter this code to prove it's really you.

Turning on 2SV is essential for your most important work accounts, like email and social media. Your online banking probably has it enabled by default.

You won't have to enter a code every time you use a service. For some accounts, you can choose to do this just when signing in from a new device or changing your password.

It only takes a few minutes to set up 2SV and once you've done it, even if a cyber criminal discovers your password, they won't be able to get access to your account.

How to enable 2SV on some popular services:

Outlook (opens in a new tab)

Gmail (opens in a new tab)

iCloud (opens in a new tab)

Apple ID (opens in new tab)

Instagram (opens in new tab)

Facebook (opens in new tab)

Twitter (opens in new tab)

ITSUS CONSULTING

NCSC 10 Steps

Asset Management

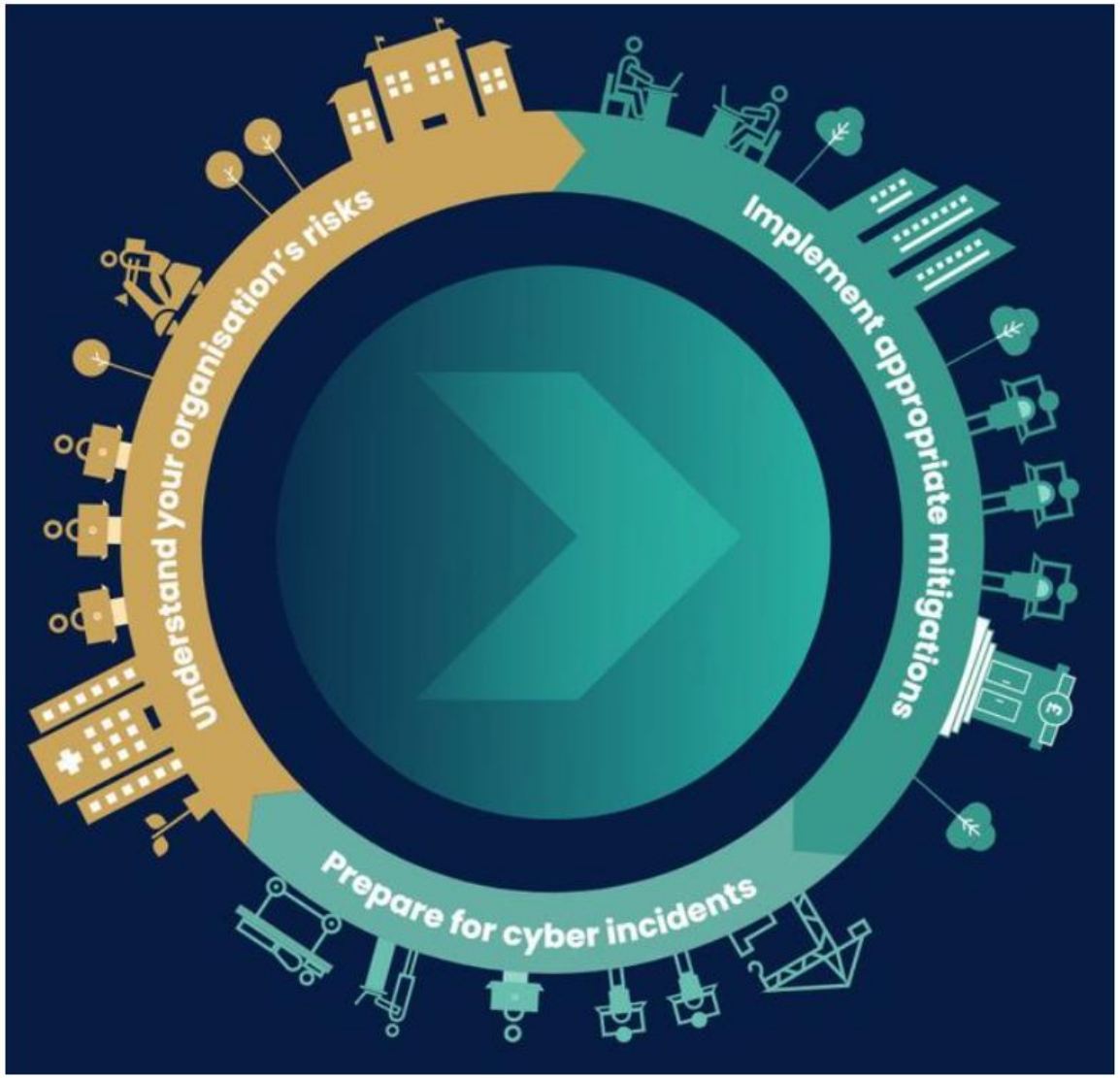
What are the benefits?

- **Ability to identify what technology and information is in your organisation,** understand what is most important to deliver your organisation's objectives, and to assess the impact if that technology or information becomes compromised in some way.
- **Ability to identify and assess vulnerabilities that may present a risk to your organisation** throughout the lifetime of your systems, reducing the likelihood of a unknown system that has not been properly maintained being exploited and causing an incident
- **Ability to apply and maintain proportionate security controls** by having an up-to-date understanding of your assets
- **Ability to plan future technology cycles** to reduce the risk of legacy or unmanaged systems, as you can plan to replace these before they becomes a security risk.

Guidance on how organisations can protect themselves in cyberspace.

