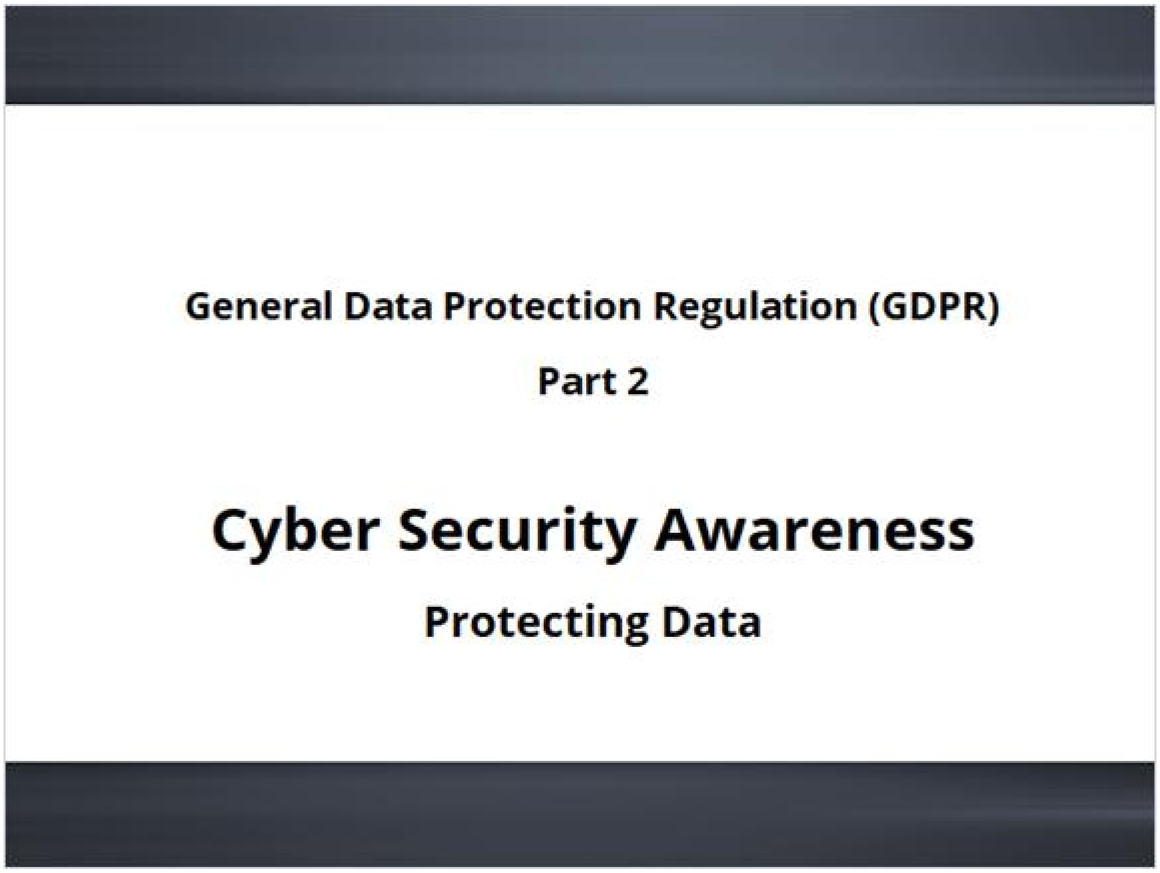
Cyber Security Awareness

1. Untitled Scene

1.1 Front Page



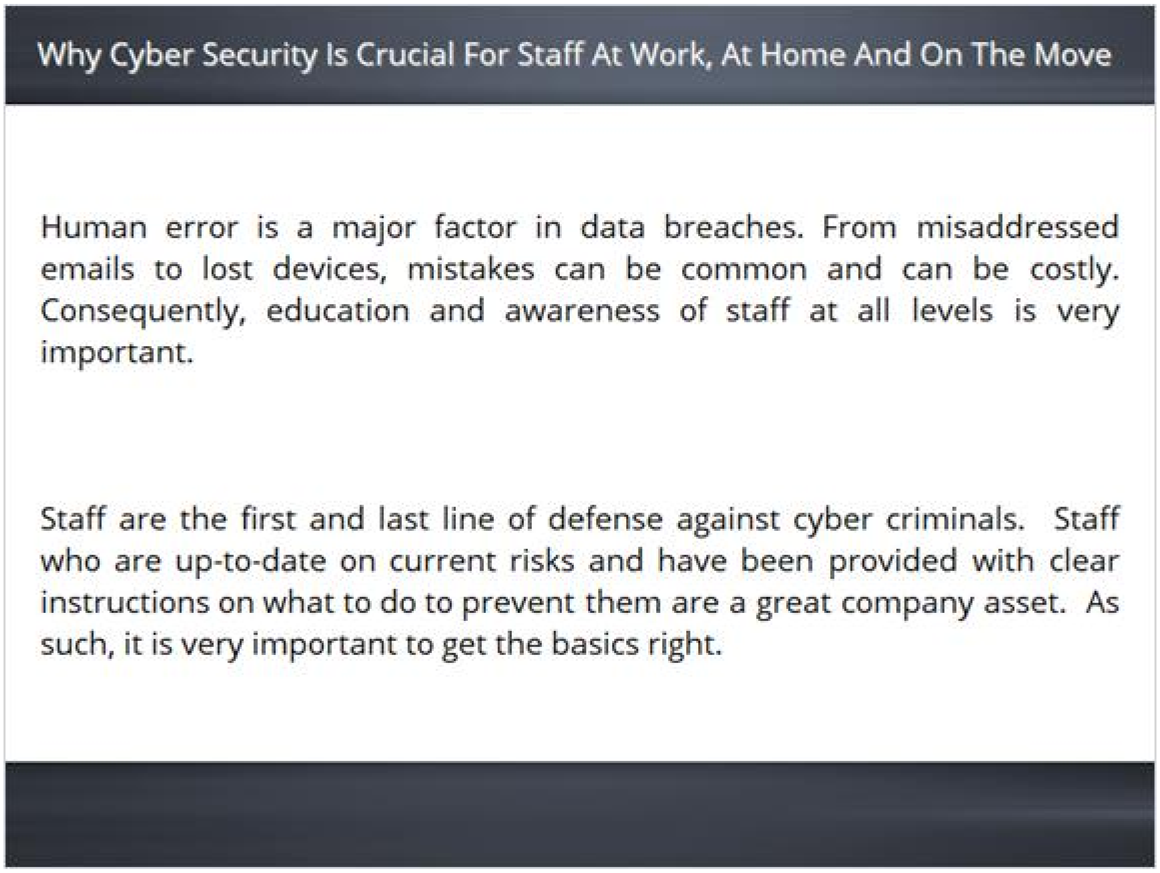
General Data Protection Regulation (GDPR)

Part 2

Cyber Security Awareness

Protecting Data

1.2 Why Cyber Security Is Crucial For Staff At Work, At Home And On The Move

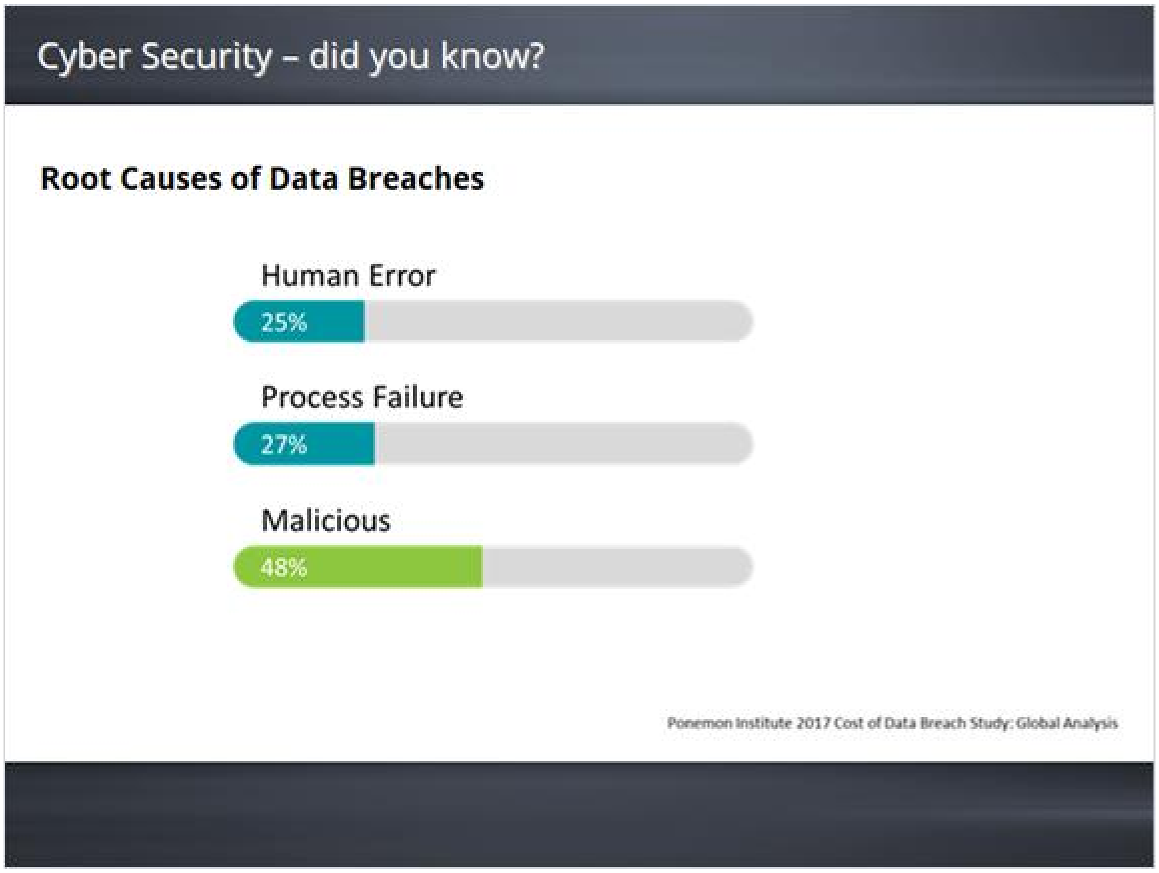


Why Cyber Security Is Crucial For Staff At Work, At Home And On The Move

Human error is a major factor in data breaches. From misaddressed emails to lost devices, mistakes can be common and can be costly. Consequently, education and awareness of staff at all levels is very important.

Staff are the first and last line of defense against cyber criminals. Staff who are up-to-date on current risks and have been provided with clear instructions on what to do to prevent them are a great company asset. As such, it is very important to get the basics right.

1.3 Cyber Security – did you know?



Cyber Security – did you know?

Root Causes of Data Breaches

Human Error

25%

Process Failure

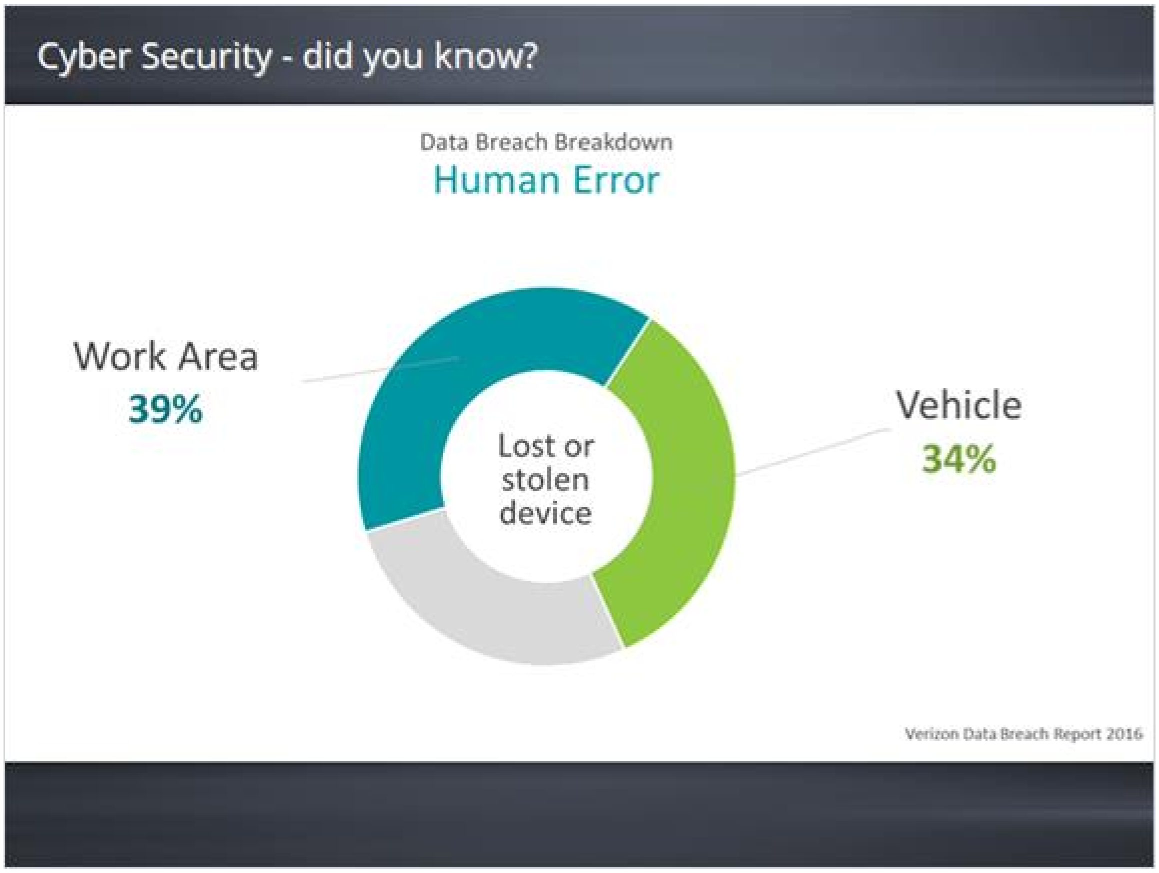
27%

Malicious

48%

Ponemon Institute 2017 Cost of Data Breach Study: Global Analysis

1.4 Cyber Security - did you know?



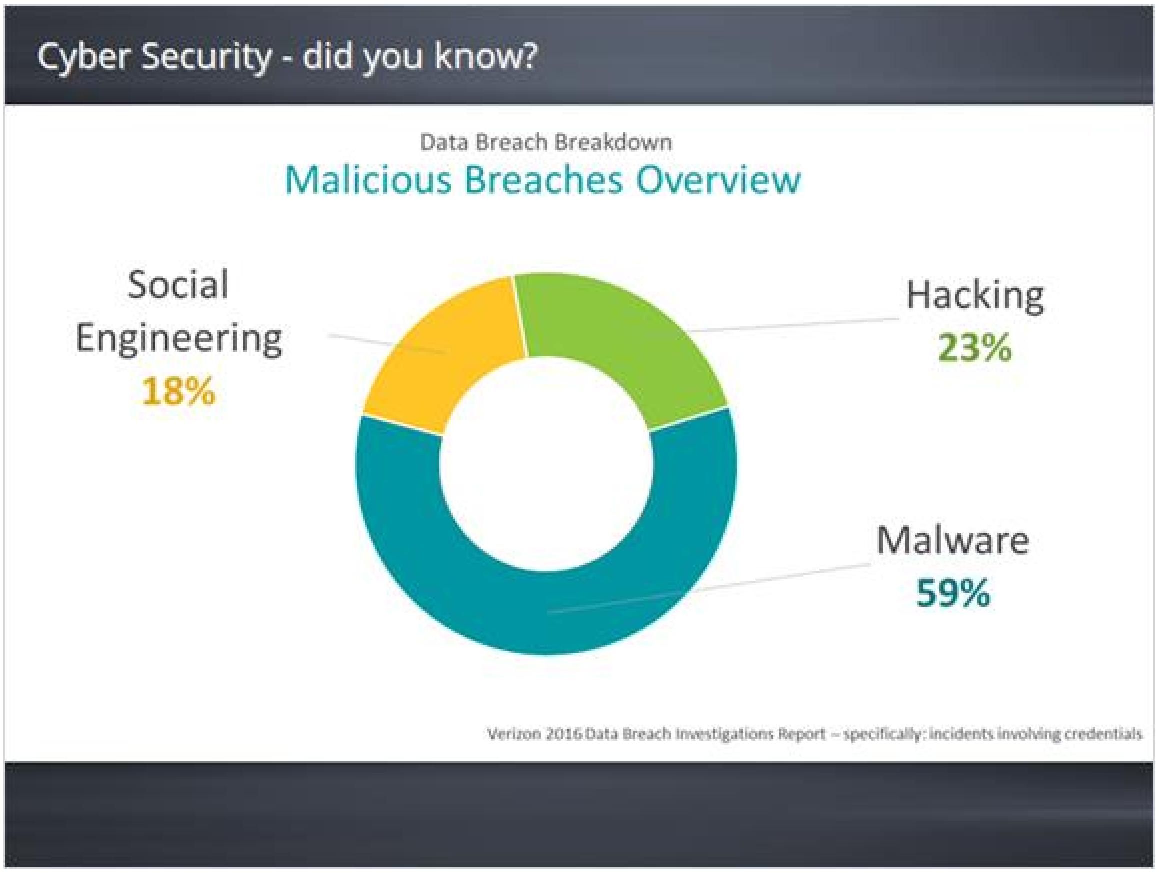
Cyber Security - did you know?

Data Breach Breakdown

Human Error

Verizon Data Breach Report 2016

1.5 Cyber Security - did you know?



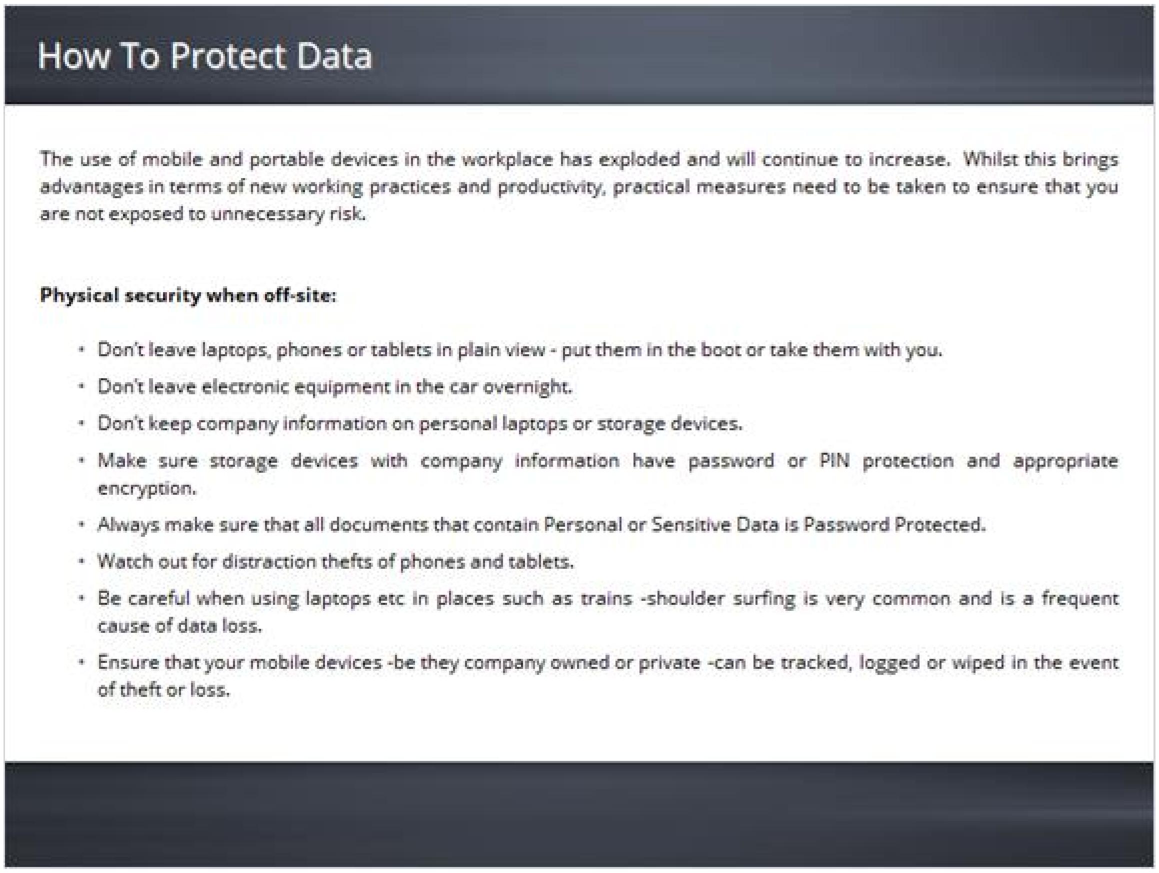
Cyber Security - did you know?

