



Staying Safe in a Digital World

Security Awareness
for Employees



Contents

Security Awareness Training

Introduction 03

Why is security awareness so important?	04
How will the training work?	05
Frequently Asked Questions	06

Cyber Awareness Toolkit 07

Cyber Threats and Risks	08
The importance of good password hygiene	09
Internet and Email Security	10
How to spot a phishing email	11
Social Engineering	12
Physical Security	13
Incident Reporting	14

Introduction

In today's interconnected world, security awareness has become essential to business safety. Organisations are responsible for protecting their data, systems, and assets, and their employees play a crucial role in achieving this goal. By having security awareness training for employees, organisations can help reduce the risk of cyber threats, data breaches, and other security incidents.

Employees are the first line of defence against cyber-attacks and other security incidents. You handle sensitive data and have access to critical systems, which makes your business vulnerable to security threats. With the proper security awareness training, you can recognise and respond appropriately to potential security threats, minimising the risk of a security breach.

We've partnered with a leading human risk management company to help us make sure we keep our organisation, customers and colleagues safe against evolving cyber threats. This ongoing training will involve you completing regular computer-based security awareness courses that are designed to improve our cyber security behaviour and help us reduce the likelihood of a data breach, without chipping away at our time or affecting our productivity.



Why is security awareness so important in today's world?



Any business or employee can be targeted

- Cyber criminals often target employees to gain access to sensitive information
- This is due to employees being seen as the 'weak link' in the cyber security chain
- Small to medium-sized businesses are just as likely to be hit by a cyber attack
- Criminals often launch widespread and untargeted attacks, meaning anyone is a target



We all make mistakes

- Over 90% of data breaches are a result of human error, like sending an email containing sensitive data to the wrong person, sharing passwords or leaving devices unattended
- Training helps us to make smarter security decisions every day and limit human error



Phishing attacks are getting harder to spot

- Phishing is where a cyber criminal attempts to trick victims into handing over sensitive information or installing malware, often by impersonating someone else via email
- 75% of businesses experienced phishing in 2020, and 22% of data breaches involve phishing
- Regular training ensures that we can keep up and combat new phishing techniques



Comply with regulations and frameworks

- Many regulatory frameworks and compliance standards list staff security awareness training as either mandatory or best practice whilst failure to act can result in fines

How will security awareness training benefit me?



You'll help keep our employee and customer data safe



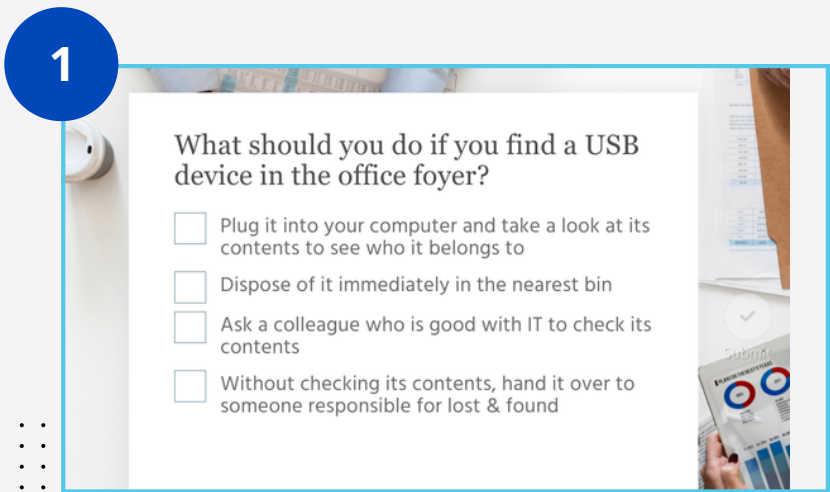
You'll learn security skills that can also be applied at home



You'll help the business avoid downtime or disruption



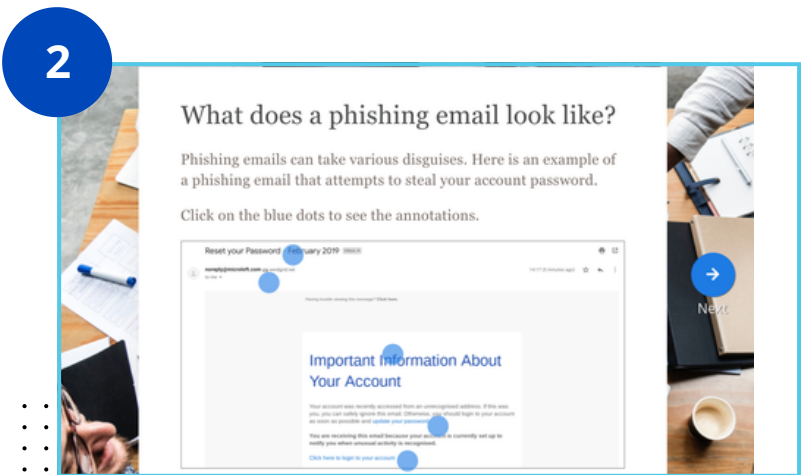
How will the training work?