Pages

PAGE 1 OF 11



PUBLISHED

11 May 2021

Password Evolution

spaghetti
Spaghetti
Spaghetti1
Spaghetti1!
spaghettisaucecheese
Icookspaghettieveryday
1Co0k$pahgett1everyday

https://haveibeenpwned.com/

- One word for everything
- Add a capital letter
- Add a number
- Add a special character
- Three random words
- Passphrase
- Passkey

Defence in Depth

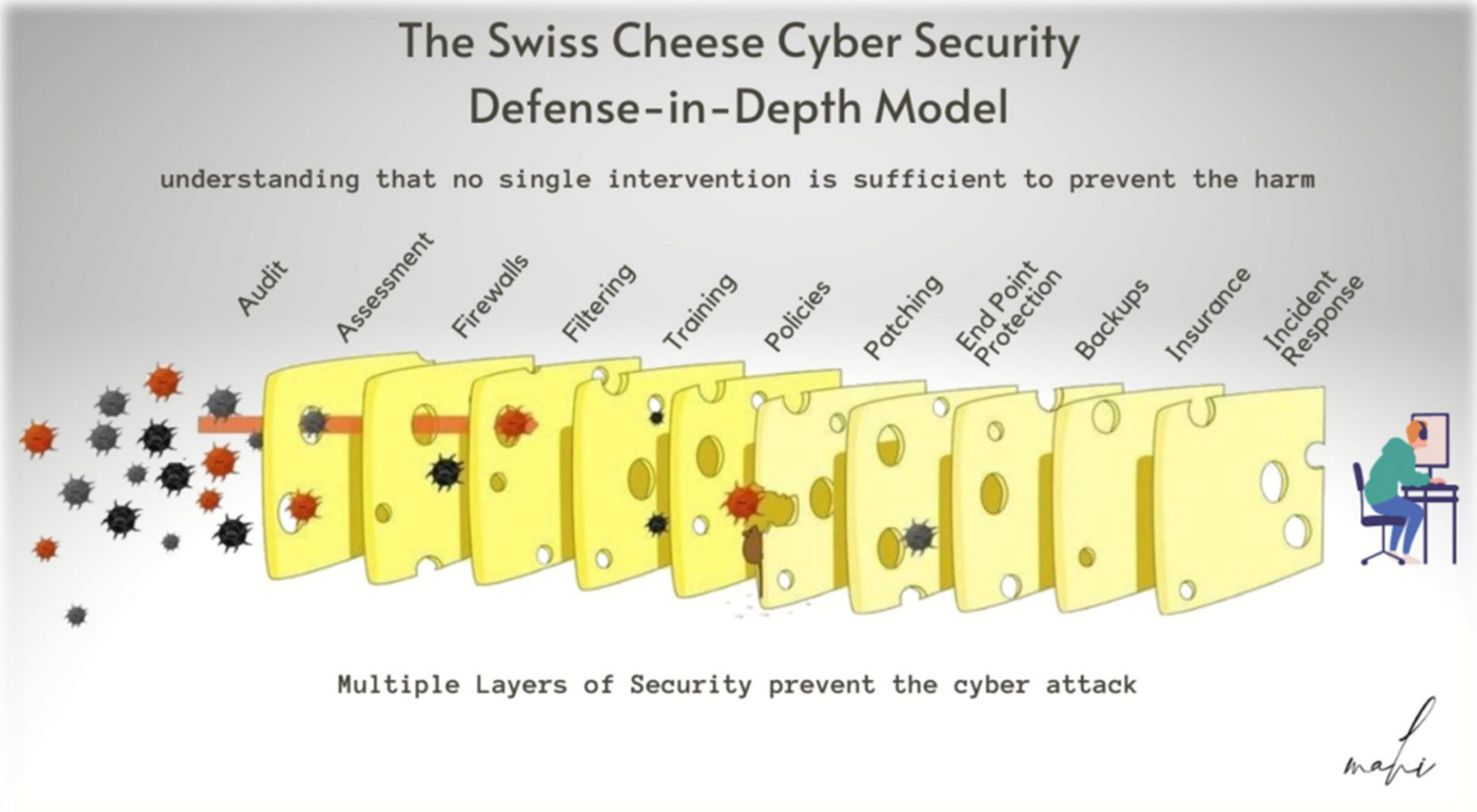
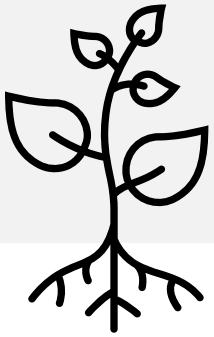


Image from https://maheshcg.me/the-swiss-cheese-cyber-security-defense-in-depth-model/

Defence in Depth

Image from https://maheshcg.me/the-swiss-cheese-cyber-security-defense-in-depth-model/