Data Breach Breakdown

Malicious Breaches Overview

Verizon 2016 Data Breach Investigations Report – specifically: incidents involving credentials

1.6 How To Protect Data



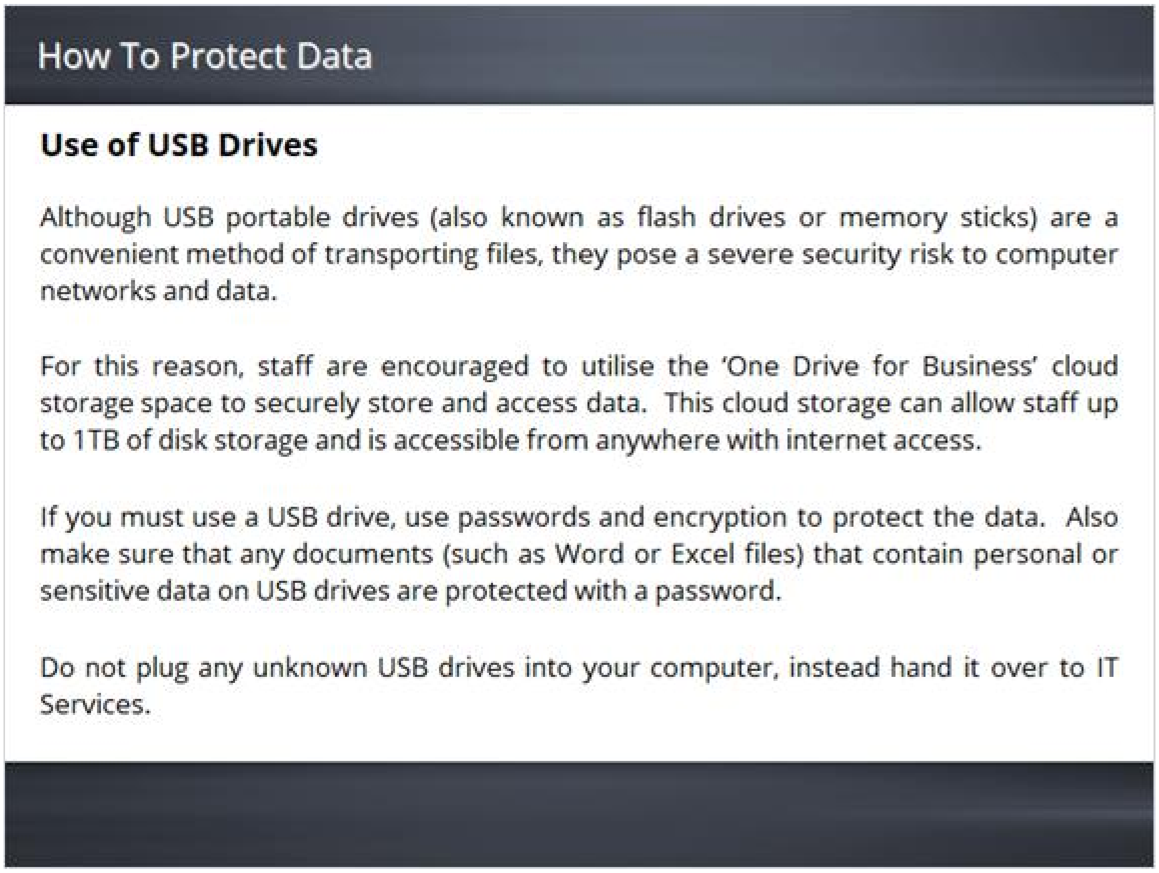
How To Protect Data

The use of mobile and portable devices in the workplace has exploded and will continue to increase. Whilst this brings advantages in terms of new working practices and productivity, practical measures need to be taken to ensure that you are not exposed to unnecessary risk.

Physical security when off-site:

- Don't leave laptops, phones or tablets in plain view - put them in the boot or take them with you.
- Don't leave electronic equipment in the car overnight.
- Don't keep company information on personal laptops or storage devices.
- Make sure storage devices with company information have password or PIN protection and appropriate encryption.
- Always make sure that all documents that contain Personal or Sensitive Data is Password Protected.
- Watch out for distraction thefts of phones and tablets.
- Be careful when using laptops etc in places such as trains -shoulder surfing is very common and is a frequent cause of data loss.
- Ensure that your mobile devices -be they company owned or private -can be tracked, logged or wiped in the event of theft or loss.

1.7 How To Protect Data



How To Protect Data

Use of USB Drives

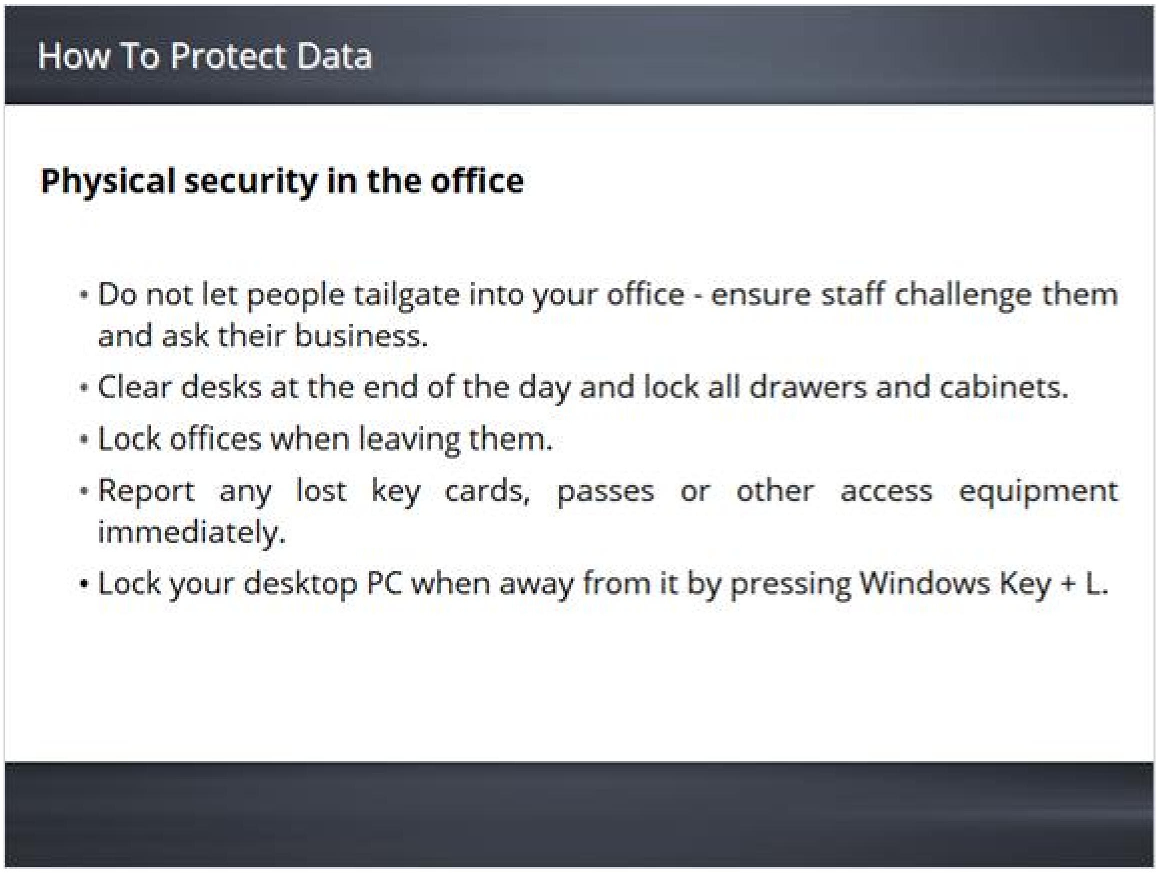
Although USB portable drives (also known as flash drives or memory sticks) are a convenient method of transporting files, they pose a severe security risk to computer networks and data.

For this reason, staff are encouraged to utilise the 'One Drive for Business' cloud storage space to securely store and access data. This cloud storage can allow staff up to 1TB of disk storage and is accessible from anywhere with internet access.

If you must use a USB drive, use passwords and encryption to protect the data. Also make sure that any documents (such as Word or Excel files) that contain personal or sensitive data on USB drives are protected with a password.

Do not plug any unknown USB drives into your computer, instead hand it over to IT Services.

1.8 How To Protect Data

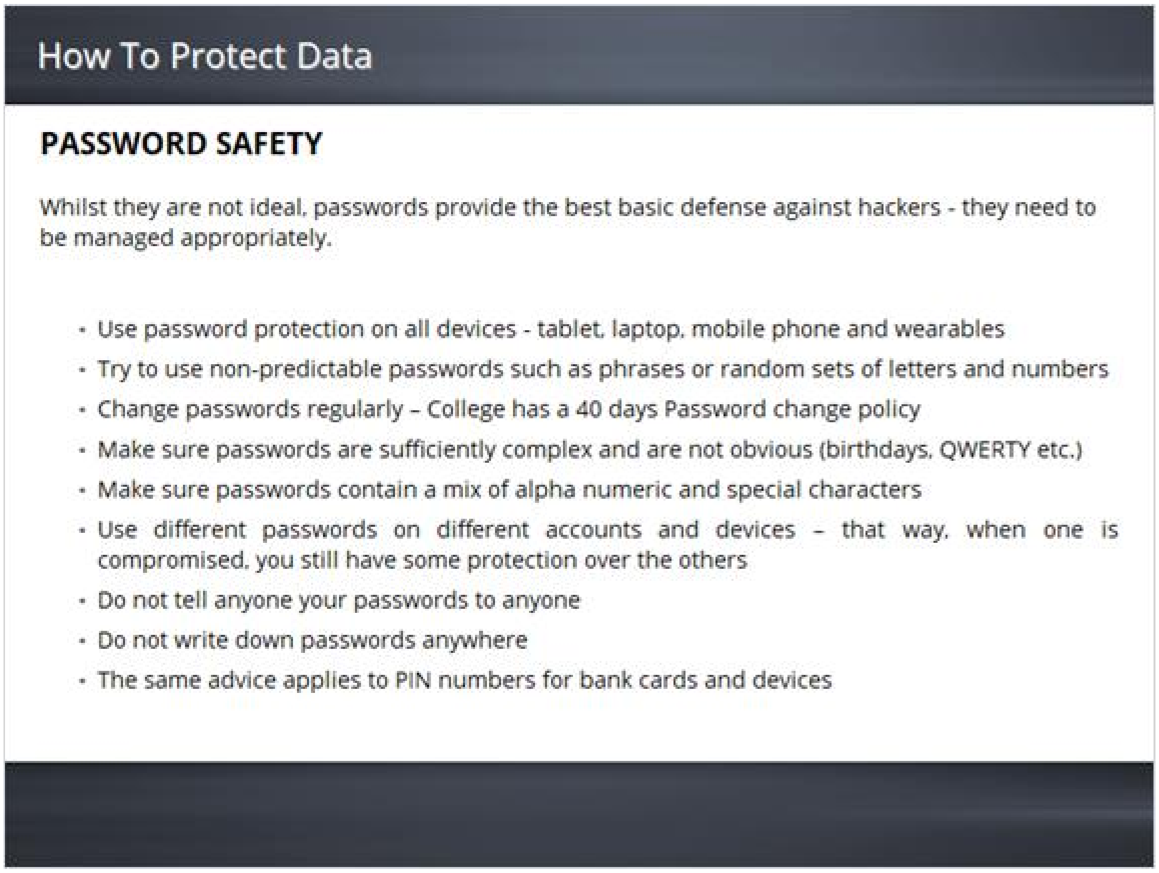


How To Protect Data

Physical security in the office

- Do not let people tailgate into your office - ensure staff challenge them and ask their business.
- Clear desks at the end of the day and lock all drawers and cabinets.
- Lock offices when leaving them.
- Report any lost key cards, passes or other access equipment immediately.
- Lock your desktop PC when away from it by pressing Windows Key + L.

1.9 How To Protect Data



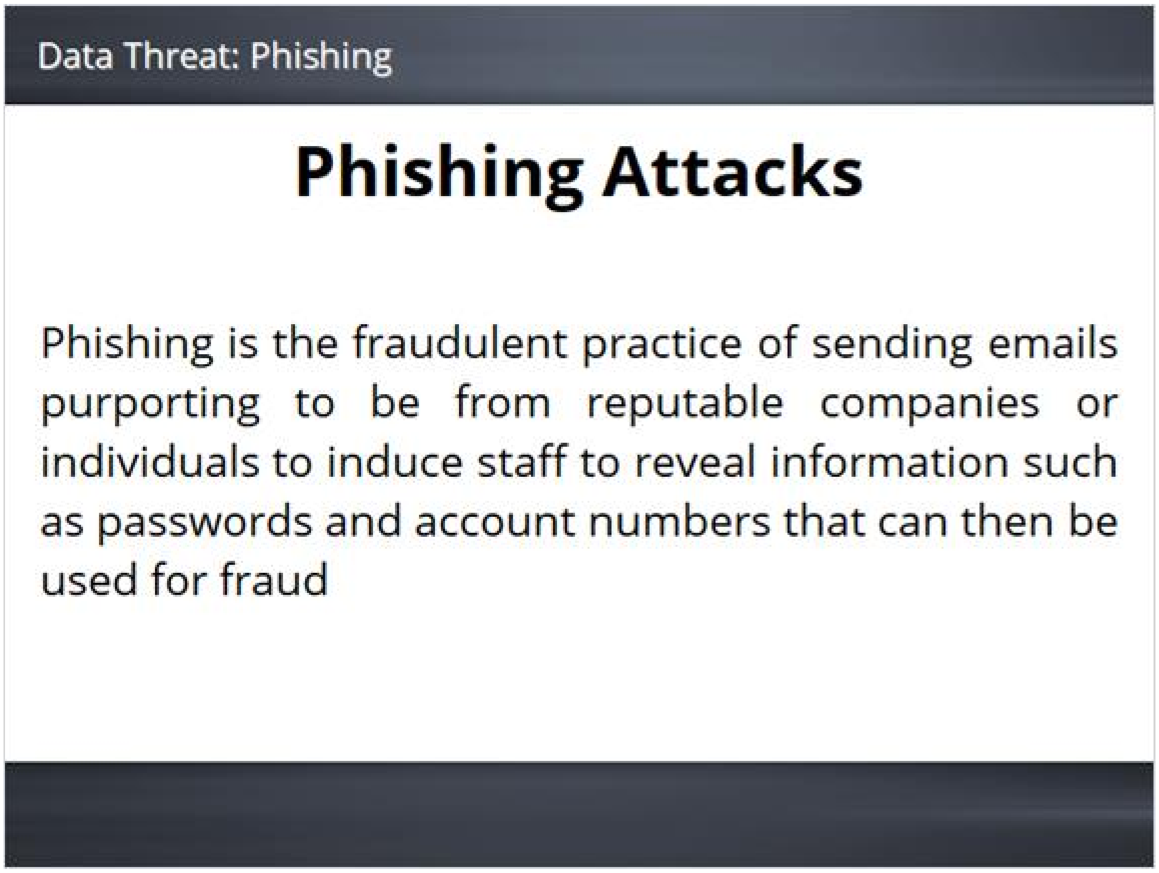
How To Protect Data

PASSWORD SAFETY

Whilst they are not ideal, passwords provide the best basic defense against hackers - they need to be managed appropriately.

- Use password protection on all devices - tablet, laptop, mobile phone and wearables
- Try to use non-predictable passwords such as phrases or random sets of letters and numbers
- Change passwords regularly – College has a 40 days Password change policy
- Make sure passwords are sufficiently complex and are not obvious (birthdays, QWERTY etc.)
- Make sure passwords contain a mix of alpha numeric and special characters
- Use different passwords on different accounts and devices – that way, when one is compromised, you still have some protection over the others
- Do not tell anyone your passwords to anyone
- Do not write down passwords anywhere
- The same advice applies to PIN numbers for bank cards and devices

1.10 Data Threat: Phishing

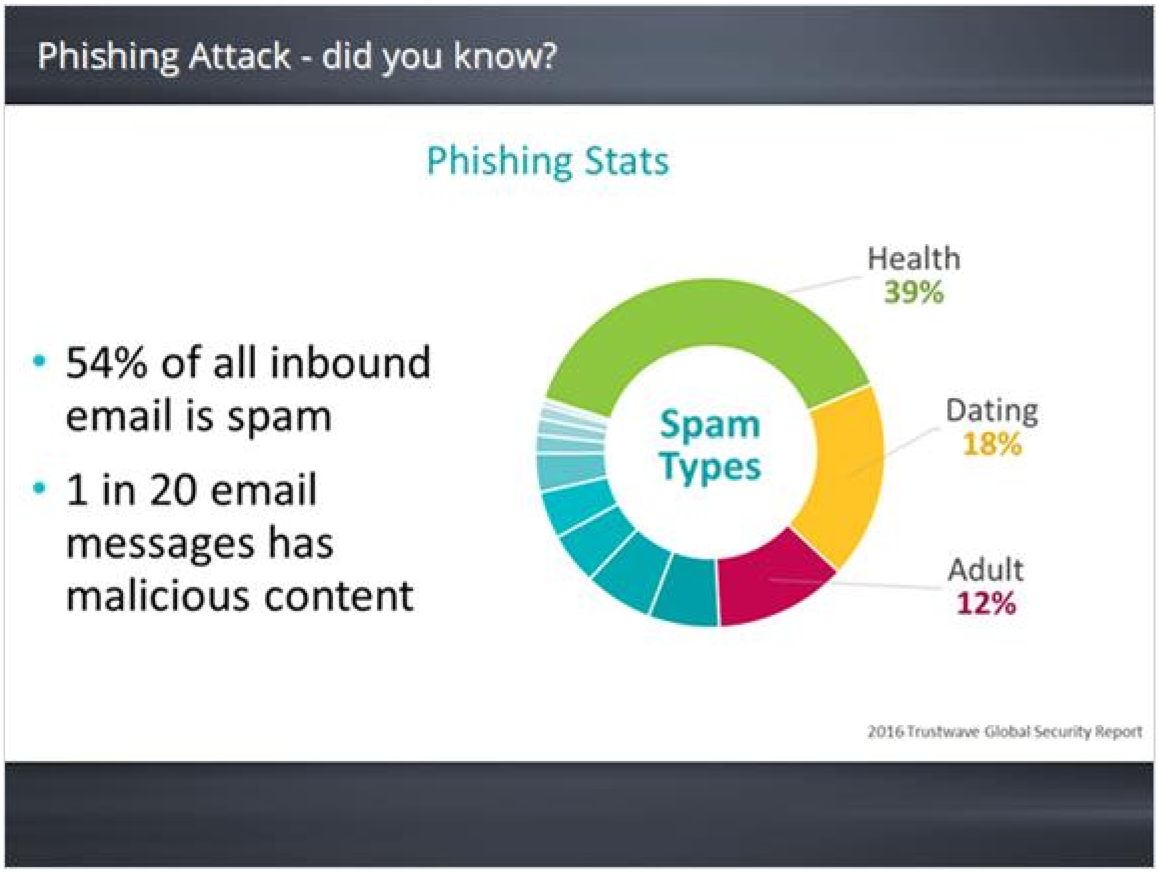


Data Threat: Phishing

Phishing Attacks

Phishing is the fraudulent practice of sending emails purporting to be from reputable companies or individuals to induce staff to reveal information such as passwords and account numbers that can then be used for fraud

