Bournemouth University

Business Continuity Awareness Week

"Cyber security is everyone's responsibility."

Business Continuity Awareness Week
#BCAW2018
14th – 18th May 2018

Avoid work disruption:

Would you leave your house or car unlocked? So why leave your computer unlocked?

Is your personal information and login details safe?

Can you trust the USB stick you're about to plug into your network?

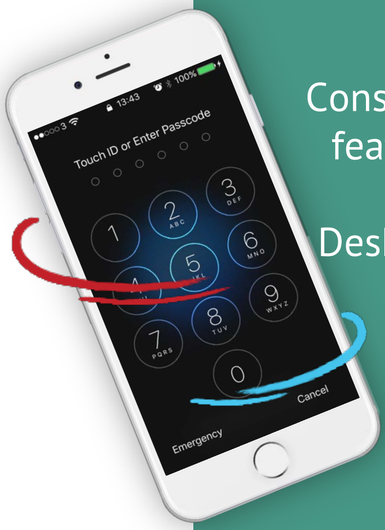
Can you trust the public WiFi you've just allowed to access your computer?

Can you really trust that link you're about to click on?

- @BUBusCont

Need help? Call IT Service Desk on +44 (0)1202 9 65515.

Would you leave your house or car unlocked? So why leave your computer unlocked?



Consider the auto-locking feature is enabled on all your devices (e.g. Desktops, laptops,mobile phones and tablets). This will enable your device's screen locks automatically when you step away.

Use strong passwords to unlock your devices to prevent anyone from guessing your passwords.

Is your personal information and login details safe?

5 WAYS THAT THIEVES CAN STEAL YOUR IDENTITY

Drive-by-download

Fake news on Twitter, funny videos on Facebook, images on Snapshot. When you click on them, you get redirected to a theft website which will download malicious code onto your device to start recording your online activity.

SMShing

Posing as the NHS, a thief sends you a text message containing a link for a hospital appointment. When you click the link on the message, the thief can start accessing your personal information.

Social media stalking

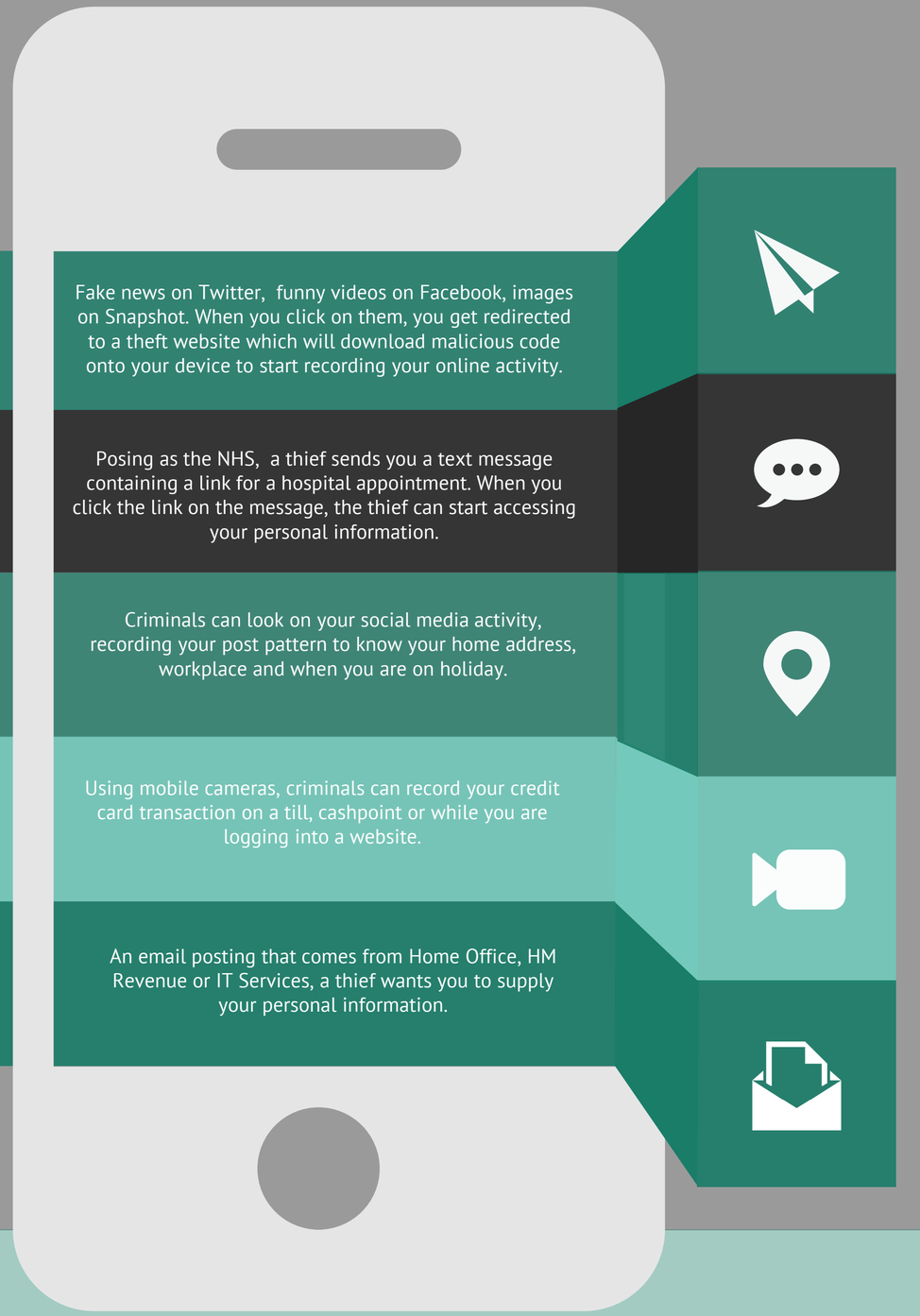
Criminals can look on your social media activity, recording your post pattern to know your home address, workplace and when you are on holiday.