Longer Term Strategy



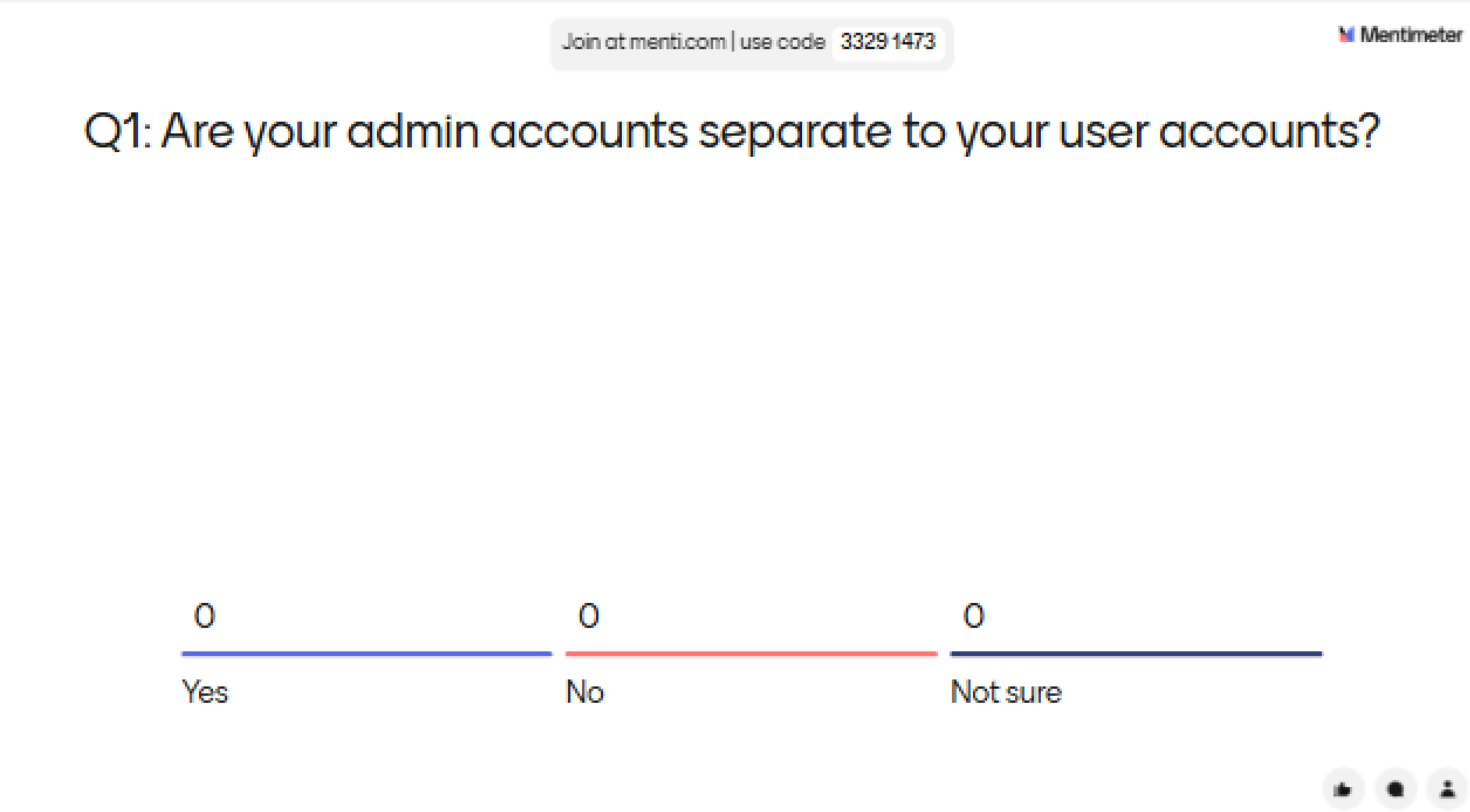
- Cyber Essentials / Essentials Plus
- ISO 27001? Senior leadership buy-in
- Check your back ups
- Incident Response plans, Disaster Recovery plans, Business Continuity
- Table top exercises
- Simulations
- Custom configuration of technical controls – e.g. Microsoft Office 365 E3 / E5
- Create a culture of good cyber security