1.11 Phishing Attack - did you know?



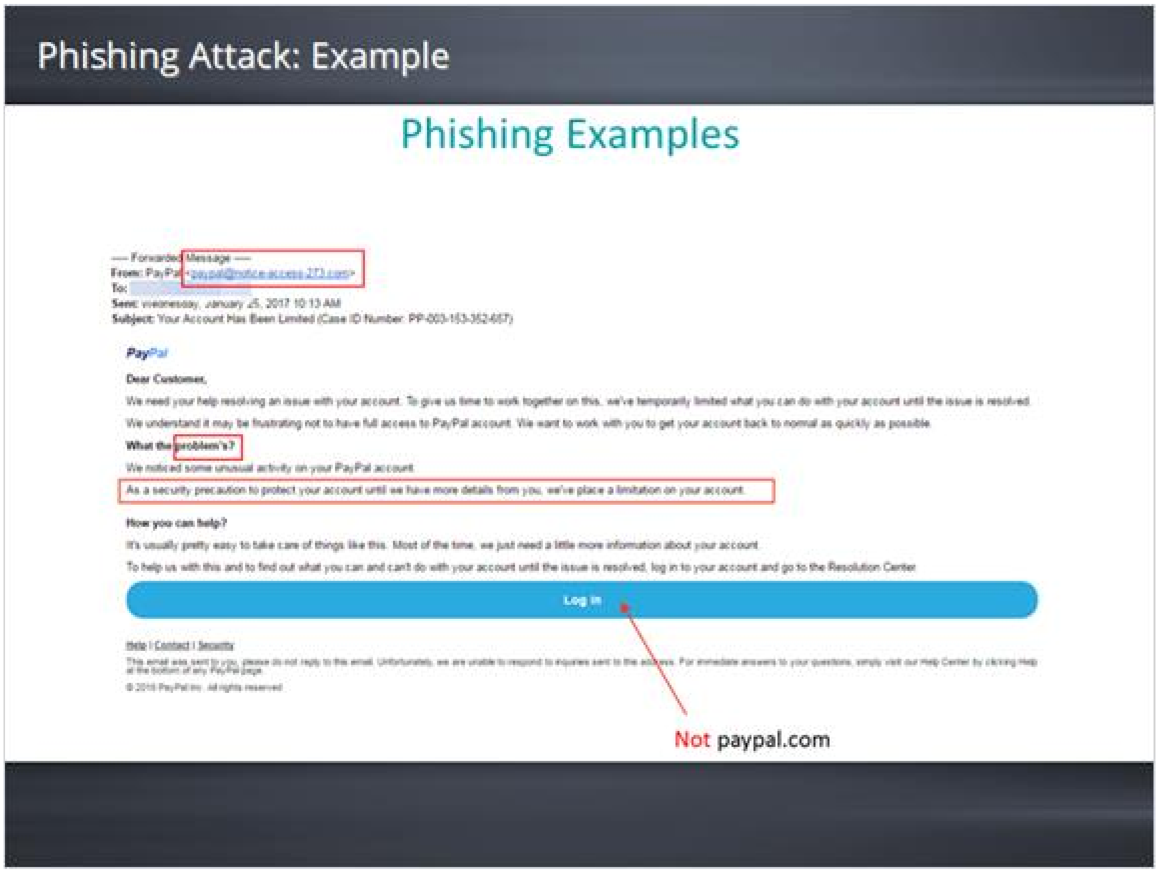
Phishing Attack - did you know?

Phishing Stats

- 54% of all inbound email is spam
- 1 in 20 email messages has malicious content

2016 Trustwave Global Security Report

1.12 Phishing Attack: Example



Phishing Attack: Example

Phishing Examples

---- Forwarded Message ----
From: PayPal <paypal@notice-access-273.com>
To: [redacted]
Sent: Wednesday, January 25, 2017 10:13 AM
Subject: Your Account Has Been Limited (Case ID Number: PP-003-153-352-657)

Dear Customer,

We need your help resolving an issue with your account. To give us time to work together on this, we've temporarily limited what you can do with your account until the issue is resolved.

We understand it may be frustrating not to have full access to PayPal account. We want to work with you to get your account back to normal as quickly as possible.

What the problem's?

We noticed some unusual activity on your PayPal account.

As a security precaution to protect your account until we have more details from you, we've place a limitation on your account.

How you can help?

It's usually pretty easy to take care of things like this. Most of the time, we just need a little more information about your account.

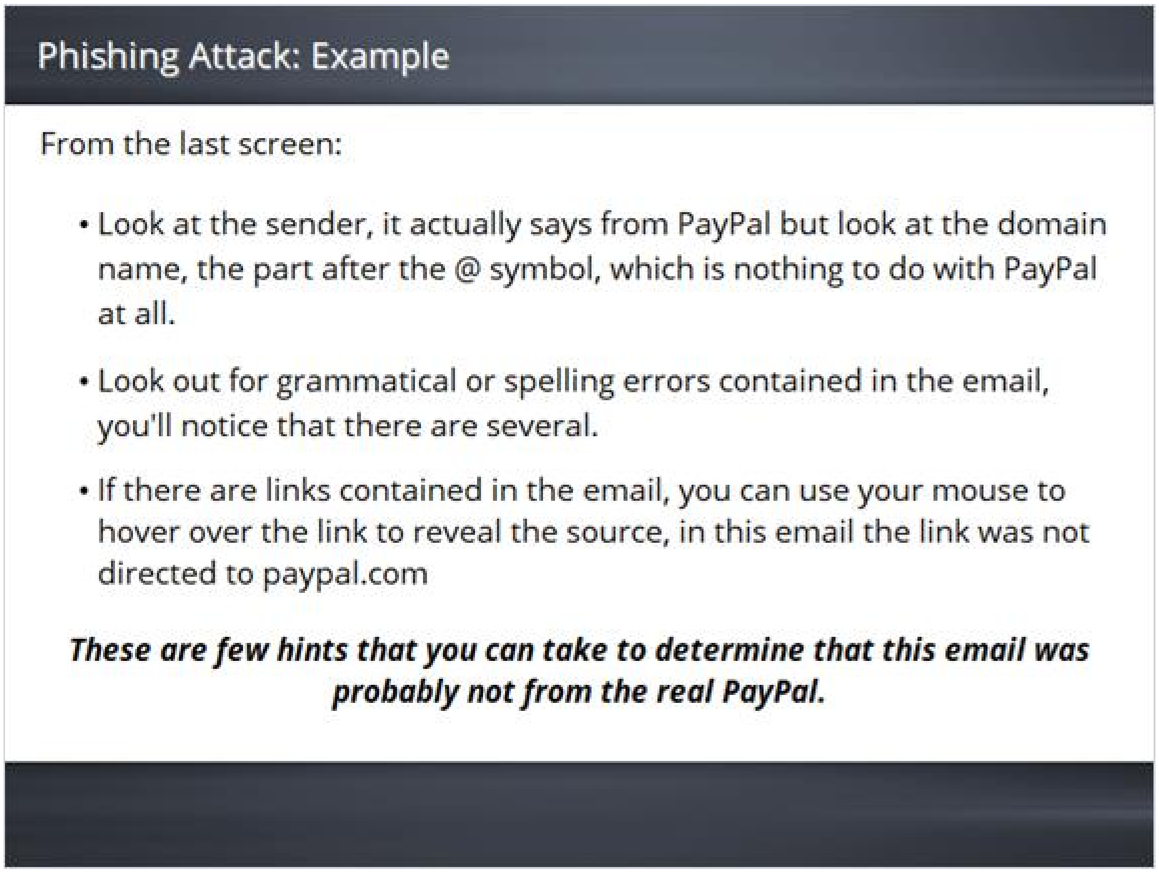
To help us with this and to find out what you can and can't do with your account until the issue is resolved, log in to your account and go to the Resolution Center.

This email was sent to you, please do not reply to this email. Unfortunately, we are unable to respond to inquiries sent to this address. For immediate answers to your questions, simply visit our Help Center by clicking Help at the bottom of any PayPal page.

© 2016 PayPal Inc. All rights reserved.

Not paypal.com

1.13 Phishing Attack: Example



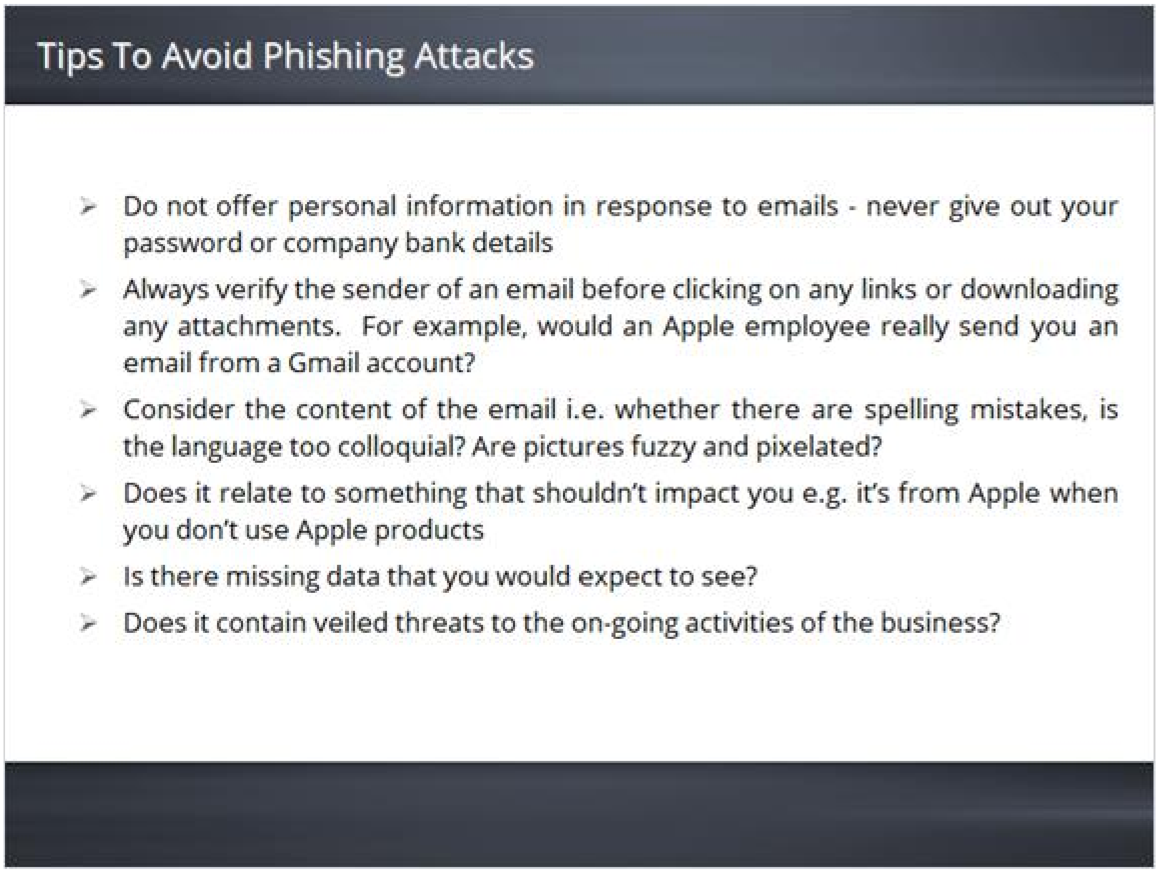
Phishing Attack: Example

From the last screen:

- Look at the sender, it actually says from PayPal but look at the domain name, the part after the @ symbol, which is nothing to do with PayPal at all.
- Look out for grammatical or spelling errors contained in the email, you'll notice that there are several.
- If there are links contained in the email, you can use your mouse to hover over the link to reveal the source, in this email the link was not directed to paypal.com

These are few hints that you can take to determine that this email was probably not from the real PayPal.

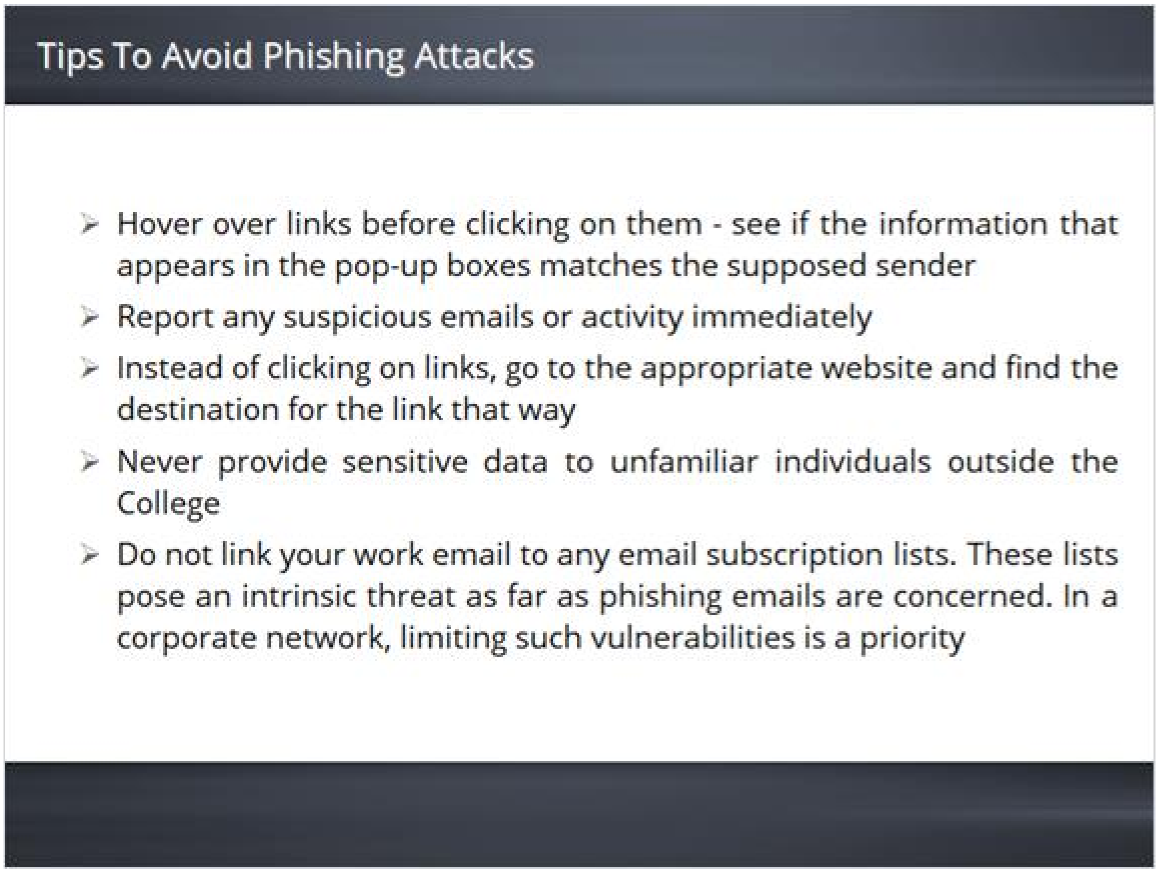
1.14 Tips To Avoid Phishing Attacks



Tips To Avoid Phishing Attacks

- Do not offer personal information in response to emails - never give out your password or company bank details
- Always verify the sender of an email before clicking on any links or downloading any attachments. For example, would an Apple employee really send you an email from a Gmail account?
- Consider the content of the email i.e. whether there are spelling mistakes, is the language too colloquial? Are pictures fuzzy and pixelated?
- Does it relate to something that shouldn't impact you e.g. it's from Apple when you don't use Apple products
- Is there missing data that you would expect to see?
- Does it contain veiled threats to the on-going activities of the business?

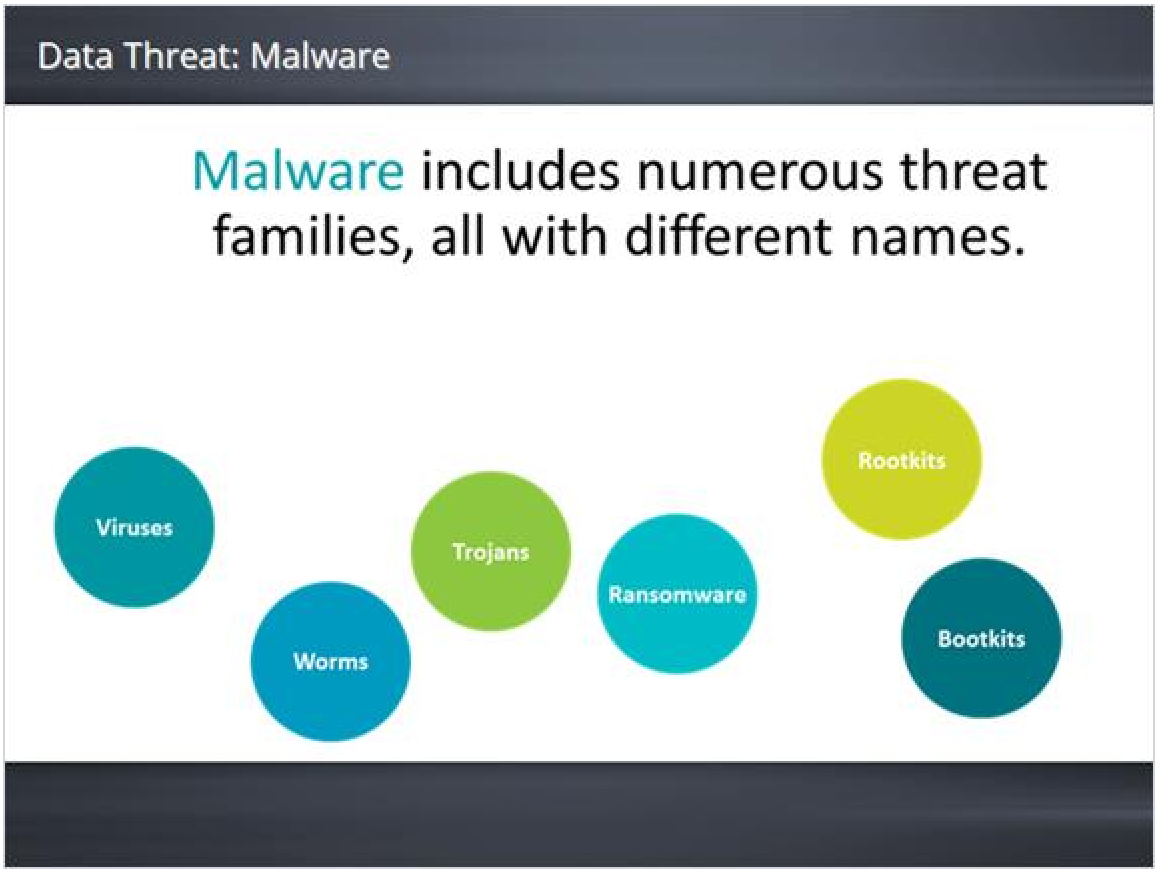
1.15 Tips To Avoid Phishing Attacks



Tips To Avoid Phishing Attacks

- Hover over links before clicking on them - see if the information that appears in the pop-up boxes matches the supposed sender
- Report any suspicious emails or activity immediately
- Instead of clicking on links, go to the appropriate website and find the destination for the link that way
- Never provide sensitive data to unfamiliar individuals outside the College
- Do not link your work email to any email subscription lists. These lists pose an intrinsic threat as far as phishing emails are concerned. In a corporate network, limiting such vulnerabilities is a priority