You'll be sent a short Gap Analysis Questionnaire to complete

This questionnaire measures your current security knowledge and identifies areas that need improvement, such as 'Secure Passwords' or 'Phishing'. This only takes between 10-15 minutes to complete and provides a baseline for what topics you'll be trained on first.

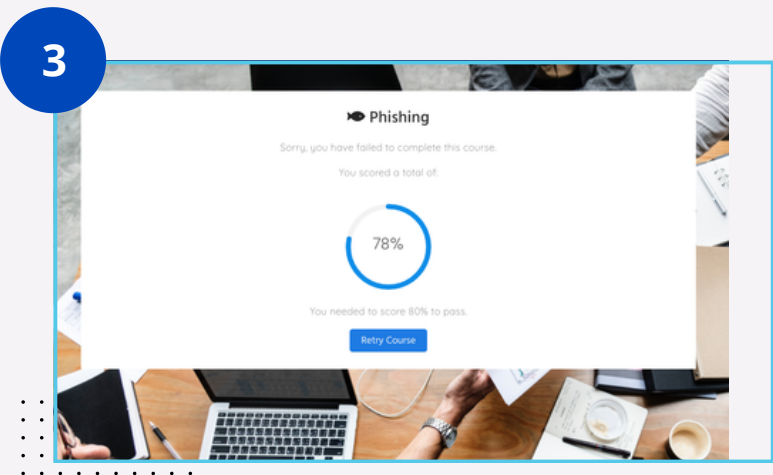
- ✓ Quick one-off questionnaire
- ✓ Measures your security knowledge
- ✓ Baselines your training journey



You'll then be sent your first security awareness course

Once your Gap Analysis results are in, you'll get an email invitation to access your first course. The course you receive first will depend on which area you scored lowest in during the Gap Analysis - e.g. 'Secure Passwords'. These courses take approximately 5-10 minutes to complete, which includes a quick quiz at the end that is used to measure how much you've learned.

- ✓ Quick 5-10 minute course
- ✓ Short recap quiz at the end
- ✓ You'll be trained on weakest areas first



You'll continue to receive regular course invitations over time

To help make sure your security behaviour is improving, you'll receive an email invite to a new course each month (although, this frequency can be changed at the business' discretion). You'll be able to complete these courses when it is convenient for you, but we recommend completing these as soon as possible to avoid them building up.

- ✓ You'll be invited to new courses over time
- ✓ Course grades and progress will be measured
- ✓ You'll see your grade at the end of each course

Frequently Asked Questions



? How do I access my courses?

You'll receive an email invitation to your courses via your work email address. Each course is emailed out to you separately over time, where you'll find a link to begin your course.

? Is course completion mandatory?

Yes, completing these courses is mandatory, as it helps us comply with various policies, regulations and frameworks, and helps protect our business from a potential data breach.

? How long do these courses take to complete?

The one-off Gap Analysis Questionnaire that you'll receive at the start of your training journey takes approximately 10-15 minutes to complete, and each course takes approximately 5-10 minutes to complete.

? What happens if I don't pass the quiz at the end of my course?

Each course requires you to get a minimum amount of questions correct in your quiz, with the minimum pass rate being 80% (unless set otherwise). If you score less than the minimum pass score, you'll simply be asked to re-start the course until you reach the set pass rate.

? How often will I receive a course?

You'll receive a minimum of one course per month, but this frequency can be increased or decreased at the discretion of the training manager/admins.

? Once I've received a course invite, how long do I have to complete it?

Once you've received your course invitation via email, you'll be able to complete the course at a time convenient for you. Although, it is expected that you complete these courses as soon as possible to keep your training regular, effective and to avoid courses building up.

? What do the courses look like?

Your courses include a mixture of textual, video and interactive content to help keep them engaging, and unnecessary tech jargon has been avoided to make sure the courses are easy to understand.