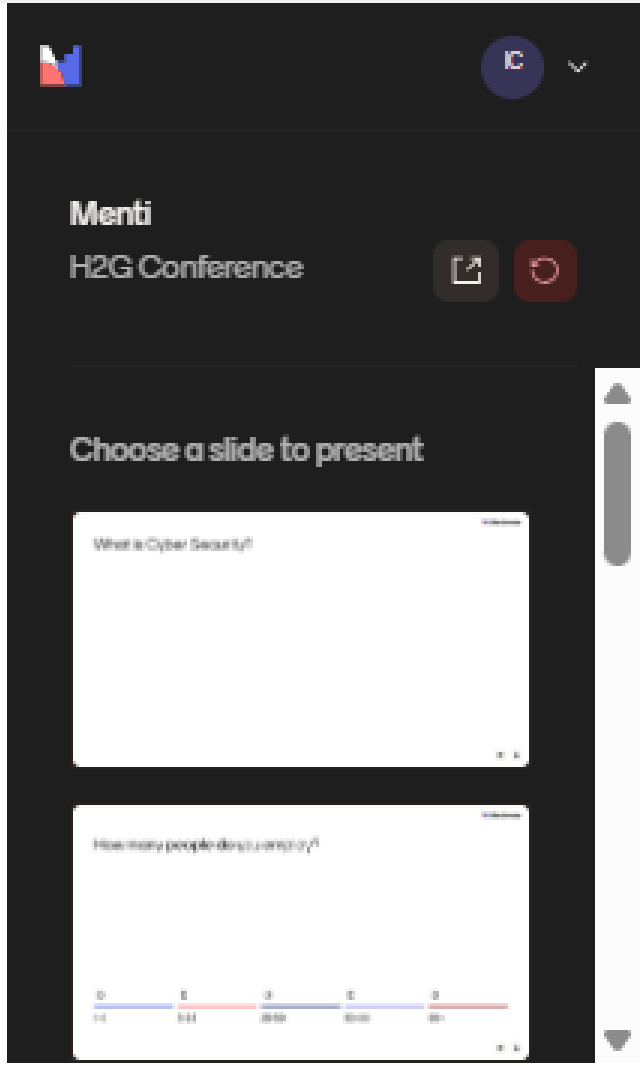
Least privilege

Zero Trust

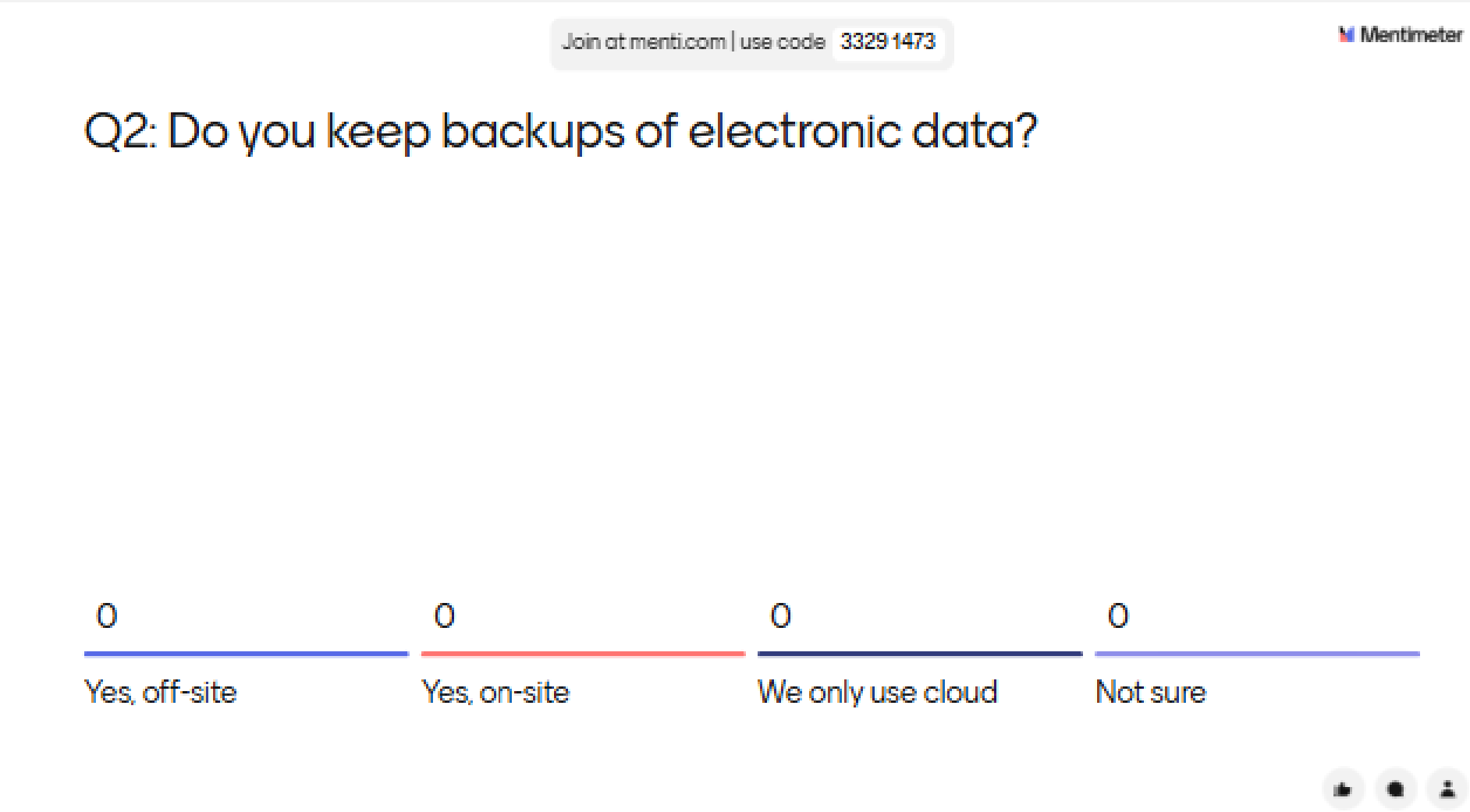
Cloud First

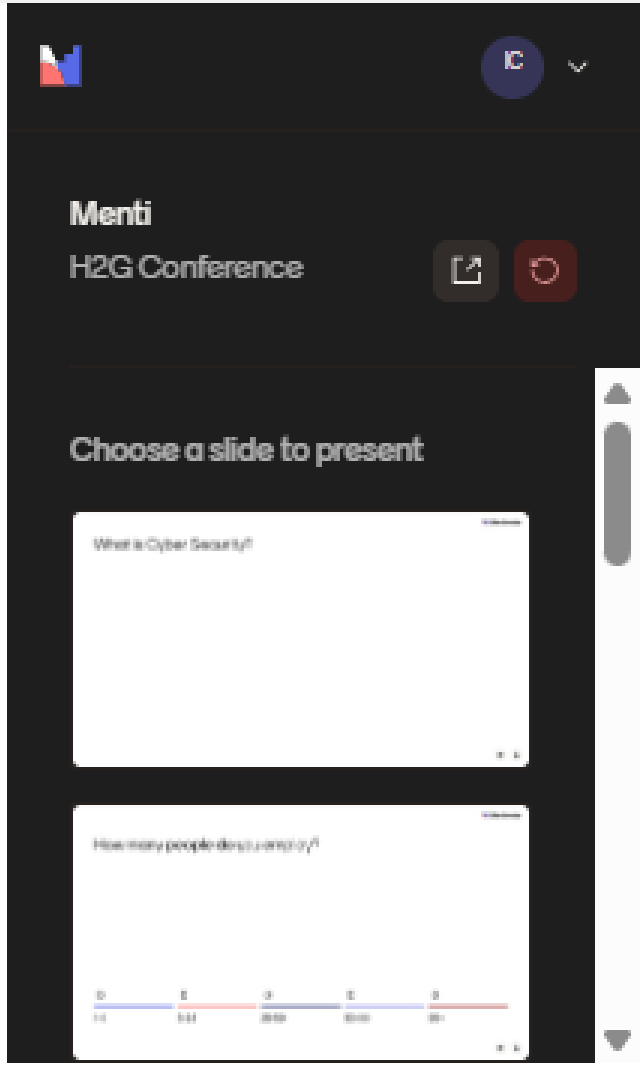