1.16 Data Threat: Malware

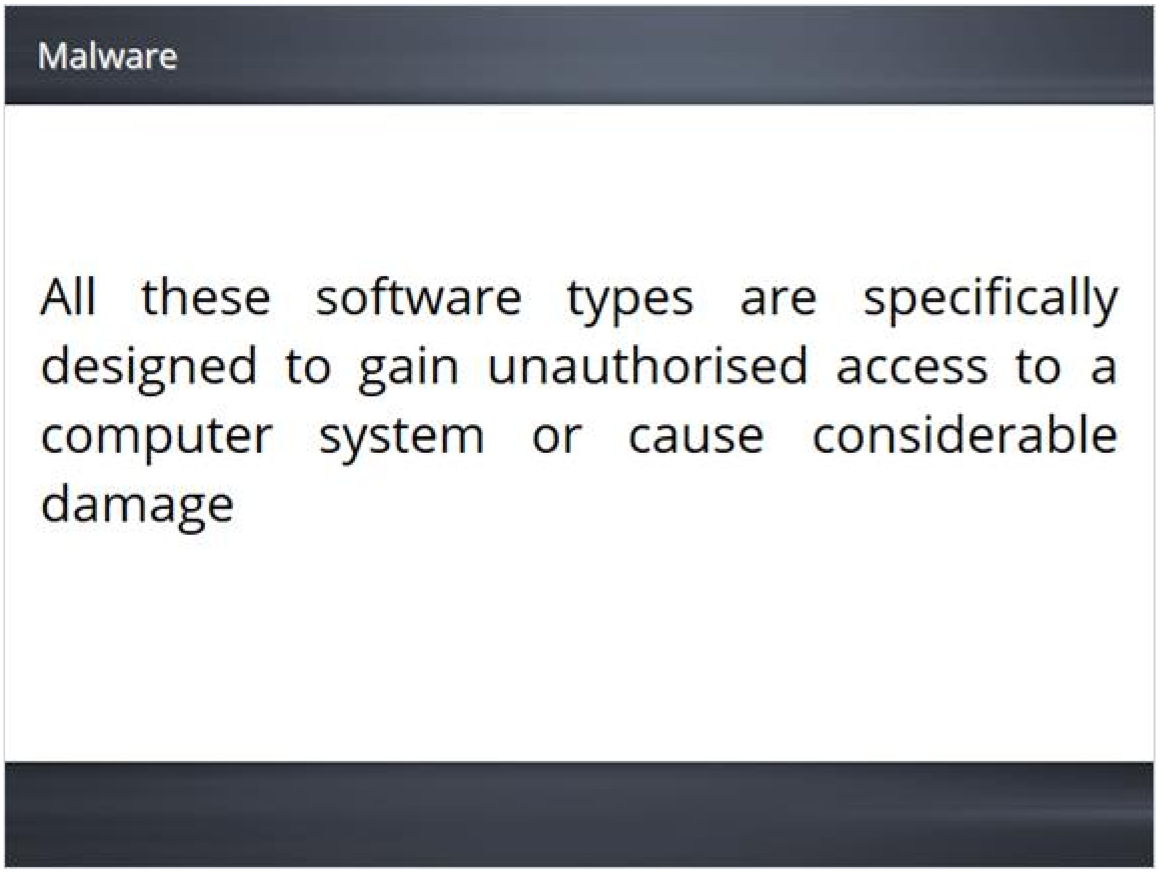


Data Threat: Malware

Malware includes numerous threat families, all with different names.

Viruses
Worms
Trojans
Ransomware
Rootkits
Bootkits

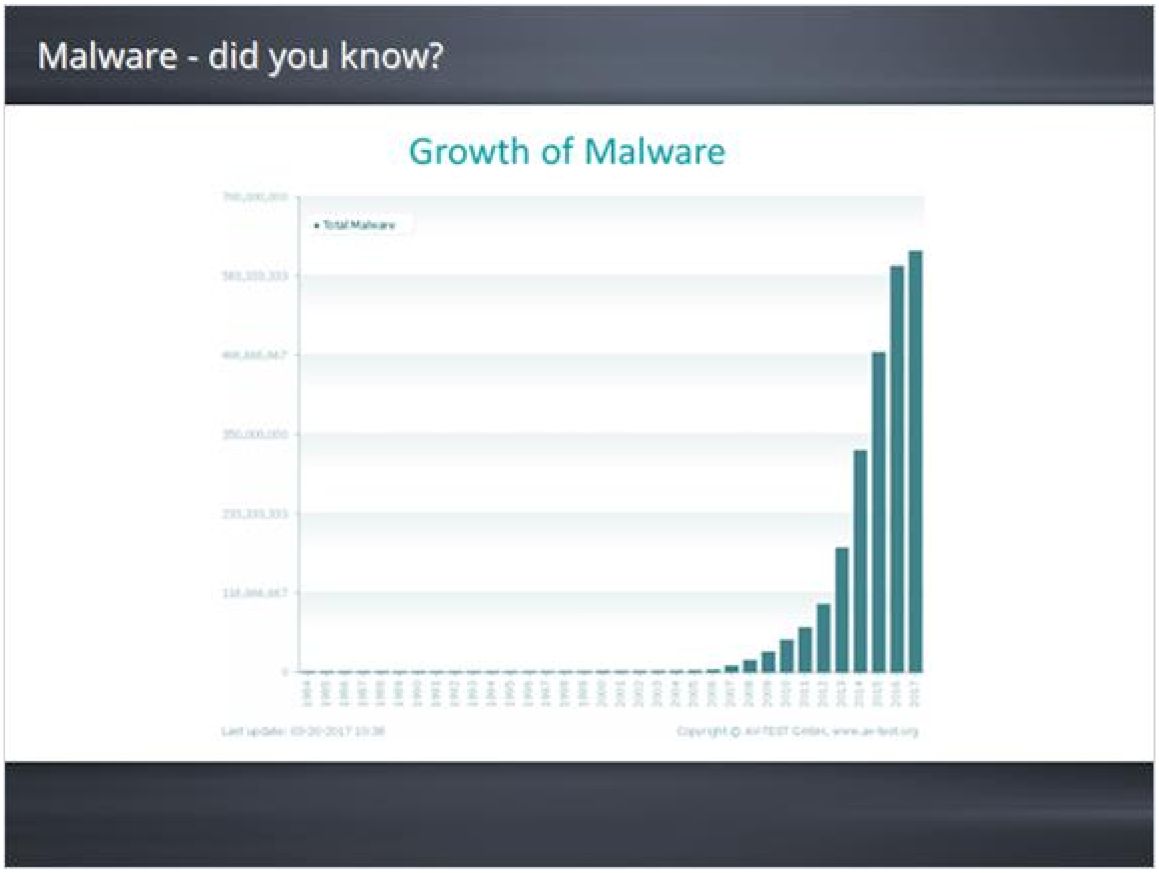
1.17 Malware



Malware

All these software types are specifically designed to gain unauthorised access to a computer system or cause considerable damage

1.18 Malware - did you know?



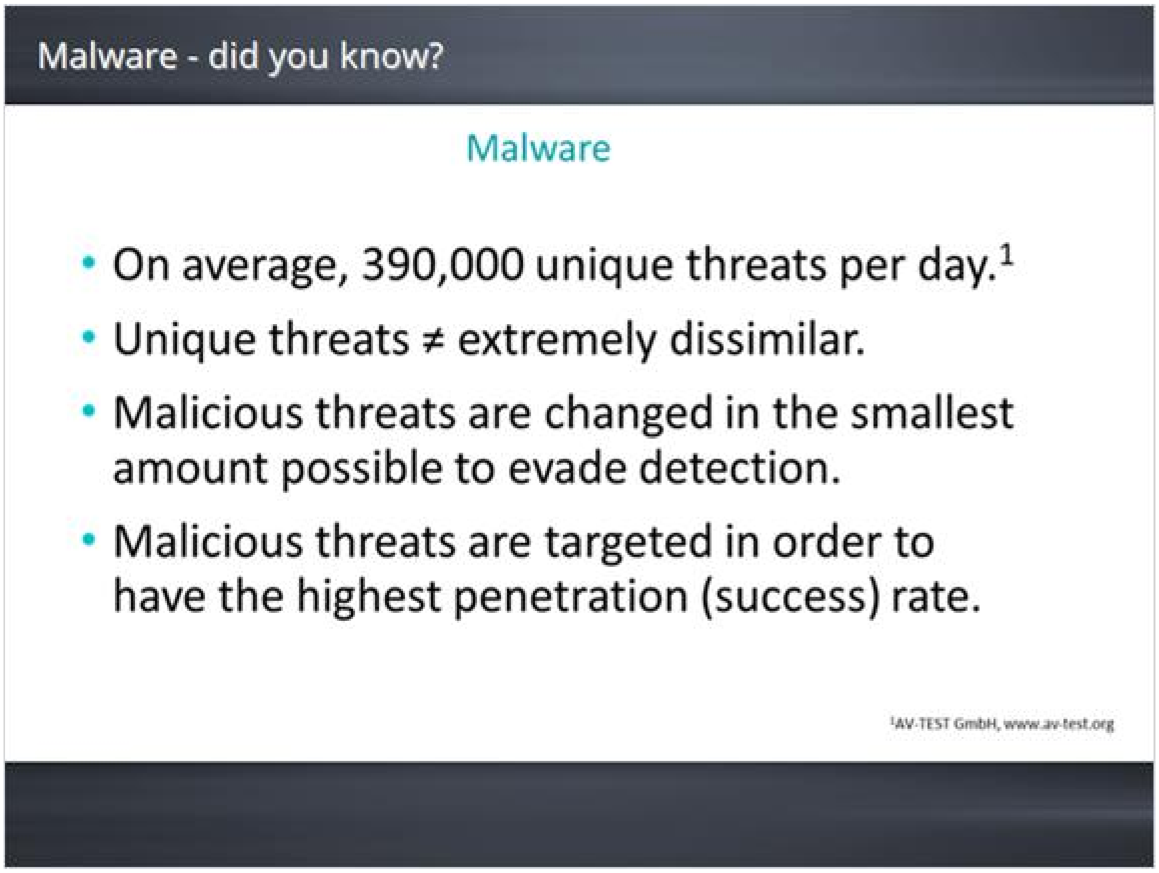
Malware - did you know?

Growth of Malware

Last update: 03-20-2017 10:38

Copyright © AV-TEST GmbH, www.av-test.org

1.19 Malware - did you know?



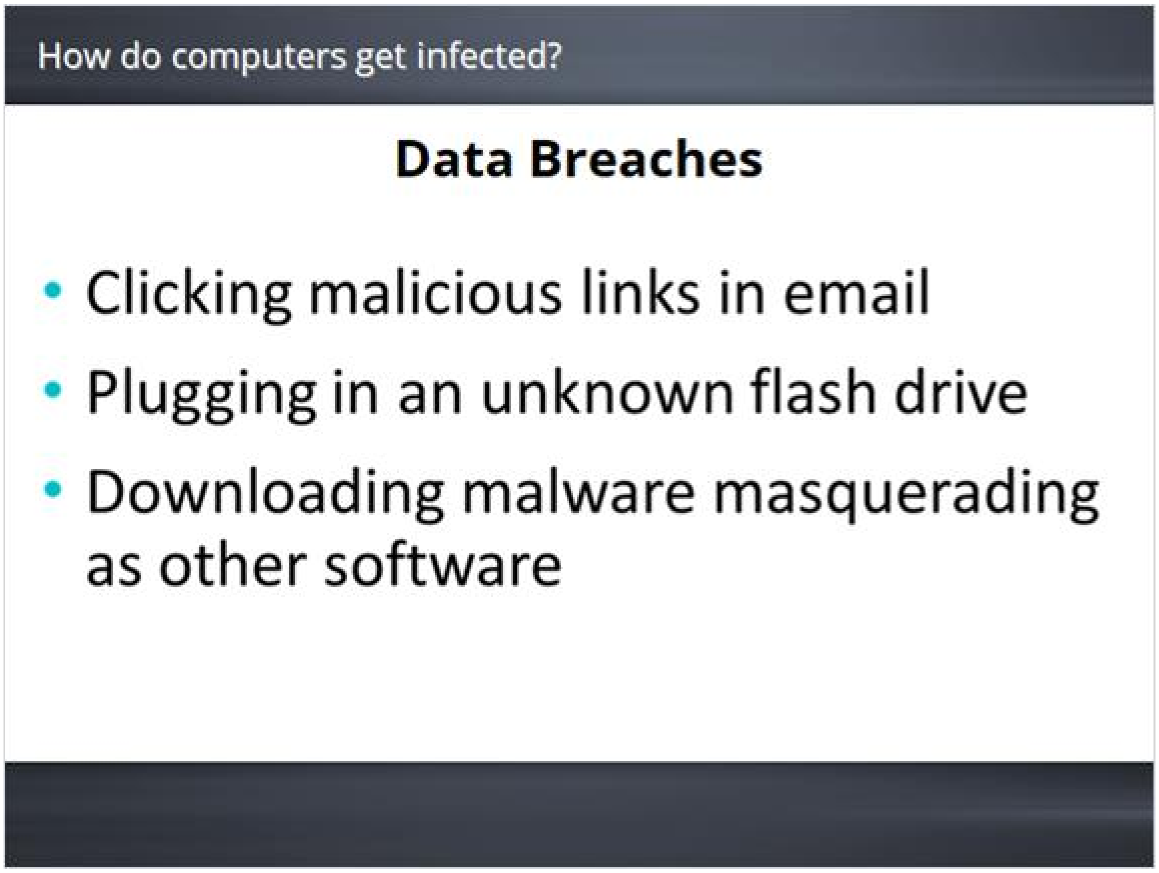
Malware - did you know?

Malware

- On average, 390,000 unique threats per day.[1]
- Unique threats ≠ extremely dissimilar.
- Malicious threats are changed in the smallest amount possible to evade detection.
- Malicious threats are targeted in order to have the highest penetration (success) rate.

[1]AV-TEST GmbH, www.av-test.org

1.20 How do computers get infected?

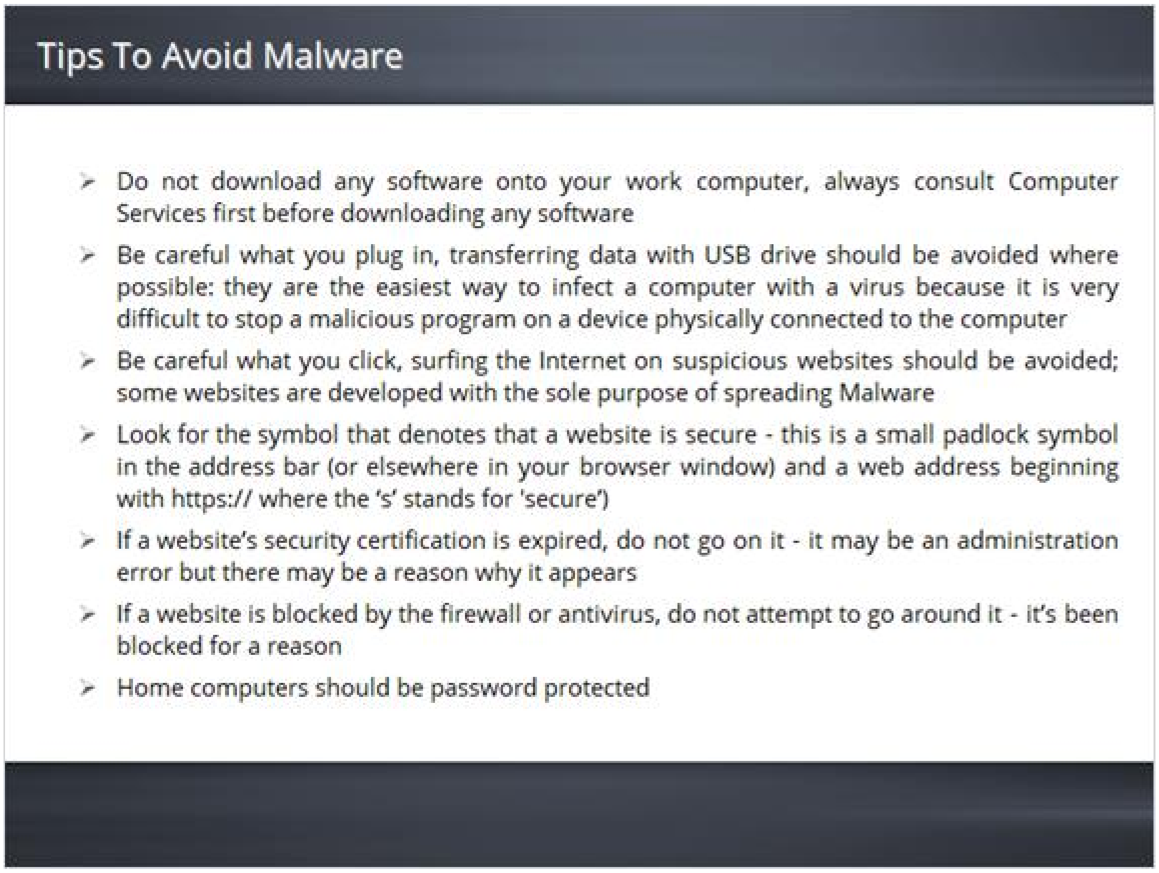


How do computers get infected?