Your Cyber Awareness Toolkit



Tips for keeping safe in the workplace

Cyber Threats and Risks

As technology continues to advance and more work is done remotely, the risks of cyber threats and attacks have become increasingly prevalent. Cybersecurity is no longer just the responsibility of IT professionals, but also of every employee in a business. Whether you're working from home, travelling, or working in the office, it's important to be aware of the different types of cyber threats and how to protect yourself and your organisation from them.

Common Cyber Threats



Phishing: This involves tricking employees into sharing sensitive information, such as login credentials or personal data, through email or other forms of digital communication.



Malware: Malicious software can infect an employee's device through email attachments or unsecured websites, allowing hackers to gain access to sensitive data or even take control of the device.



Ransomware: This type of malware encrypts an employee's files and demands payment in exchange for the decryption key, making it impossible for the employee to access their own data.



Social engineering: This involves manipulating employees into divulging sensitive information or performing actions that compromise security through tactics like impersonation, pretexting, or baiting.

The importance of good password hygiene



The humble password is the first line of defence against unauthorised access to sensitive information and systems. Weak or easily guessable passwords can be easily cracked by hackers, allowing them to gain access to an employee's account or even an entire system, putting the entire business at risk.

Strong passwords, changing passwords regularly, and not sharing passwords, can help prevent unauthorised access and protect sensitive information from cyber threats. Passwords that are easy to guess, shared among coworkers, or reused across multiple accounts can compromise an organization's security and put it at risk for data breaches, financial loss, or damage to its reputation.








Tips for perfect password management!

- ✓ **Use strong passwords:** Your password should be at least 12 characters long and include a mix of upper and lowercase letters, numbers, and symbols. Avoid using common words or phrases, and don't use the same password for multiple accounts.
- ✓ **Use a password manager:** A password manager can generate and store strong passwords for you, making it easier to keep track of them without having to remember each one.
- ✓ **Enable multi-factor authentication:** Multi-factor authentication adds an extra layer of security to your accounts by requiring a second form of verification, such as a code sent to your phone or email.
- ✓ **Change passwords regularly:** It's a good idea to change your passwords every three to six months, especially for accounts that contain sensitive information.
- ✓ **Don't share passwords:** Never share your passwords with anyone, including coworkers or family members.
- ✓ **Be careful where you enter your password:** Always make sure you're entering your password on a secure website or app, and avoid entering your password on public Wi-Fi networks or other unsecured connections.
- ✓ **Be wary of phishing scams:** Hackers may try to trick you into giving up your password through phishing emails or fake websites. Always verify the authenticity of the website or email before entering your password.

Internet and Email Security



It's important to be vigilant when it comes to safe internet and email use. As an employee, it is essential to protect sensitive information, prevent cyber attacks, and maintain a secure network when accessing your company email and browsing online.

-  **Be careful with phishing emails:** Phishing emails are emails that pretend to be from a legitimate source but are actually trying to trick you into revealing sensitive information. Be cautious of emails that ask you to click on a link or download an attachment from an unknown source.
-  **Keep your software up-to-date:** Keep your computer, operating system, and software applications up-to-date with the latest security patches and updates. This will help protect your system against known vulnerabilities and exploits.
-  **Log out of accounts:** Always log out of your accounts when you finish using them, especially if you are using a public or shared computer.
-  **Use antivirus software:** Install reputable antivirus software on your computer and keep it up-to-date. This will help protect your system from malware and viruses.
-  **Avoid public Wi-Fi:** Public Wi-Fi networks are often unsecured and can be used by hackers to intercept your online activity. If possible, avoid using public Wi-Fi to access sensitive information.
-  **Use encryption:** Encryption is the process of converting data into a code to prevent unauthorized access. Use encryption tools like virtual private networks (VPNs) and secure email services to protect your online communication.
-  **Avoid downloading unauthorised software:** Download software only from trusted sources and check with your IT team before you hit download, if you are unsure.

Learn how to spot a phishing email



1 Suspicious Sender

Cybercriminals use various spoofing techniques to trick users into believing an email is legitimate. Check the domain closely for close 'cousin' domains. Be cautious when reading email on your mobile device, as only the display name may be visible even if the email is bogus.

2 Subject Line & Tone

Enticing, urgent, or threatening language is commonly used to encourage the recipient to take immediate action. Evoking a sense of curiosity, greed, or fear is a common tactic among phishing schemes.