Closing Quiz



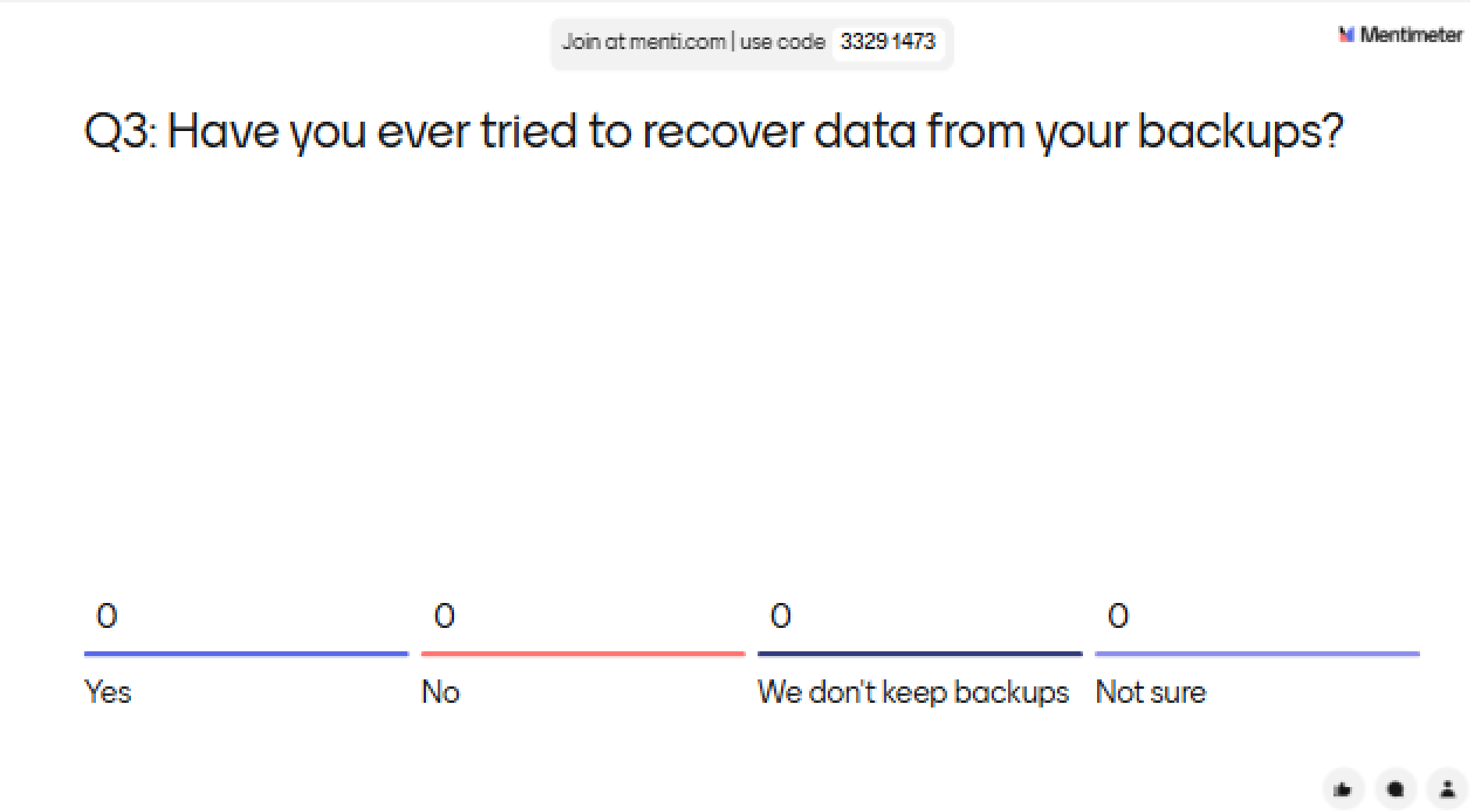


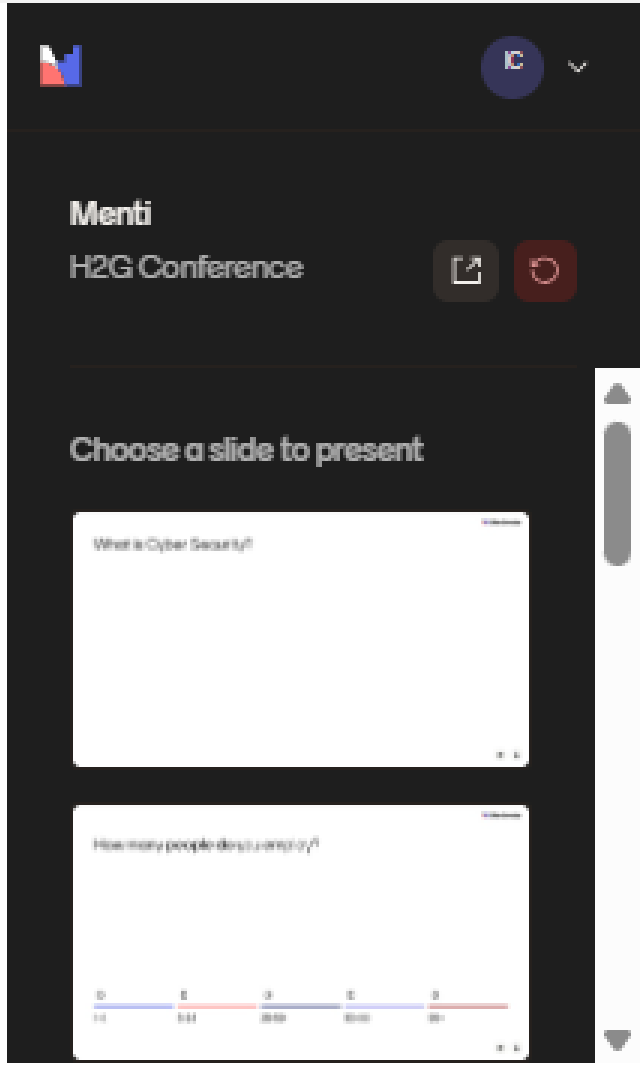
Closing Quiz



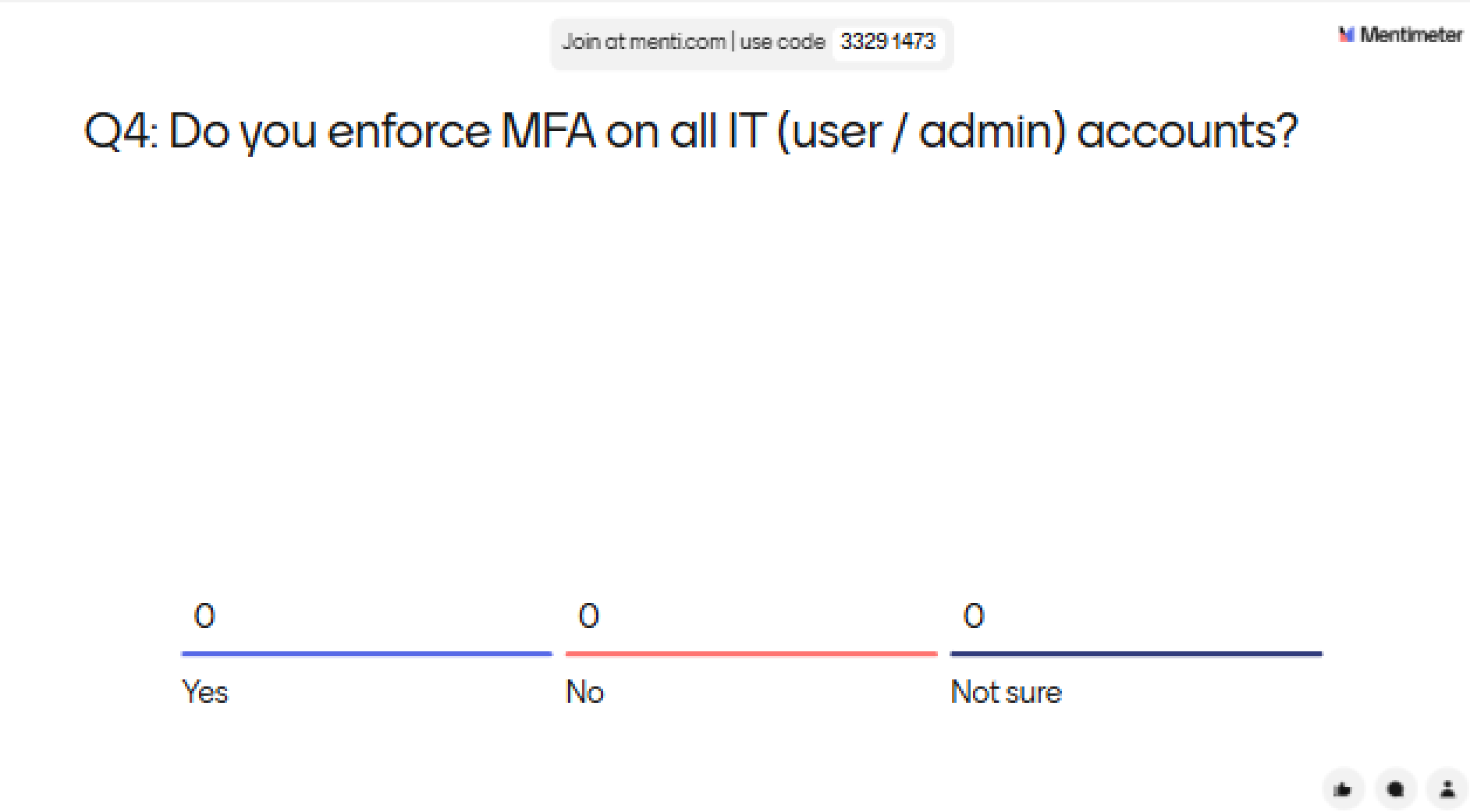