Data Breaches

- Clicking malicious links in email
- Plugging in an unknown flash drive
- Downloading malware masquerading as other software

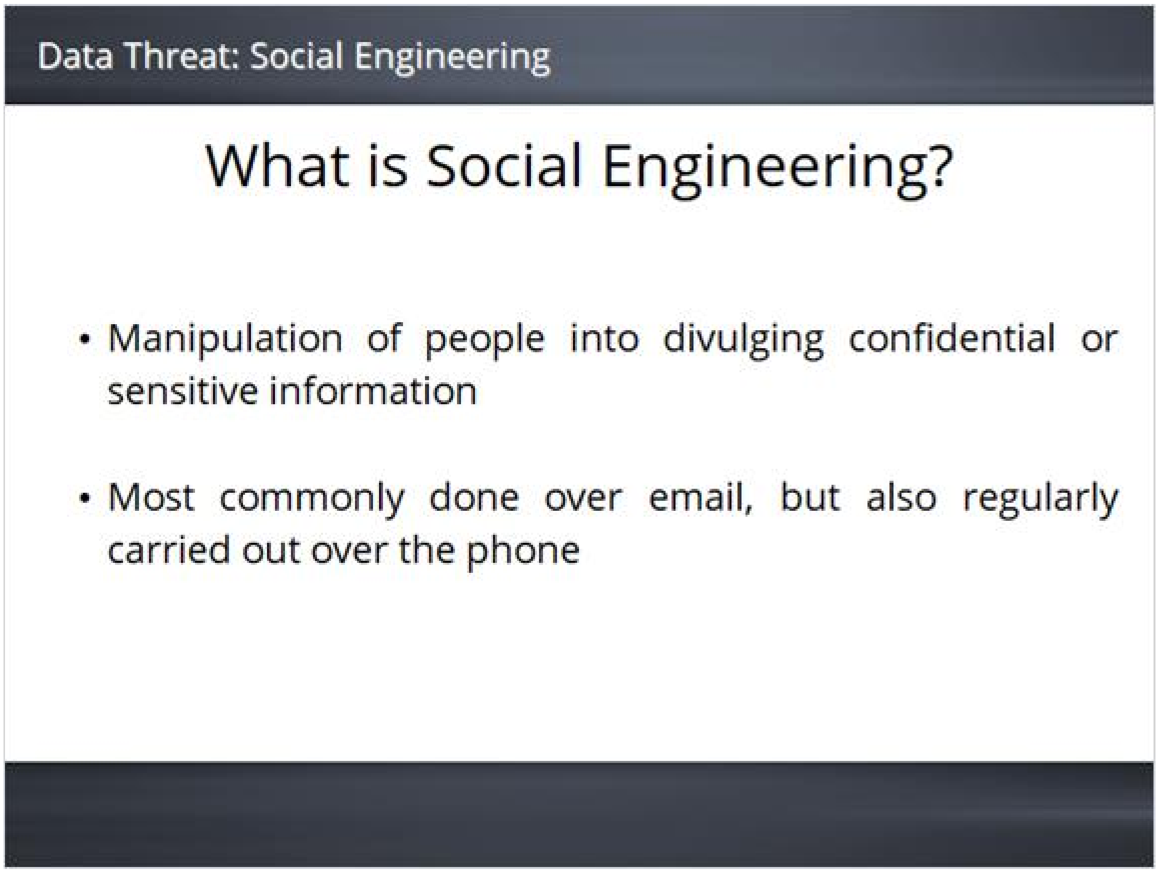
1.21 Tips To Avoid Malware



Tips To Avoid Malware

- Do not download any software onto your work computer, always consult Computer Services first before downloading any software
- Be careful what you plug in, transferring data with USB drive should be avoided where possible: they are the easiest way to infect a computer with a virus because it is very difficult to stop a malicious program on a device physically connected to the computer
- Be careful what you click, surfing the Internet on suspicious websites should be avoided; some websites are developed with the sole purpose of spreading Malware
- Look for the symbol that denotes that a website is secure - this is a small padlock symbol in the address bar (or elsewhere in your browser window) and a web address beginning with https:// where the ‘s’ stands for 'secure’)
- If a website’s security certification is expired, do not go on it - it may be an administration error but there may be a reason why it appears
- If a website is blocked by the firewall or antivirus, do not attempt to go around it - it’s been blocked for a reason
- Home computers should be password protected

1.22 Data Threat: Social Engineering

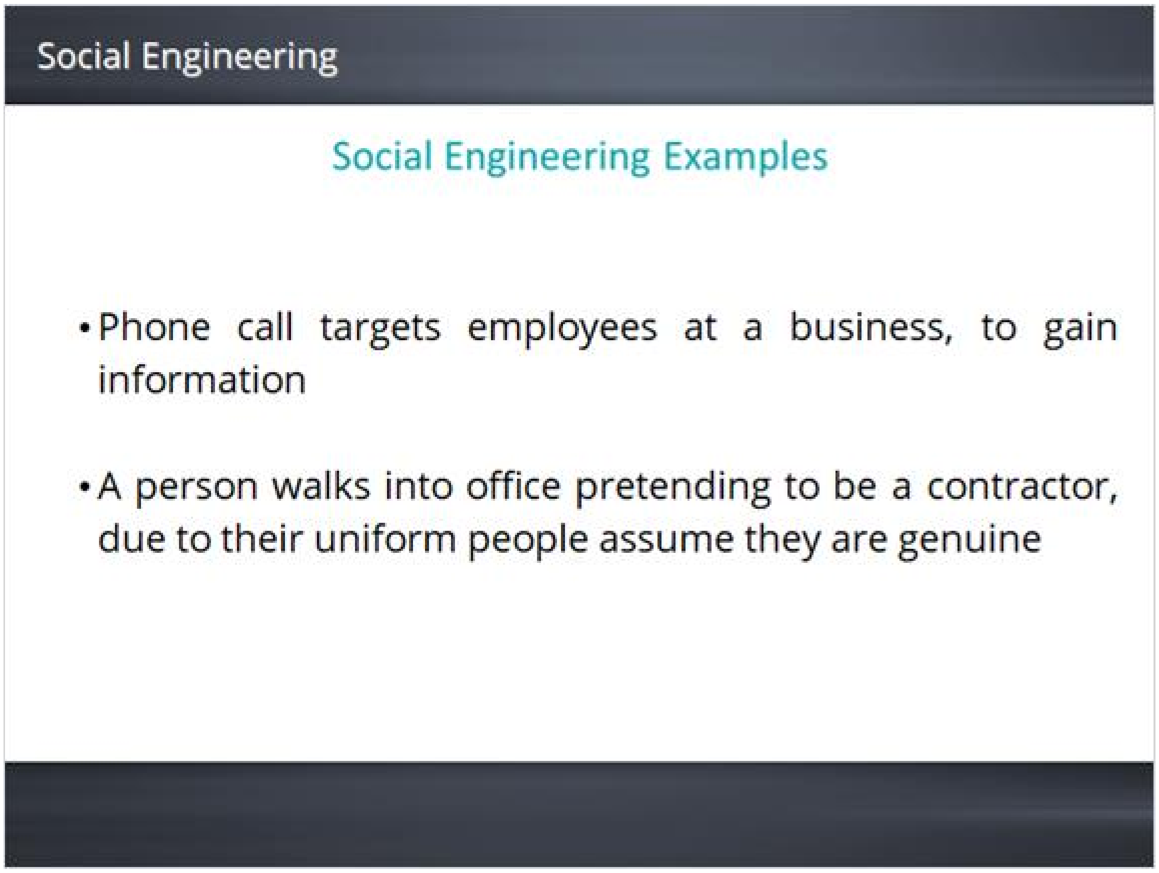


Data Threat: Social Engineering

What is Social Engineering?

- Manipulation of people into divulging confidential or sensitive information
- Most commonly done over email, but also regularly carried out over the phone

1.23 Social Engineering

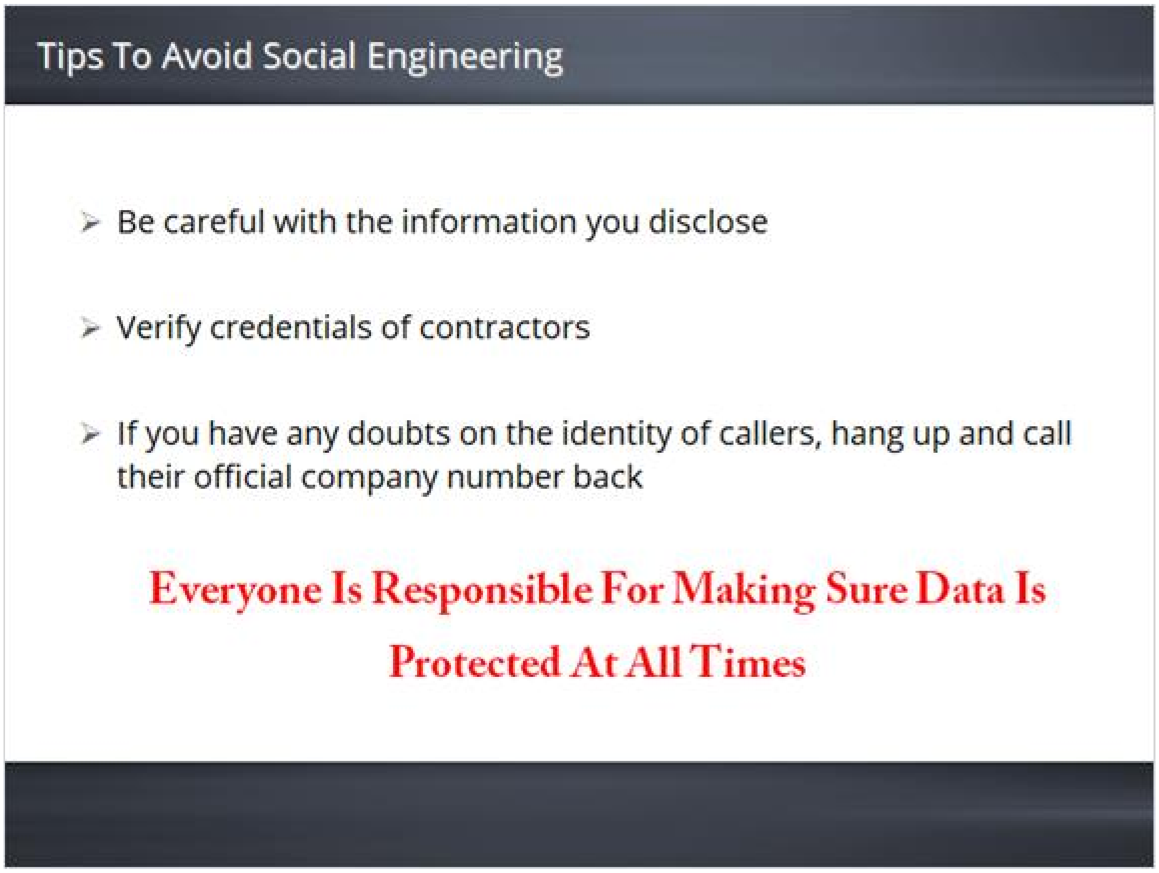


Social Engineering

Social Engineering Examples

- Phone call targets employees at a business, to gain information
- A person walks into office pretending to be a contractor, due to their uniform people assume they are genuine

1.24 Tips To Avoid Social Engineering

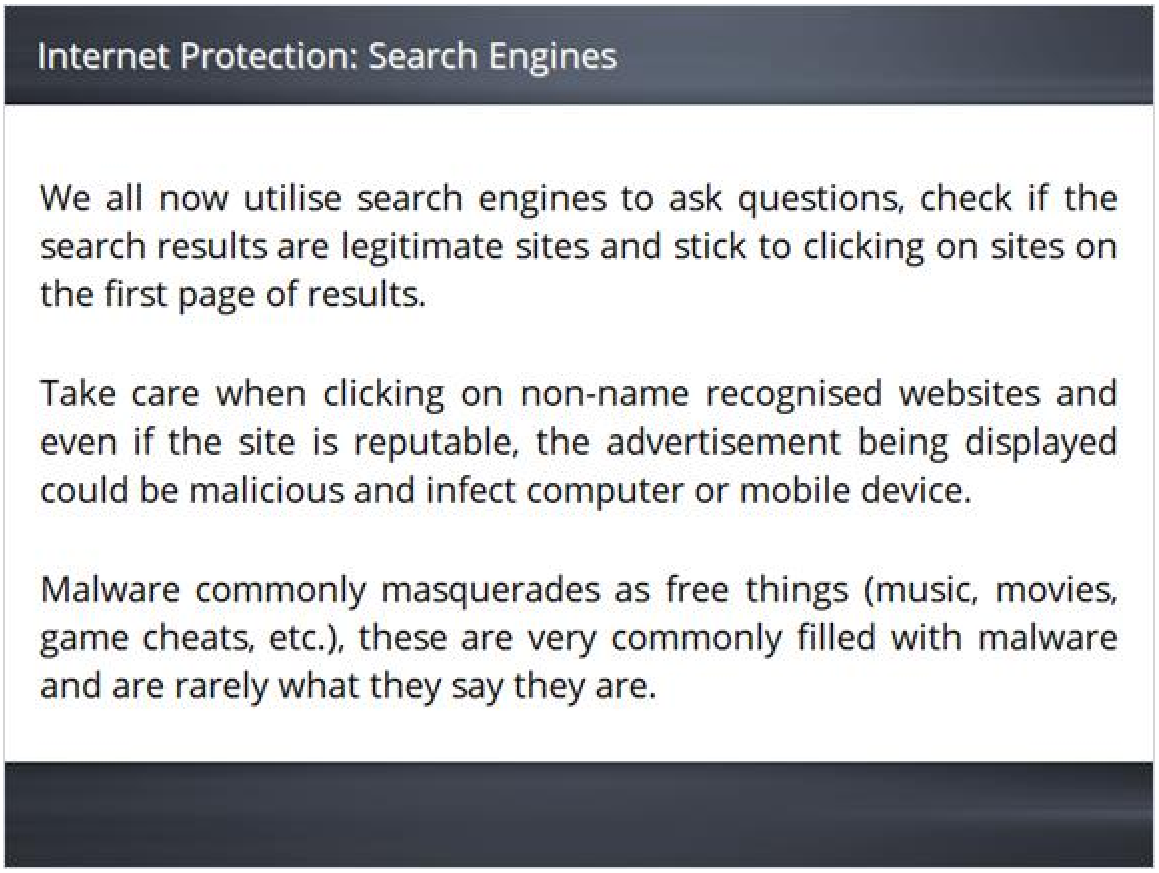


Tips To Avoid Social Engineering

- Be careful with the information you disclose
- Verify credentials of contractors
- If you have any doubts on the identity of callers, hang up and call their official company number back

Everyone Is Responsible For Making Sure Data Is Protected At All Times

1.25 Internet Protection: Search Engines



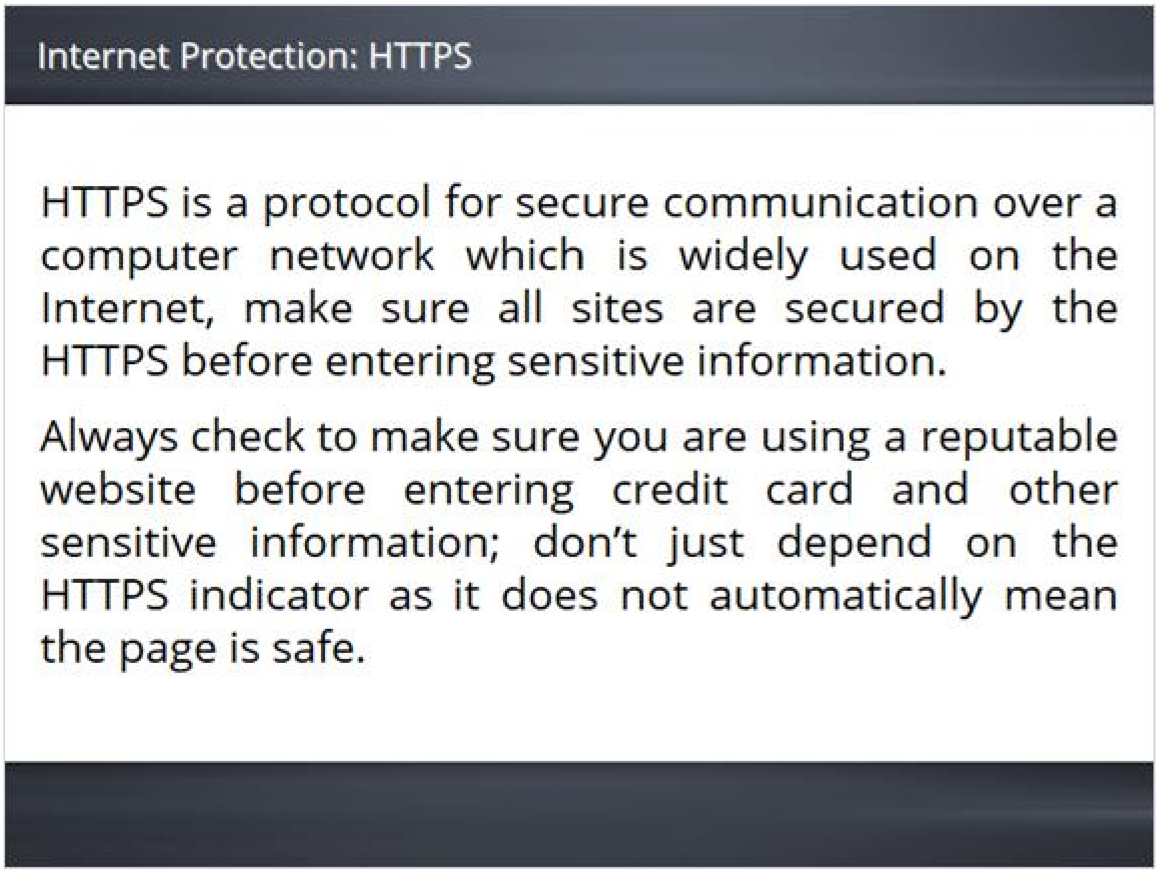
Internet Protection: Search Engines

We all now utilise search engines to ask questions, check if the search results are legitimate sites and stick to clicking on sites on the first page of results.

Take care when clicking on non-name recognised websites and even if the site is reputable, the advertisement being displayed could be malicious and infect computer or mobile device.

Malware commonly masquerades as free things (music, movies, game cheats, etc.), these are very commonly filled with malware and are rarely what they say they are.

1.26 Internet Protection: HTTPS

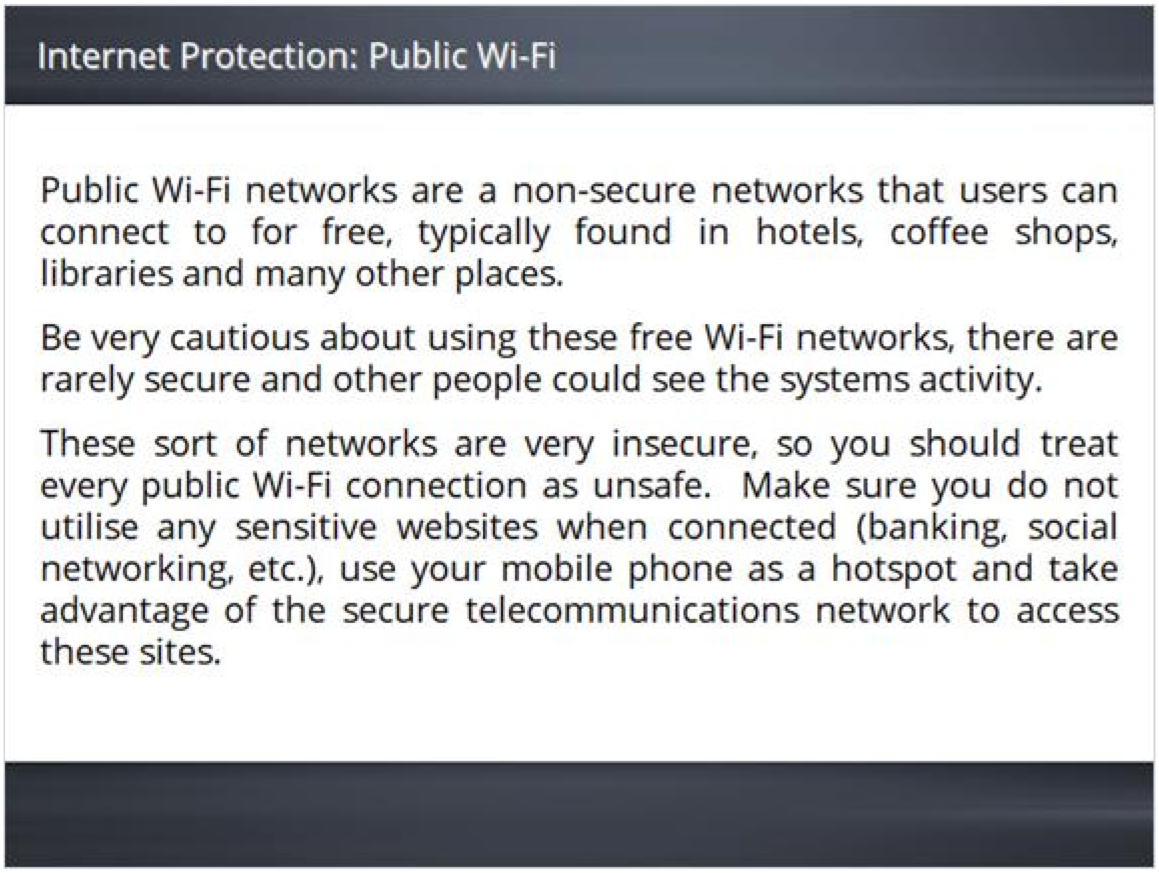


Internet Protection: HTTPS

HTTPS is a protocol for secure communication over a computer network which is widely used on the Internet, make sure all sites are secured by the HTTPS before entering sensitive information.