3 Greeting

Phishers often send out mass emails to gather information, so they use generic greetings. But, sophisticated phishers personalise their emails with information such as names, email addresses, and even breached passwords.

4 Errors

Read the email carefully. Grammatical errors are an obvious red flag, but sophisticated hackers do not make glaring errors. Instead, there may be more subtle mistakes, such as minor spacing issues or use of symbols instead of words. In some cases, there will be no errors.

5 Links

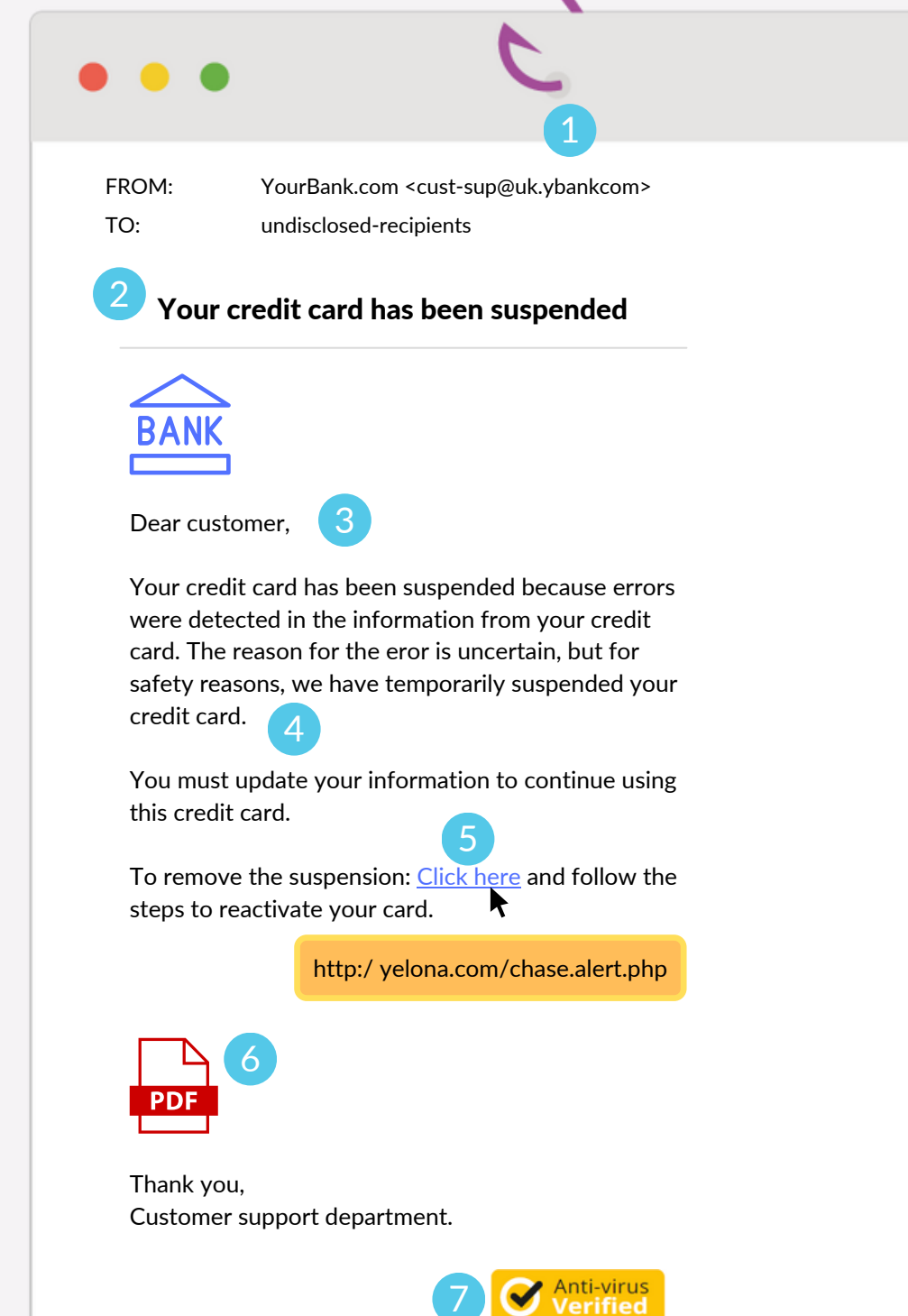
Before clicking, hover over the link to see the URL of where the link actually leads, and beware of link shorteners, such as Bitly or Ti-nnyURL. Keep in mind that phishing emails can include clean URLs in addition to the phishing URL to trick users and email filters.