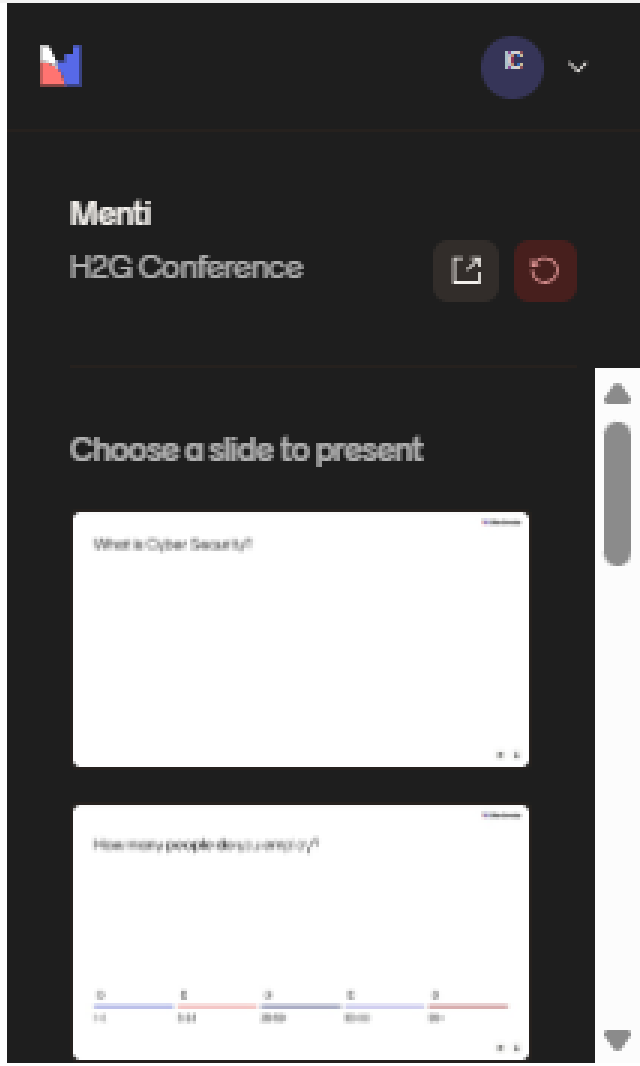
Closing Quiz





Closing Quiz





Closing Quiz

Join at menti.com | use code 3329 1473

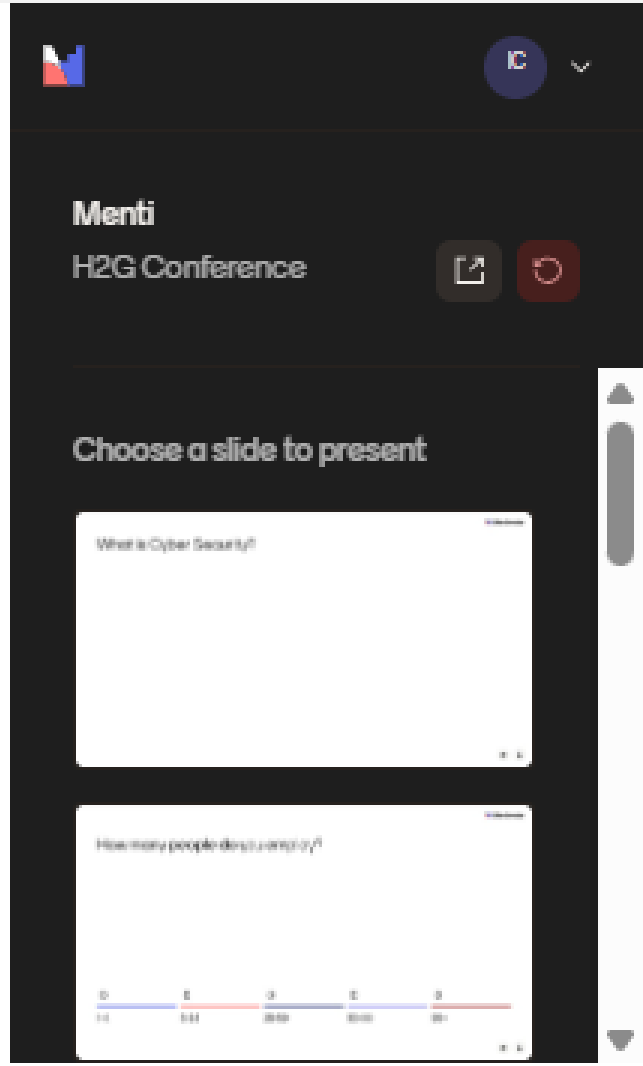