Always check to make sure you are using a reputable website before entering credit card and other sensitive information; don’t just depend on the HTTPS indicator as it does not automatically mean the page is safe.

1.27 Internet Protection: Public Wi-Fi



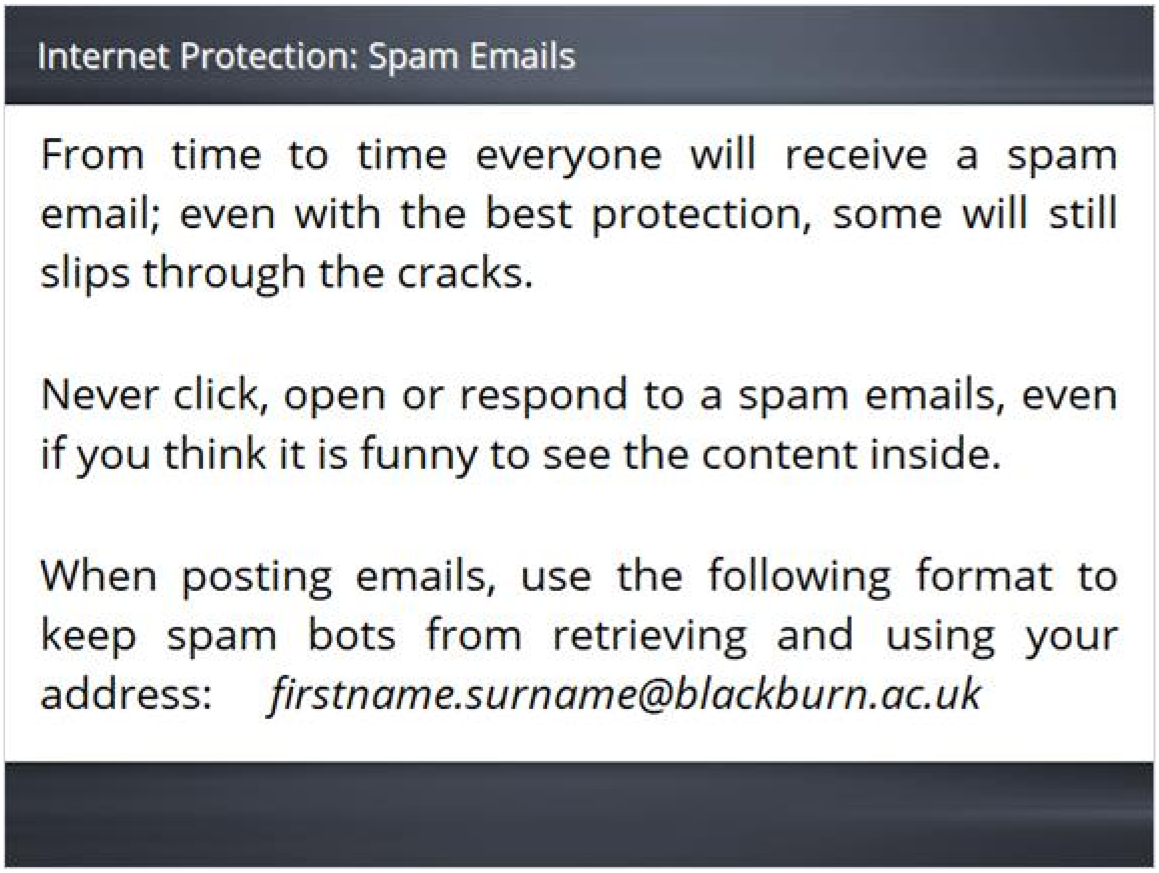
Internet Protection: Public Wi-Fi

Public Wi-Fi networks are a non-secure networks that users can connect to for free, typically found in hotels, coffee shops, libraries and many other places.

Be very cautious about using these free Wi-Fi networks, there are rarely secure and other people could see the systems activity.

These sort of networks are very insecure, so you should treat every public Wi-Fi connection as unsafe. Make sure you do not utilise any sensitive websites when connected (banking, social networking, etc.), use your mobile phone as a hotspot and take advantage of the secure telecommunications network to access these sites.

1.28 Internet Protection: Spam Emails



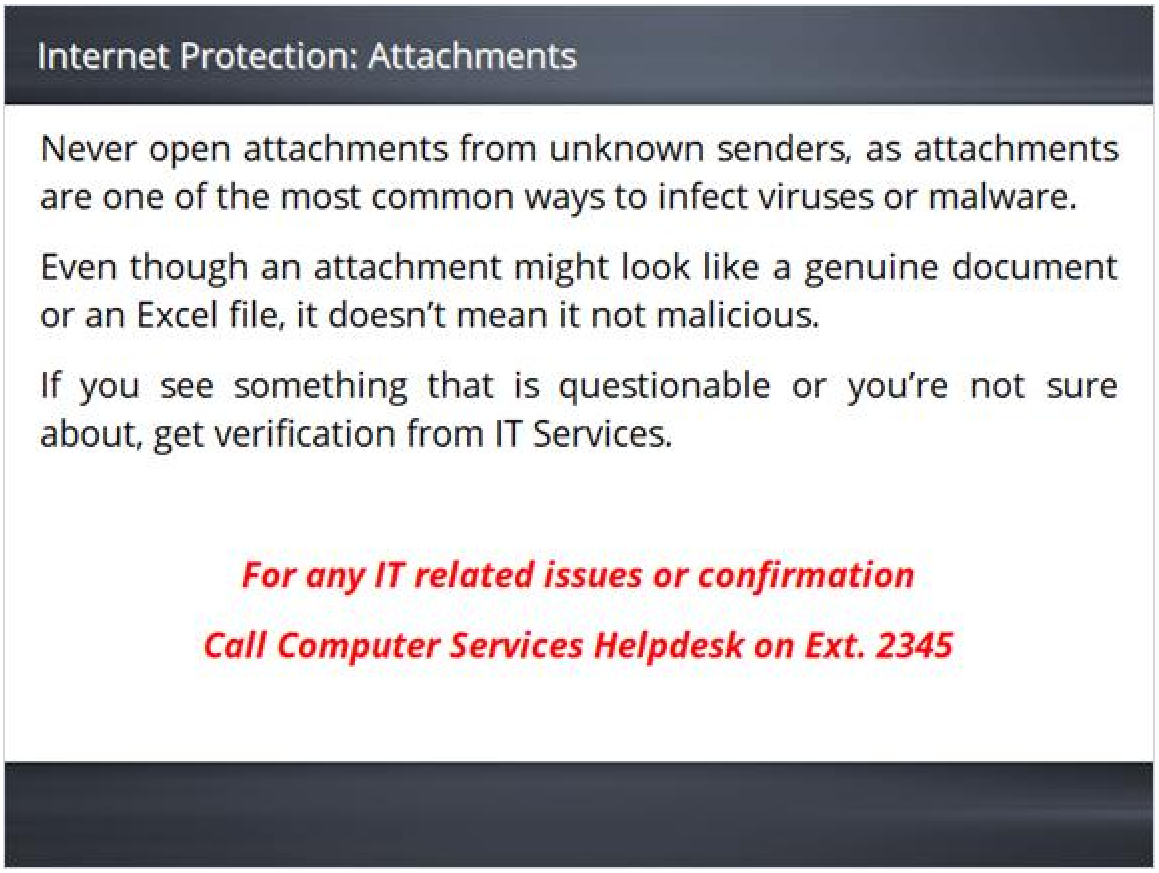
Internet Protection: Spam Emails

From time to time everyone will receive a spam email; even with the best protection, some will still slips through the cracks.

Never click, open or respond to a spam emails, even if you think it is funny to see the content inside.

When posting emails, use the following format to keep spam bots from retrieving and using your address: *firstname.surname@blackburn.ac.uk*

1.29 Internet Protection: Attachments



Internet Protection: Attachments

Never open attachments from unknown senders, as attachments are one of the most common ways to infect viruses or malware.

Even though an attachment might look like a genuine document or an Excel file, it doesn’t mean it not malicious.

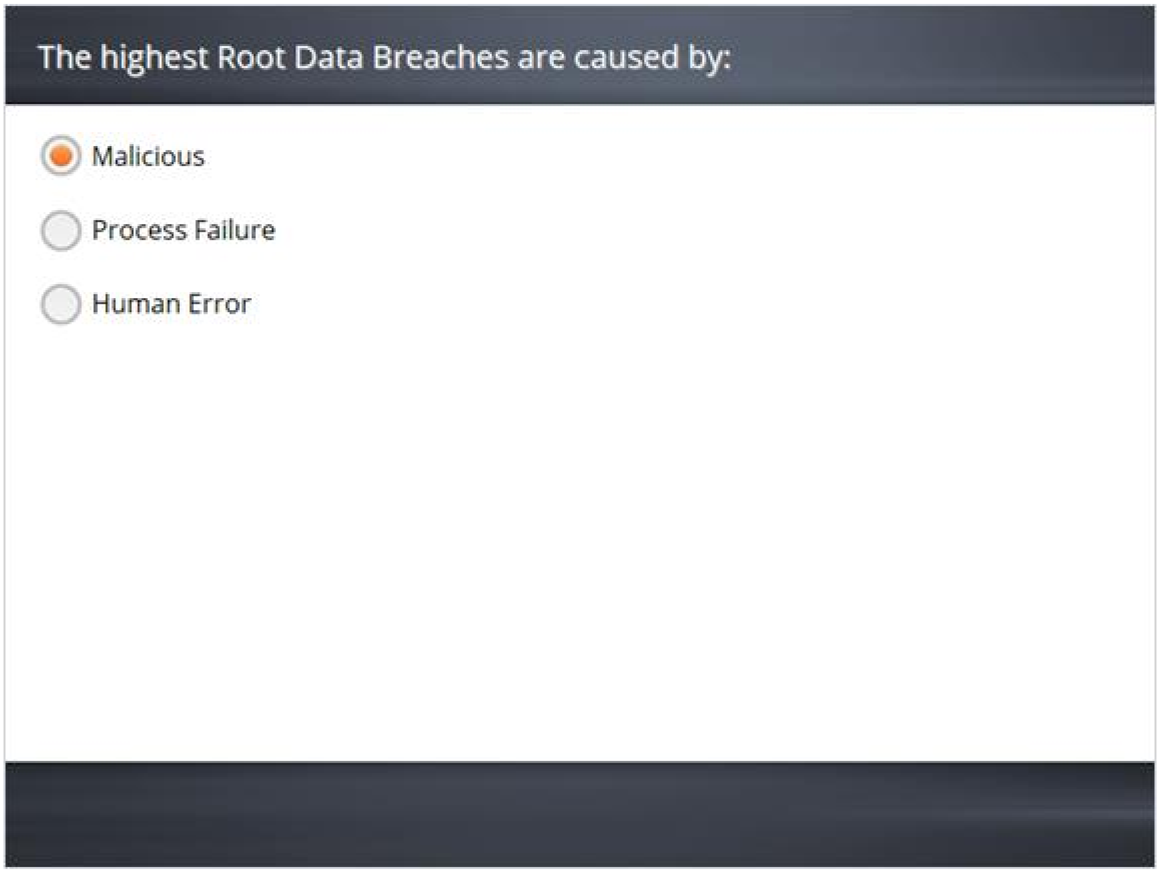
If you see something that is questionable or you’re not sure about, get verification from IT Services.

For any IT related issues or confirmation

Call Computer Services Helpdesk on Ext. 2345

1.30 The highest Root Data Breaches are caused by:

(Multiple Choice, 10 points, 1 attempt permitted)



The highest Root Data Breaches are caused by:

● Malicious

○ Process Failure

○ Human Error

Correct	Choice
X	Malicious
	Process Failure
	Human Error

Feedback when correct:

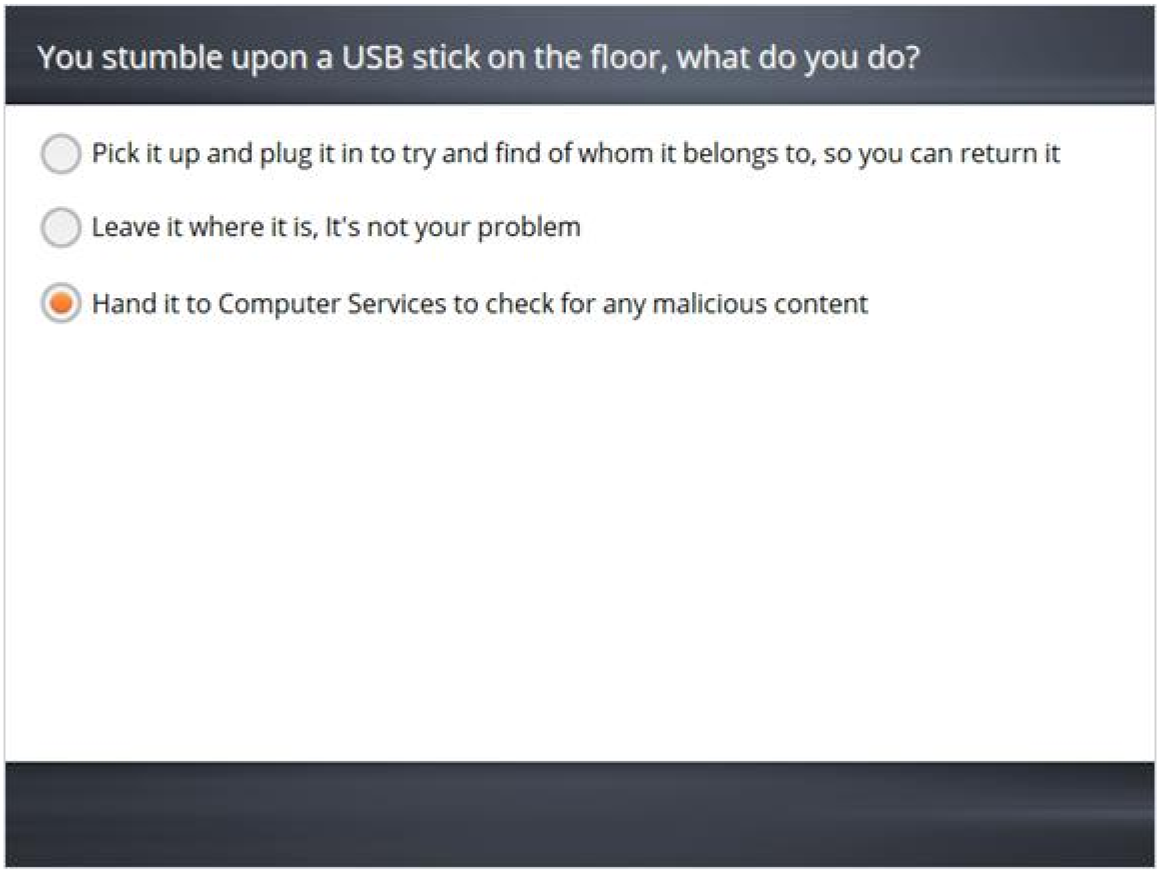
That's right! 48% Data Breaches are caused by Malicious

Feedback when incorrect:

You did not select the correct response.

1.31 You stumble upon a USB stick on the floor, what do you do?

(Multiple Choice, 10 points, 1 attempt permitted)



You stumble upon a USB stick on the floor, what do you do?

○ Pick it up and plug it in to try and find of whom it belongs to, so you can return it

○ Leave it where it is, It's not your problem

● Hand it to Computer Services to check for any malicious content

Correct	Choice
	Pick it up and plug it in to try and find of whom it belongs to, so you can return it
	Leave it where it is, It's not your problem
X	Hand it to Computer Services to check for any malicious content

Feedback when correct:

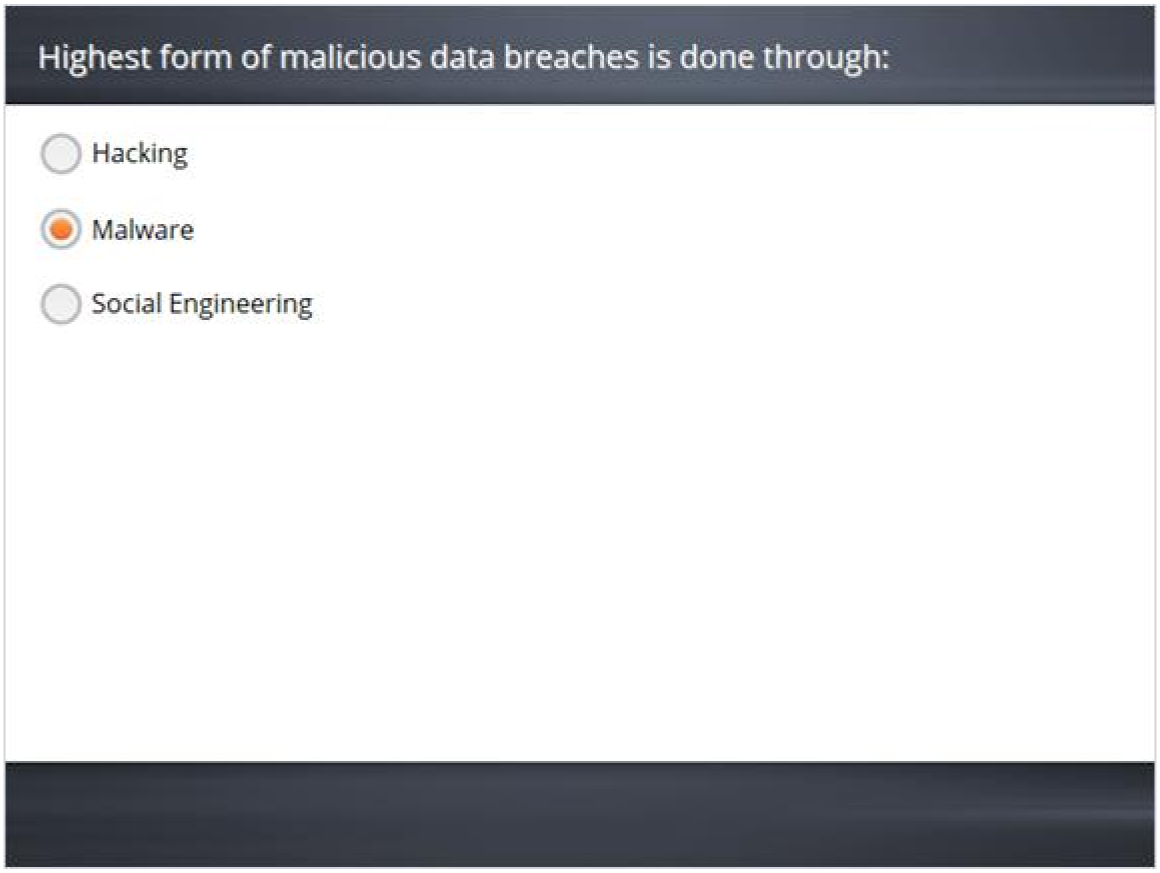
That's right! You selected the correct response.

Feedback when incorrect:

You did not select the correct response.