6 Attachments

Be wary of emails that include attachments. Phishing emails may include a link in an attachment, rather than the body of the email, to avoid detection by an email filter.

7 Images

Cybercriminals can easily replicate brand logos, images, and badges in emails and webpages that are indistinguishable from the real thing. Consider all the above factors as you decide whether to click.



Social Engineering



Social engineering refers to the use of psychological manipulation to trick or deceive individuals or organisations into divulging sensitive information, providing access to confidential systems, or performing actions that would otherwise be against their best interests.

Social engineering techniques can take many forms, including phishing emails, pretexting, baiting, and quid pro quo schemes. These tactics often rely on exploiting people's natural tendencies towards trust, helpfulness, curiosity, or fear.

Social engineering attacks can have serious consequences, including data breaches, financial losses, identity theft, and even physical harm. As such, it is important to be aware of the risks and to take steps to protect oneself from these types of attacks.

- ✓ **Be suspicious of unsolicited emails or phone calls:** If you receive an unexpected email or phone call asking for sensitive information or requesting that you take a particular action, be suspicious. Verify the request by checking with the sender or caller using a known, verified contact method before responding.
- ✓ **Be cautious of social media interactions:** Be careful when accepting friend requests or opening messages from people you don't know on social media. Cybercriminals often use social media to gain information about their targets.
- ✓ **Don't overshare personal or company information:** Be careful not to overshare personal or company information on social media or in public forums, as this information can be used by cybercriminals to craft more convincing social engineering attacks.
- ✓ **Don't click on links or download attachments from unknown sources:** Never click on links or download attachments from unknown sources, as they could contain malware or other malicious software that could compromise your system or network.

Physical Security



Physical security breaches can lead to compromised data and unauthorised access to company networks. For example, if an employee's laptop is stolen and contains sensitive company information, that information may fall into the wrong hands. Additionally, if an unauthorised individual gains access to a secure area, they may be able to physically access company servers or other devices, allowing them to compromise data or install malware.

Don't share your access codes or keys: Do not give your access codes or keys to anyone, and never leave them lying around. This includes not sharing your password, access cards, or any other device that allows access to restricted areas.

Be aware of your surroundings: Always be aware of what's happening around you. Notice if there are people around who shouldn't be there, or if someone is acting suspiciously.

Lock up valuables: Keep any valuable items, such as laptops or smartphones, locked up or in a secure location when not in use.

Follow proper entry and exit procedures: Follow proper entry and exit procedures when entering or leaving the building, including signing in and out, using access cards, and following any other security measures in place.

Report suspicious behaviour: If you notice any suspicious behaviour, report it to the appropriate person, such as a supervisor or security personnel.

Don't leave your workstation unattended: Never leave your workstation unattended, especially if it is logged in or contains sensitive information.



Incident Reporting

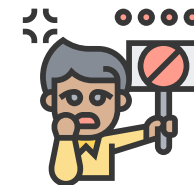
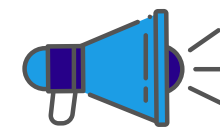


Call it Out

Promptly reporting incidents to your IT team or line manager is crucial to minimising the potential harm caused by cyber incidents. Cyber incidents can cause significant damage, including financial losses, reputational damage, and legal consequences.

Early detection and reporting of a cyber incident can enable your IT team to respond quickly, contain the threat, and prevent further damage. Delaying reporting can escalate the incident, making it harder to mitigate the damage and increasing the risk of data loss or theft.

By reporting incidents promptly, you can help your organisation to safeguard its assets, maintain its reputation, and prevent any long-term damage to its operations. Remember, a quick and effective response can make all the difference in minimising the impact of a cyber incident.



Cyber attacks can be difficult to spot, so don't hesitate to **ask for further guidance or support when something feels suspicious or unusual.**

Report attacks as soon as possible - don't assume that someone else will do it. Even if you've done something (such as clicked on a bad link), always report what's happened.

Don't be afraid to challenge policies or processes that make your job difficult. Security that gets in the way of people doing their jobs, doesn't work.



Staying safe in a digital world

If you need to report an incident, or are looking for help and advice about the security awareness programme, contact us:



servicedesk.soconnect.co.uk



servicedesk@soconnect.co.uk



0333 240 1824 (opt.1)