Mentimeter

Q5: What is the next cyber security improvement you will make?

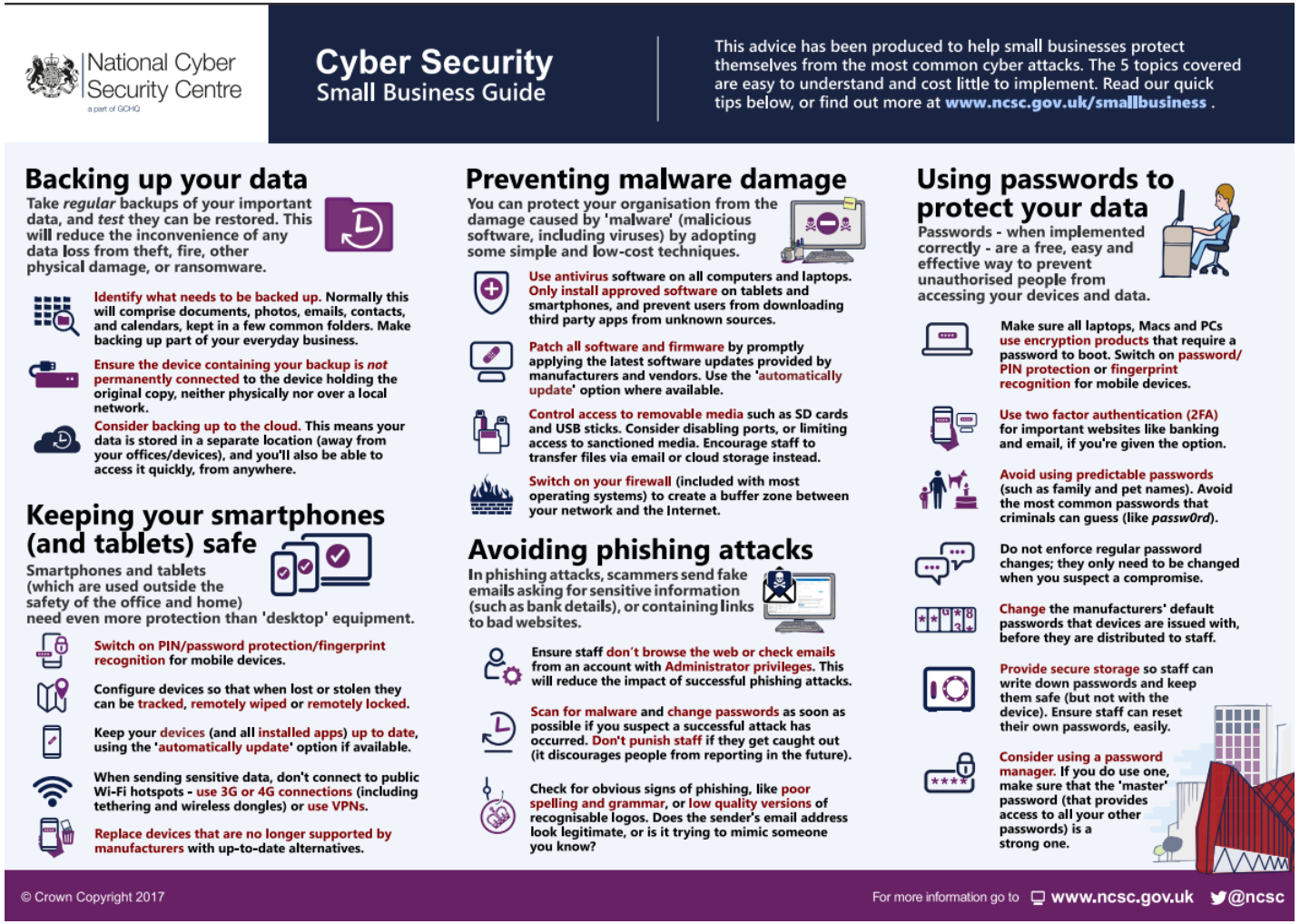
All responses to your question will be shown here