1.32 Highest form of malicious data breaches is done through:

(Multiple Choice, 10 points, 1 attempt permitted)



Highest form of malicious data breaches is done through:

○ Hacking

● Malware

○ Social Engineering

Correct	Choice
	Hacking
X	Malware
	Social Engineering

Feedback when correct:

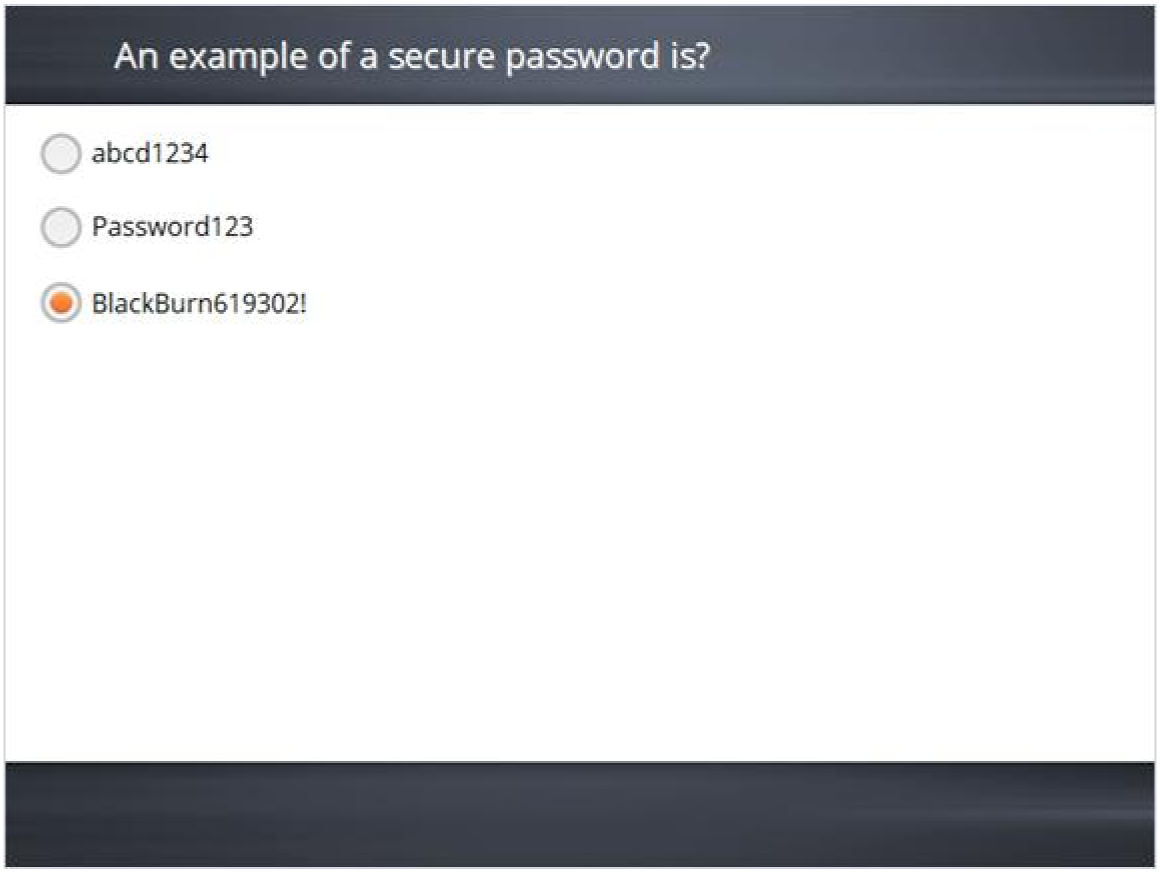
That's right! 59% of all total malicious data breaches

Feedback when incorrect:

You did not select the correct response.

1.33 An example of a secure password is?

(Multiple Choice, 10 points, 1 attempt permitted)



An example of a secure password is?

○ abcd1234

○ Password123

● BlackBurn619302!

Correct	Choice
	abcd1234
	Password123
X	BlackBurn619302!

Feedback when correct:

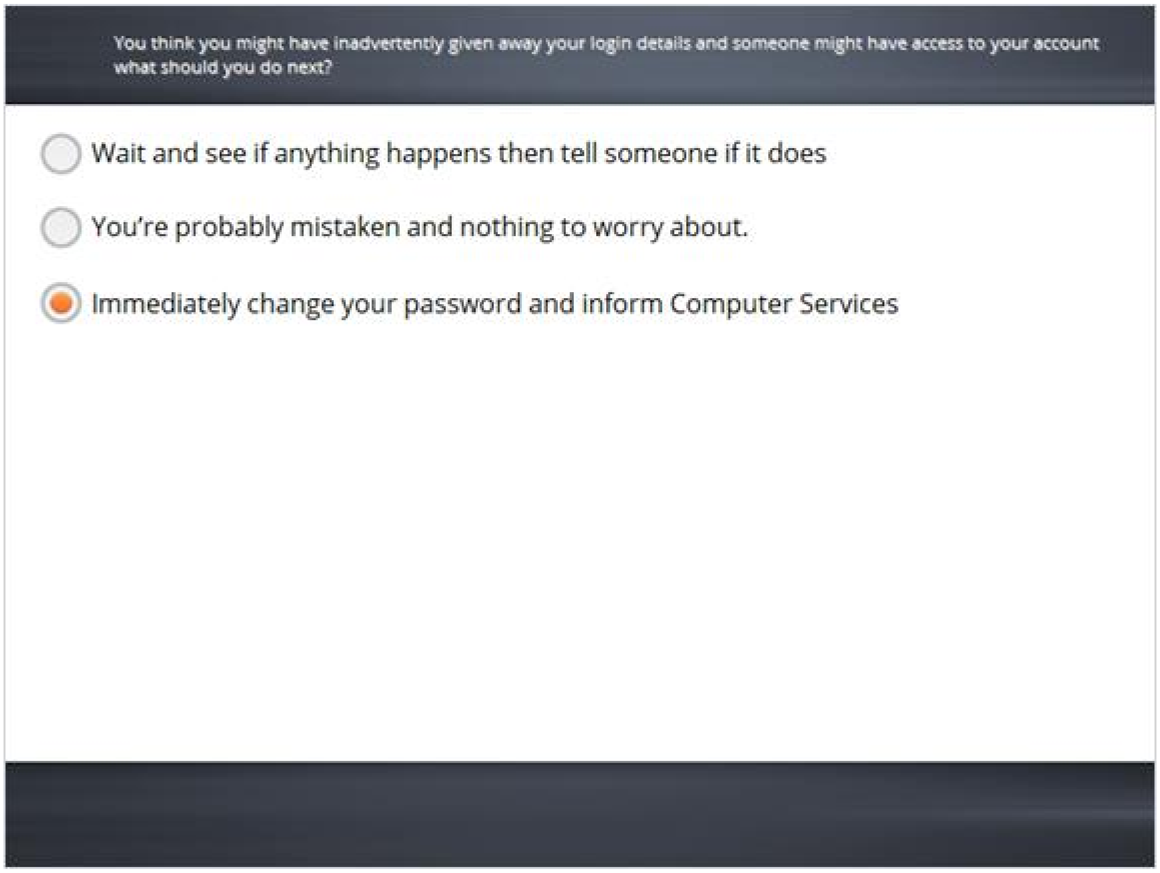
That's right! Upper/Lower case letters mixing with other characters

Feedback when incorrect:

You did not select the correct response.

1.34 You think you might have inadvertently given away your login details and someone might have access to your account what should you do next?

(Multiple Choice, 10 points, 1 attempt permitted)



You think you might have inadvertently given away your login details and someone might have access to your account what should you do next?

○ Wait and see if anything happens then tell someone if it does

○ You're probably mistaken and nothing to worry about.

● Immediately change your password and inform Computer Services

Correct	Choice
	Wait and see if anything happens then tell someone if it does
	You're probably mistaken and nothing to worry about.
X	Immediately change your password and inform Computer Services

Feedback when correct:

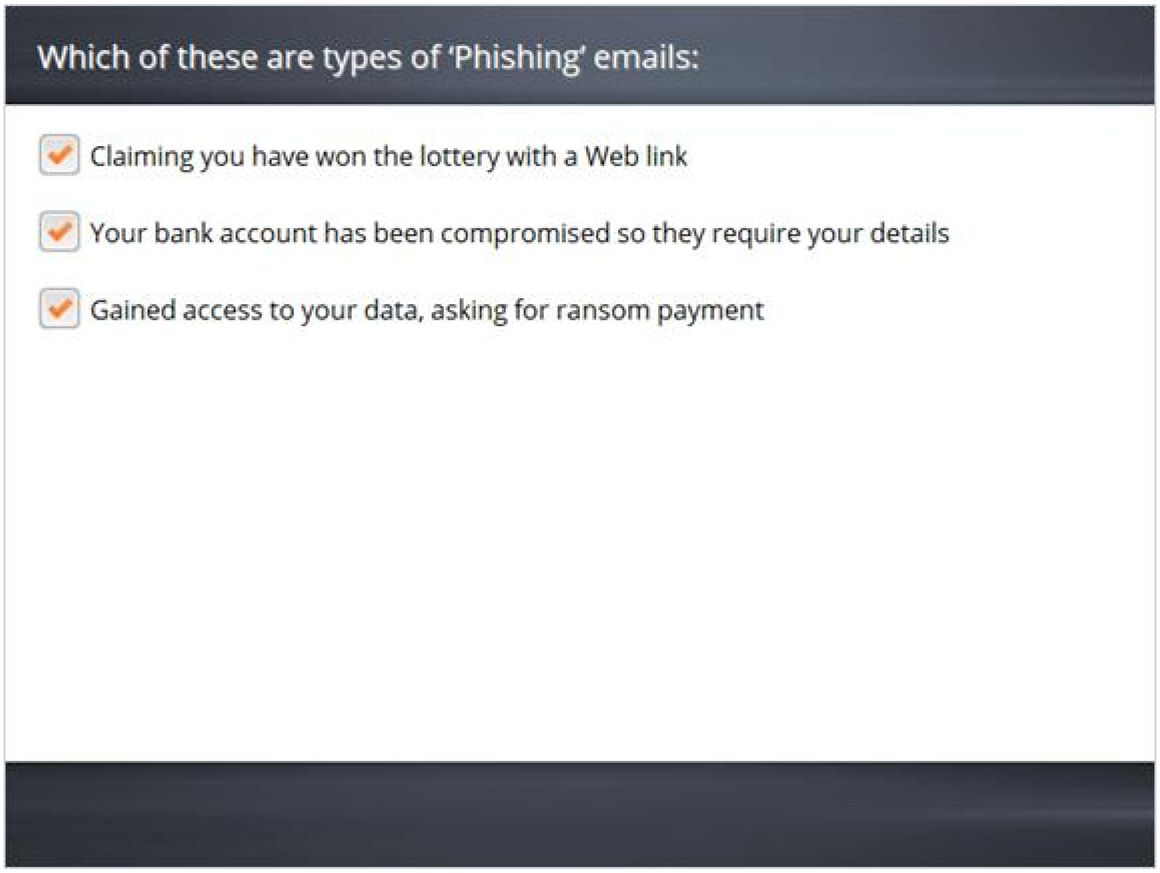
That's right! You selected the correct response.

Feedback when incorrect:

You did not select the correct response.

1.35 Which of these are types of ‘Phishing’ emails:

(Multiple Response, 10 points, 1 attempt permitted)



Which of these are types of ‘Phishing’ emails:

☑ Claiming you have won the lottery with a Web link

☑ Your bank account has been compromised so they require your details

☑ Gained access to your data, asking for ransom payment

Correct	Choice
X	Claiming you have won the lottery with a Web link
X	Your bank account has been compromised so they require your details
X	Gained access to your data, asking for ransom payment

Feedback when correct:

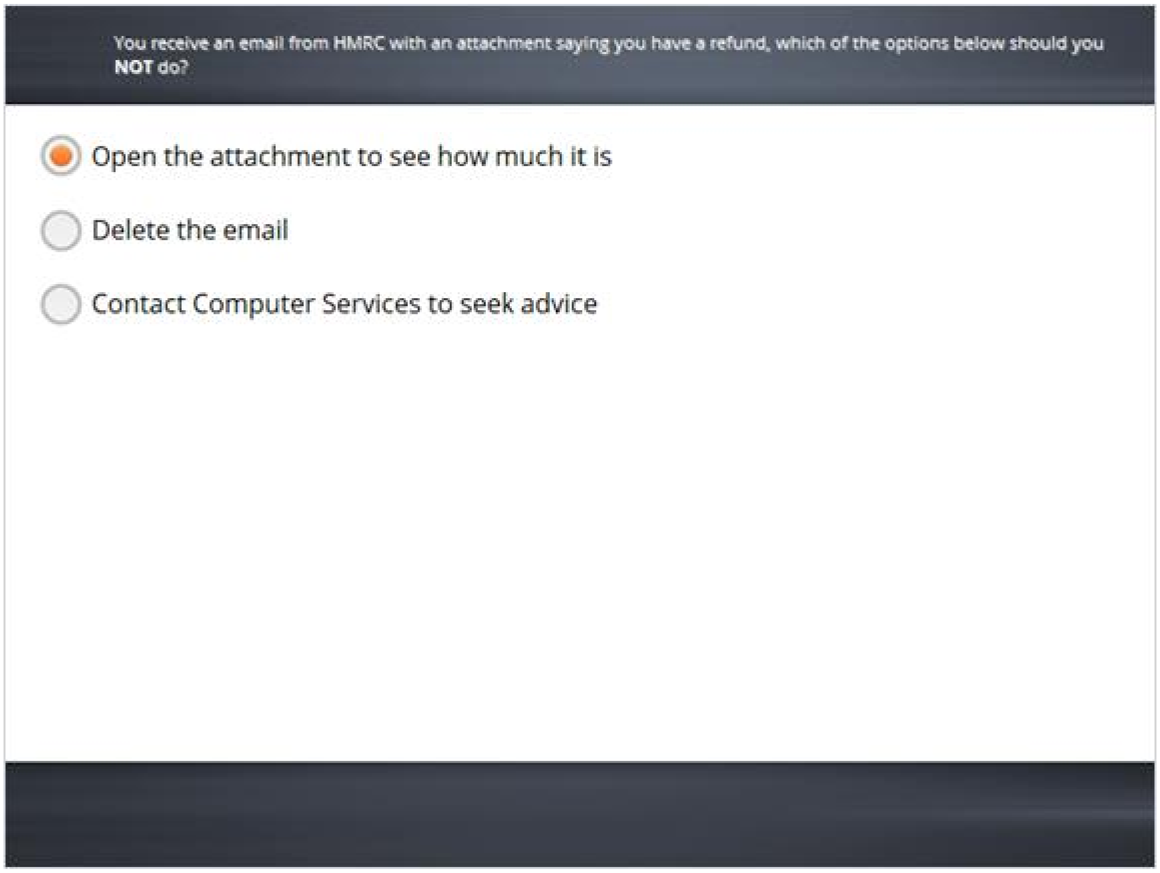
That's right! You selected the correct response.

Feedback when incorrect:

You did not select the correct response.

1.36 You receive an email from HMRC with an attachment saying you have a refund, which of the options below should you NOT do?

(Multiple Choice, 10 points, 1 attempt permitted)



You receive an email from HMRC with an attachment saying you have a refund, which of the options below should you **NOT** do?

● Open the attachment to see how much it is

○ Delete the email

○ Contact Computer Services to seek advice

Correct	Choice
X	Open the attachment to see how much it is

	Delete the email
	Contact Computer Services to seek advice

Feedback when correct:

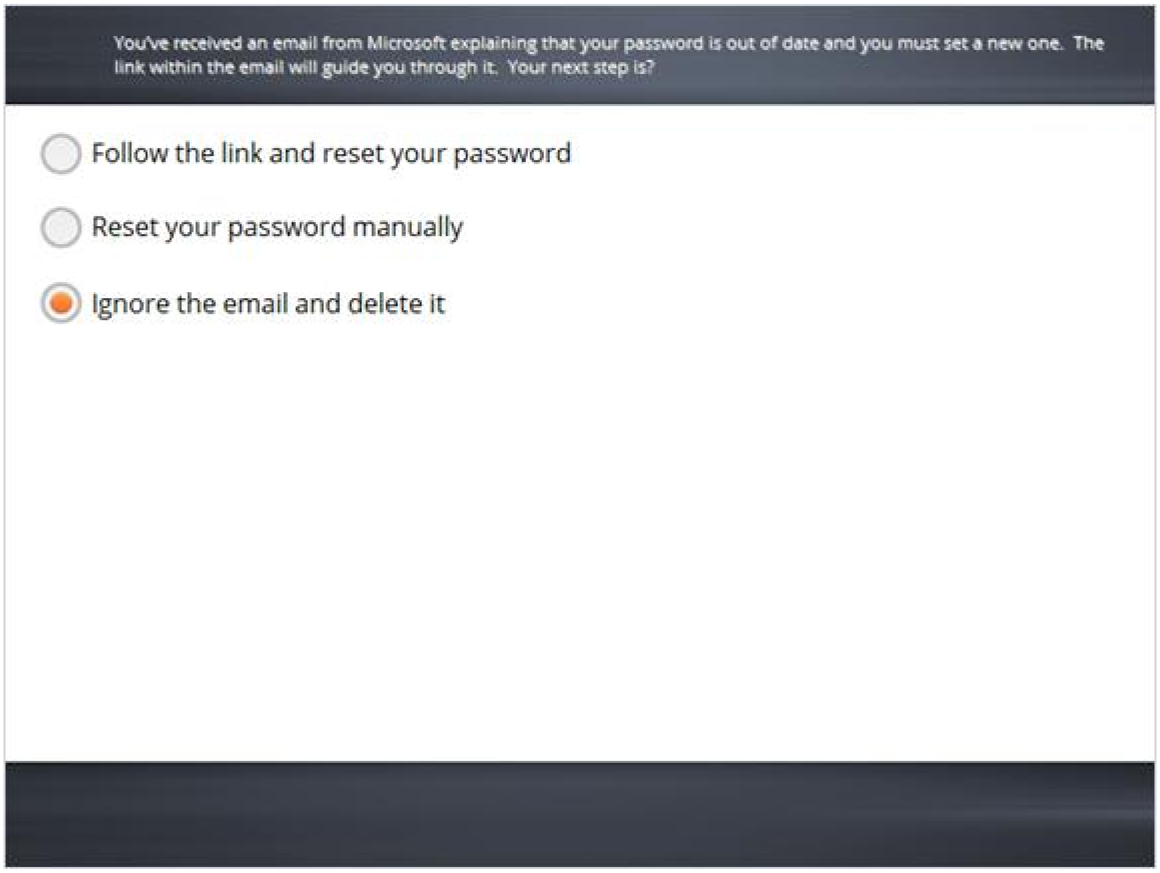
That's right! Do NOT open it

Feedback when incorrect:

You did not select the correct response.

1.37 You've received an email from Microsoft explaining that your password is out of date and you must set a new one. The link within the email will guide you through it. Your next step is?

(Multiple Choice, 10 points, 1 attempt permitted)



You've received an email from Microsoft explaining that your password is out of date and you must set a new one. The link within the email will guide you through it. Your next step is?