Each response can be up to 200 characters long

Turn on voting to let participants vote for their favorites



USEFUL RESOURCES



National Cyber Security Centre
a part of GCHQ

Cyber Security
Small Business Guide

This advice has been produced to help small businesses protect themselves from the most common cyber attacks. The 5 topics covered are easy to understand and cost little to implement. Read our quick tips below, or find out more at **www.ncsc.gov.uk/smallbusiness** .

Backing up your data

Take *regular* backups of your important data, and *test* they can be restored. This will reduce the inconvenience of any data loss from theft, fire, other physical damage, or ransomware.

Identify what needs to be backed up. Normally this will comprise documents, photos, emails, contacts, and calendars, kept in a few common folders. Make backing up part of your everyday business.

Ensure the device containing your backup is *not* permanently connected to the device holding the original copy, neither physically nor over a local network.

Consider backing up to the cloud. This means your data is stored in a separate location (away from your offices/devices), and you'll also be able to access it quickly, from anywhere.

Keeping your smartphones (and tablets) safe

Smartphones and tablets (which are used outside the safety of the office and home) need even more protection than 'desktop' equipment.

Switch on PIN/password protection/fingerprint recognition for mobile devices.

Configure devices so that when lost or stolen they can be **tracked**, **remotely wiped** or **remotely locked**.

Keep your **devices** (and all **installed apps**) **up to date**, using the '**automatically update**' option if available.

When sending sensitive data, don't connect to public Wi-Fi hotspots - **use 3G or 4G connections** (including tethering and wireless dongles) or **use VPNs**.

Replace devices that are no longer supported by manufacturers with up-to-date alternatives.

Preventing malware damage

You can protect your organisation from the damage caused by 'malware' (malicious software, including viruses) by adopting some simple and low-cost techniques.

Use antivirus software on all computers and laptops. **Only install approved software** on tablets and smartphones, and prevent users from downloading third party apps from unknown sources.

Patch all software and firmware by promptly applying the latest software updates provided by manufacturers and vendors. Use the '**automatically update**' option where available.

Control access to removable media such as SD cards and USB sticks. Consider disabling ports, or limiting access to sanctioned media. Encourage staff to transfer files via email or cloud storage instead.

Switch on your firewall (included with most operating systems) to create a buffer zone between your network and the Internet.

Avoiding phishing attacks

In phishing attacks, scammers send fake emails asking for sensitive information (such as bank details), or containing links to bad websites.

Ensure staff **don't browse the web or check emails** from an account with **Administrator privileges**. This will reduce the impact of successful phishing attacks.

Scan for malware and **change passwords** as soon as possible if you suspect a successful attack has occurred. **Don't punish staff** if they get caught out (it discourages people from reporting in the future).

Check for obvious signs of phishing, like **poor spelling and grammar**, or **low quality versions** of recognisable logos. Does the sender's email address look legitimate, or is it trying to mimic someone you know?

Using passwords to protect your data

Passwords - when implemented correctly - are a free, easy and effective way to prevent unauthorised people from accessing your devices and data.

Make sure all laptops, Macs and PCs **use encryption products** that require a password to boot. Switch on **password/PIN protection** or **fingerprint recognition** for mobile devices.

Use two factor authentication (2FA) for important websites like banking and email, if you're given the option.

Avoid using predictable passwords (such as family and pet names). Avoid the most common passwords that criminals can guess (like *passw0rd*).

Do not enforce regular password changes; they only need to be changed when you suspect a compromise.

Change the manufacturers' default passwords that devices are issued with, before they are distributed to staff.

Provide secure storage so staff can write down passwords and keep them safe (but not with the device). Ensure staff can reset their own passwords, easily.

Consider using a password manager. If you do use one, make sure that the 'master' password (that provides access to all your other passwords) is a strong one.

For more information go to www.ncsc.gov.uk @ncsc

National Cyber Security Centre
a part of GCHQ

- Check your Cyber Security
- Cyber Aware Action Plan
- Action Fraud
- Cyber Resilience Centre
- Join local Cyber Cluster

CONTACT US

Dr Clare Johnson, Capability Lead (Cyber & Networks)
clare@itsusconsulting.com

ITSUS Consulting
4 Earlswood Road, Llanishen, Cardiff CF14 5GH

Phone
T: 02920 003 170

Email
sales@itsusconsulting.com

QUESTIONS

ITSUS CONSULTING