○ Follow the link and reset your password

○ Reset your password manually

● Ignore the email and delete it

Correct	Choice
	Follow the link and reset your password
	Reset your password manually
X	Ignore the email and delete it

Feedback when correct:

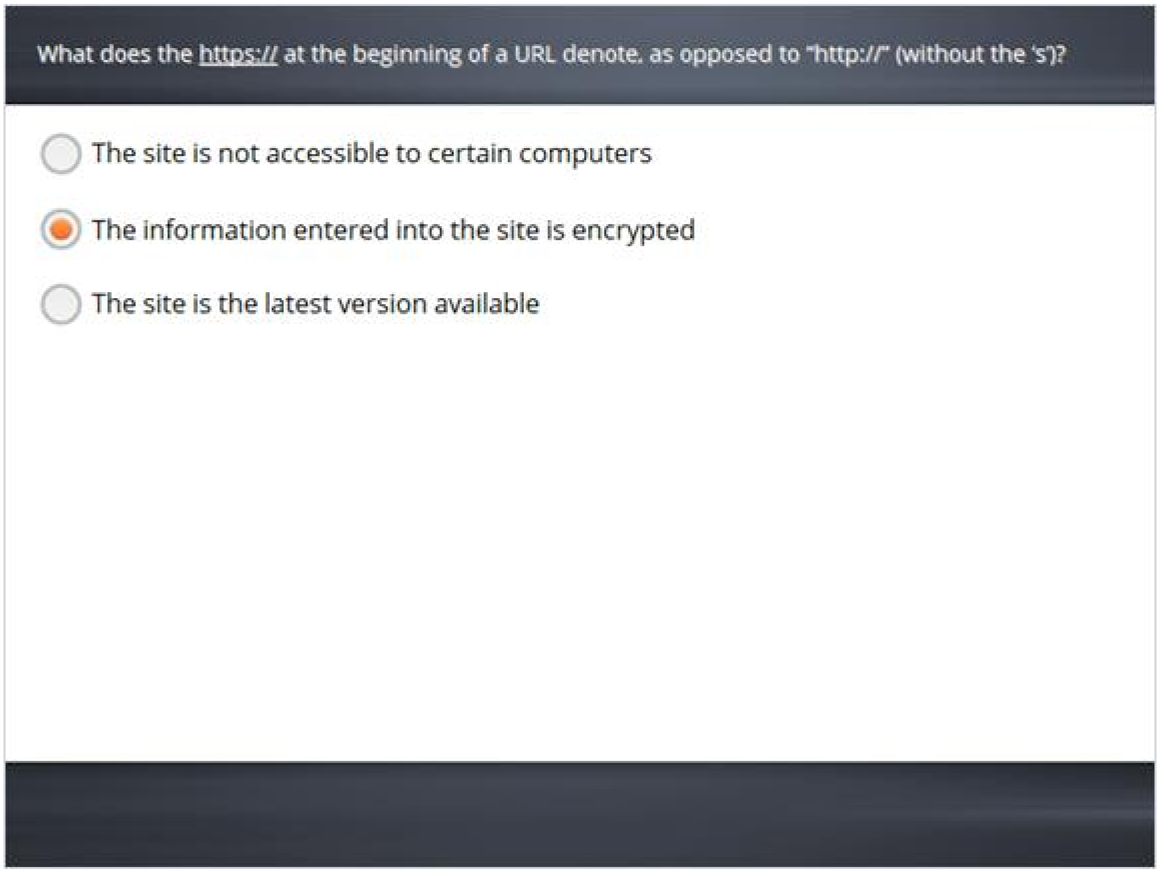
That's right! You selected the correct response.

Feedback when incorrect:

You did not select the correct response.

1.38 What does the https:// at the beginning of a URL denote, as opposed to "http://" (without the 's')?

(Multiple Choice, 10 points, 1 attempt permitted)



What does the https:// at the beginning of a URL denote, as opposed to "http://" (without the 's')?

○ The site is not accessible to certain computers

● The information entered into the site is encrypted

○ The site is the latest version available

Correct	Choice
	The site is not accessible to certain computers
X	The information entered into the site is encrypted
	The site is the latest version available

Feedback when correct:

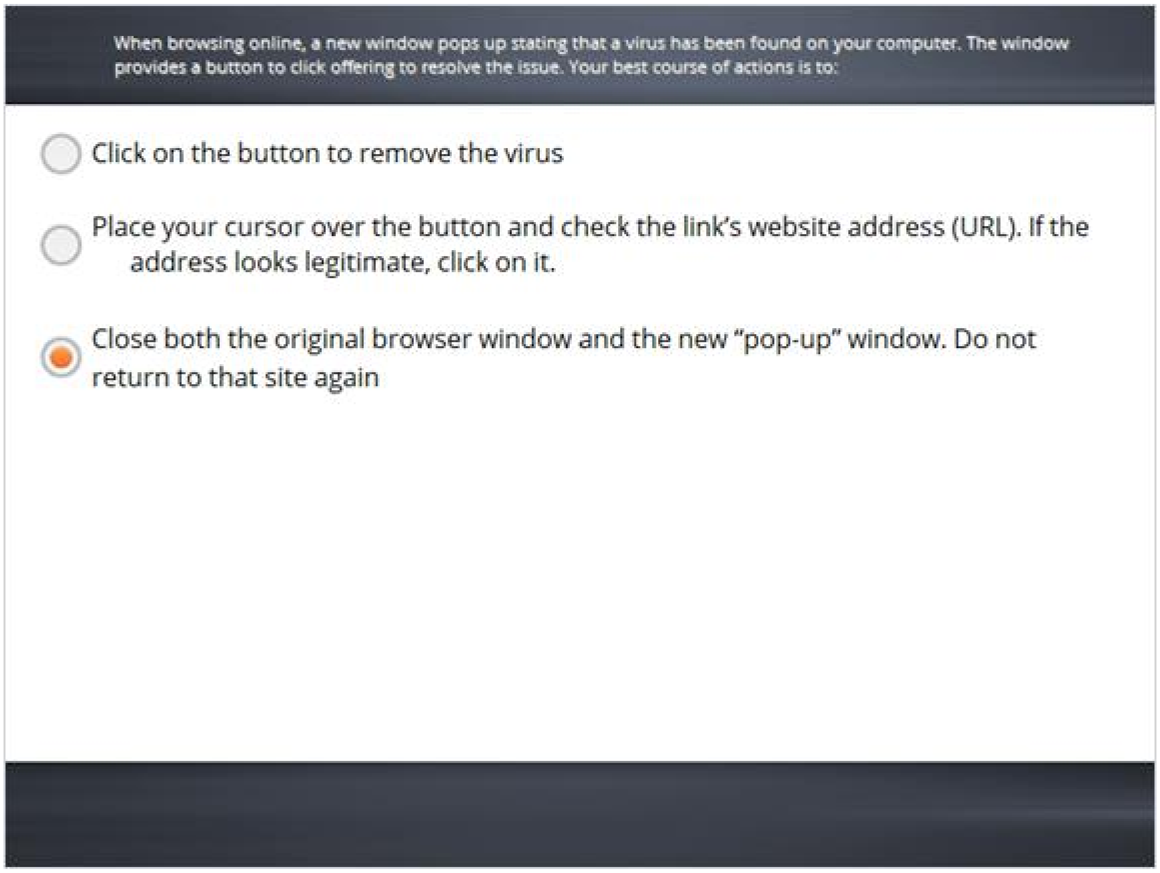
That's right! You selected the correct response.

Feedback when incorrect:

You did not select the correct response.

1.39 When browsing online, a new window pops up stating that a virus has been found on your computer. The window provides a button to click offering to resolve the issue. Your best course of actions is to:

(Multiple Choice, 10 points, 1 attempt permitted)



When browsing online, a new window pops up stating that a virus has been found on your computer. The window provides a button to click offering to resolve the issue. Your best course of actions is to:

○ Click on the button to remove the virus

○ Place your cursor over the button and check the link's website address (URL). If the address looks legitimate, click on it.

● Close both the original browser window and the new "pop-up" window. Do not return to that site again

Correct	Choice
	Click on the button to remove the virus
	Place your cursor over the button and check the link's website address (URL). If the address looks legitimate, click on it.
X	Close both the original browser window and the new "pop-up" window. Do not

return to that site again

Feedback when correct:

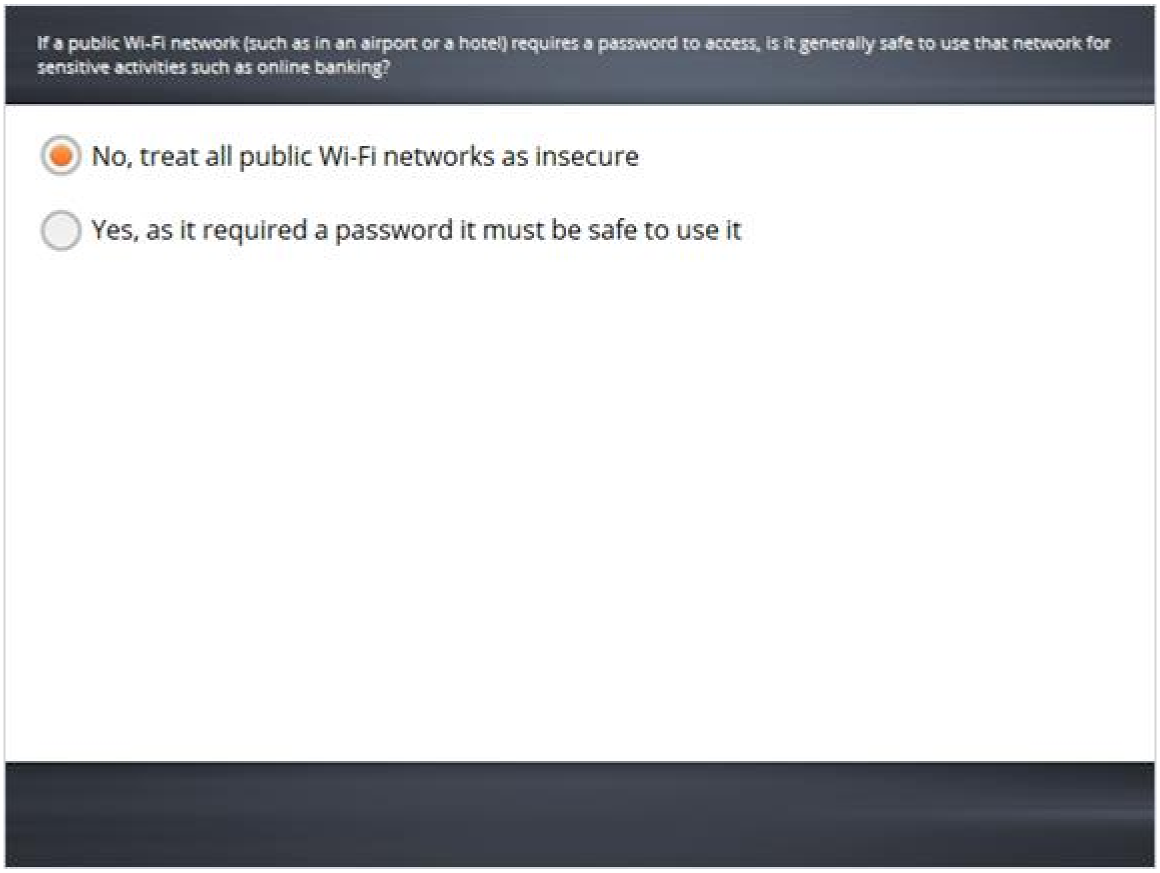
That's right! You selected the correct response.

Feedback when incorrect:

You did not select the correct response.

1.40 If a public Wi-Fi network (such as in an airport or a hotel) requires a password to access, is it generally safe to use that network for sensitive activities such as online banking?

(Multiple Choice, 10 points, 1 attempt permitted)



If a public Wi-Fi network (such as in an airport or a hotel) requires a password to access, is it generally safe to use that network for sensitive activities such as online banking?

● No, treat all public Wi-Fi networks as insecure

○ Yes, as it required a password it must be safe to use it

Correct	Choice
X	No, treat all public Wi-Fi networks as insecure
	Yes, as it required a password it must be safe to use it

Feedback when correct:

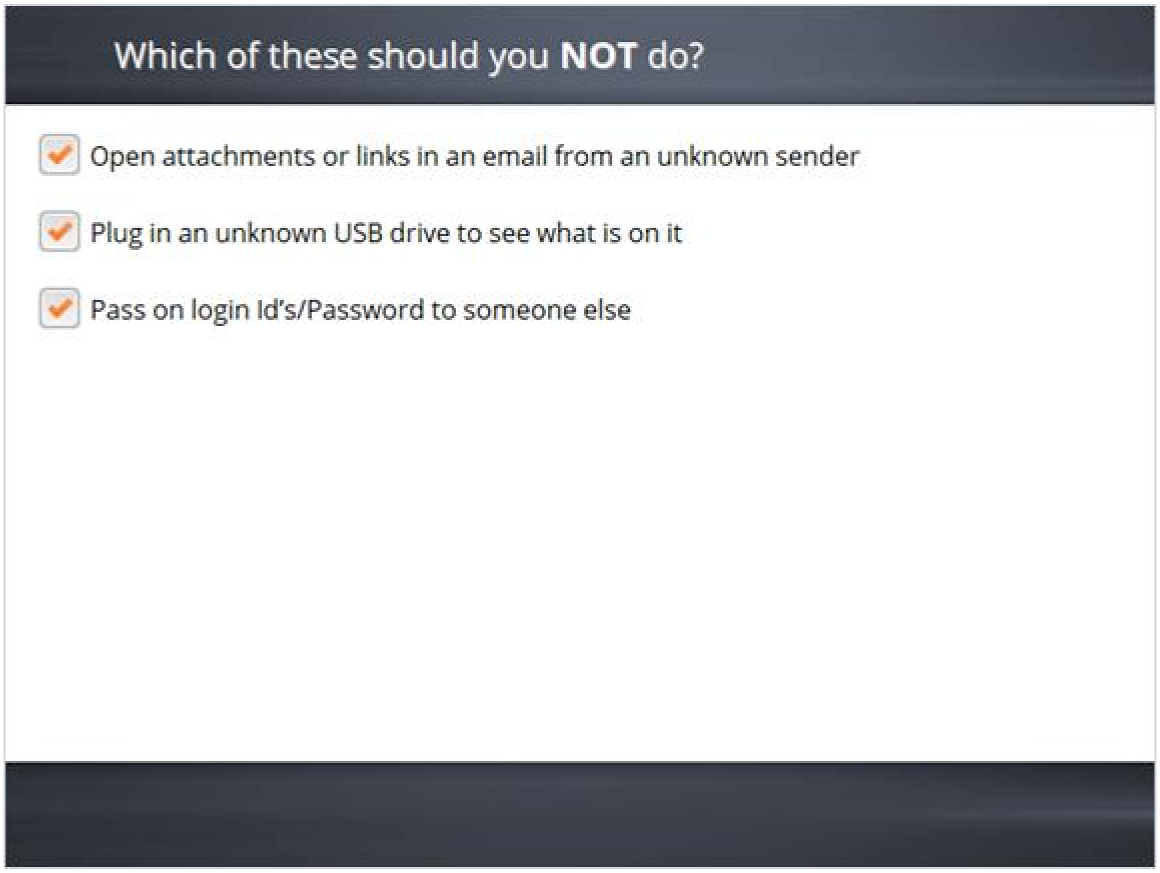
That's right! You selected the correct response.

Feedback when incorrect:

You did not select the correct response.

1.41 Which of these should you NOT do?

(Multiple Response, 10 points, 1 attempt permitted)



Which of these should you **NOT** do?

☑ Open attachments or links in an email from an unknown sender

☑ Plug in an unknown USB drive to see what is on it

☑ Pass on login Id's/Password to someone else

Correct	Choice
X	Open attachments or links in an email from an unknown sender
X	Plug in an unknown USB drive to see what is on it
X	Pass on login Id’s/Password to someone else

Feedback when correct:

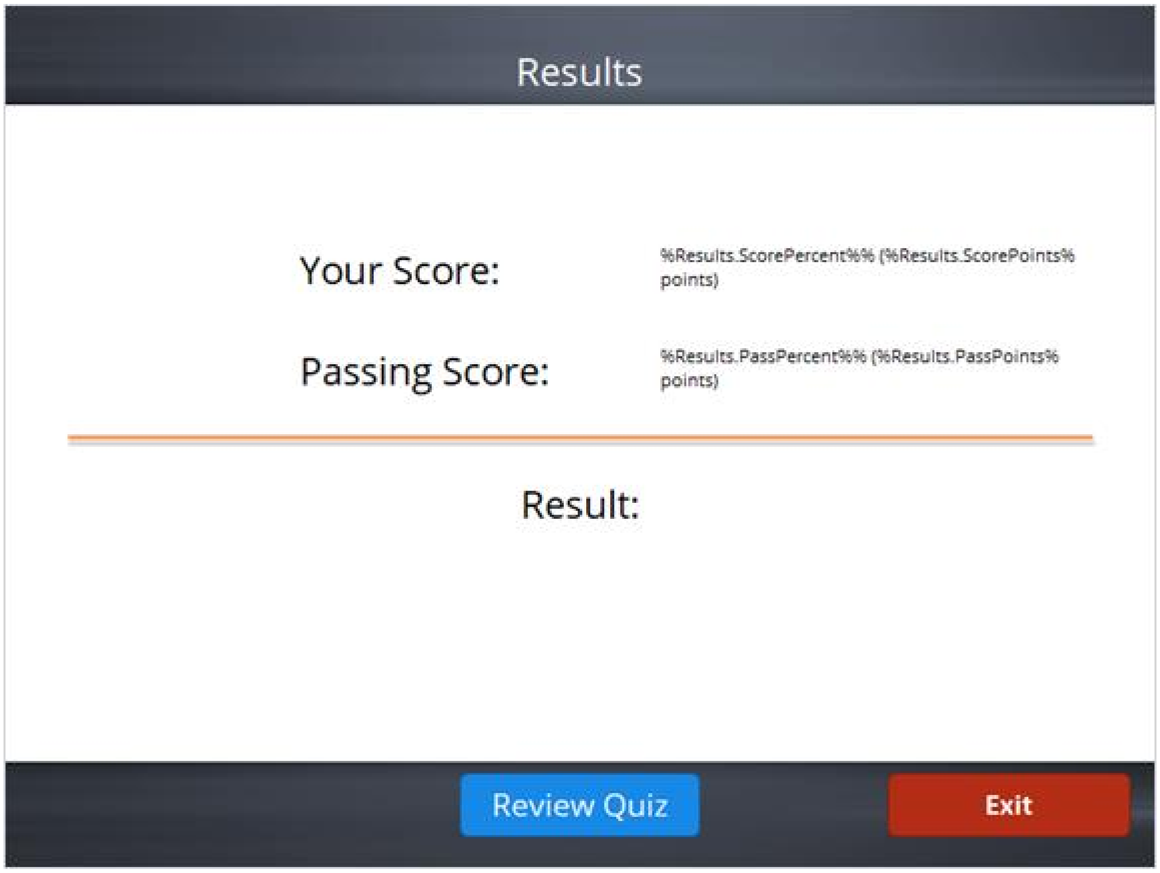
That's right! You selected the correct response.

Feedback when incorrect:

You did not select the correct response.

1.42 Results Slide

(Results Slide, 0 points, 1 attempt permitted)



Results

Your Score: %Results.ScorePercent%% (%Results.ScorePoints% points)

Passing Score: %Results.PassPercent%% (%Results.PassPoints% points)

Result:

Results for
1.30 The highest Root Data Breaches are caused by:
1.31 You stumble upon a USB stick on the floor, what do you do?
1.32 Highest form of malicious data breaches is done through:
1.33 An example of a secure password is?
1.34 You think you might have inadvertently given away your login details and someone might have access to your account what should you do next?
1.35 Which of these are types of ‘Phishing’ emails:
1.36 You receive an email from HMRC with an attachment saying you have a refund, which of

the options below should you NOT do?
1.37 You’ve received an email from Microsoft explaining that your password is out of date and you must set a new one. The link within the email will guide you through it. Your next step is?
1.38 What does the https:// at the beginning of a URL denote, as opposed to “http://” (without the ‘s’)?
1.39 When browsing online, a new window pops up stating that a virus has been found on your computer. The window provides a button to click offering to resolve the issue. Your best course of actions is to:
1.40 If a public Wi-Fi network (such as in an airport or a hotel) requires a password to access, is it generally safe to use that network for sensitive activities such as online banking?
1.41 Which of these should you NOT do?

Result slide properties

Passing Score	80%