Shoulder surfing

Using mobile cameras, criminals can record your credit card transaction on a till, cashpoint or while you are logging into a website.

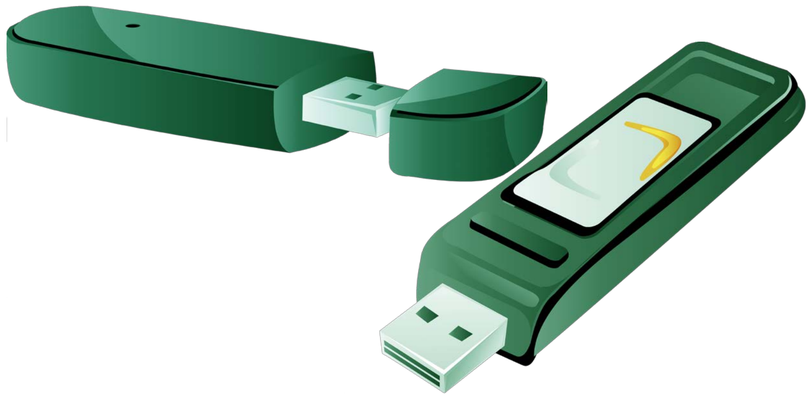
Phishing

An email posting that comes from Home Office, HM Revenue or IT Services, a thief wants you to supply your personal information.



Need help? Call IT Service Desk on +44 (0)1202 9 65515.

Can you trust the USB stick you're about to plug into your network?



USB-Specific Malware

Plugging in a USB memory device on computer without knowing who is the source or where it came from is a big risk. Some malicious software stored in a USB stick auto-runs once you plug into computer without your knowledge and there is a high success of being undetected by a security software such as anti-virus.

Found USB sticks

Consider not to use a USB memory device that you find lying around or a give away from a conference/event. Treat USB sticks as infectious devices that may harm your computer and your files. Always seek assistance before using a USB stick if unsure, or better not to use at all.

USB drive essentials

Always encrypt your USB sticks so if it gets lost, it will be very difficult for someone to look on the stored data. Make a habit of backing up your data so it can recovery quickly and save time re-creating hard to produce documents.

Can you trust the public WiFi you've just allowed to access your computer?

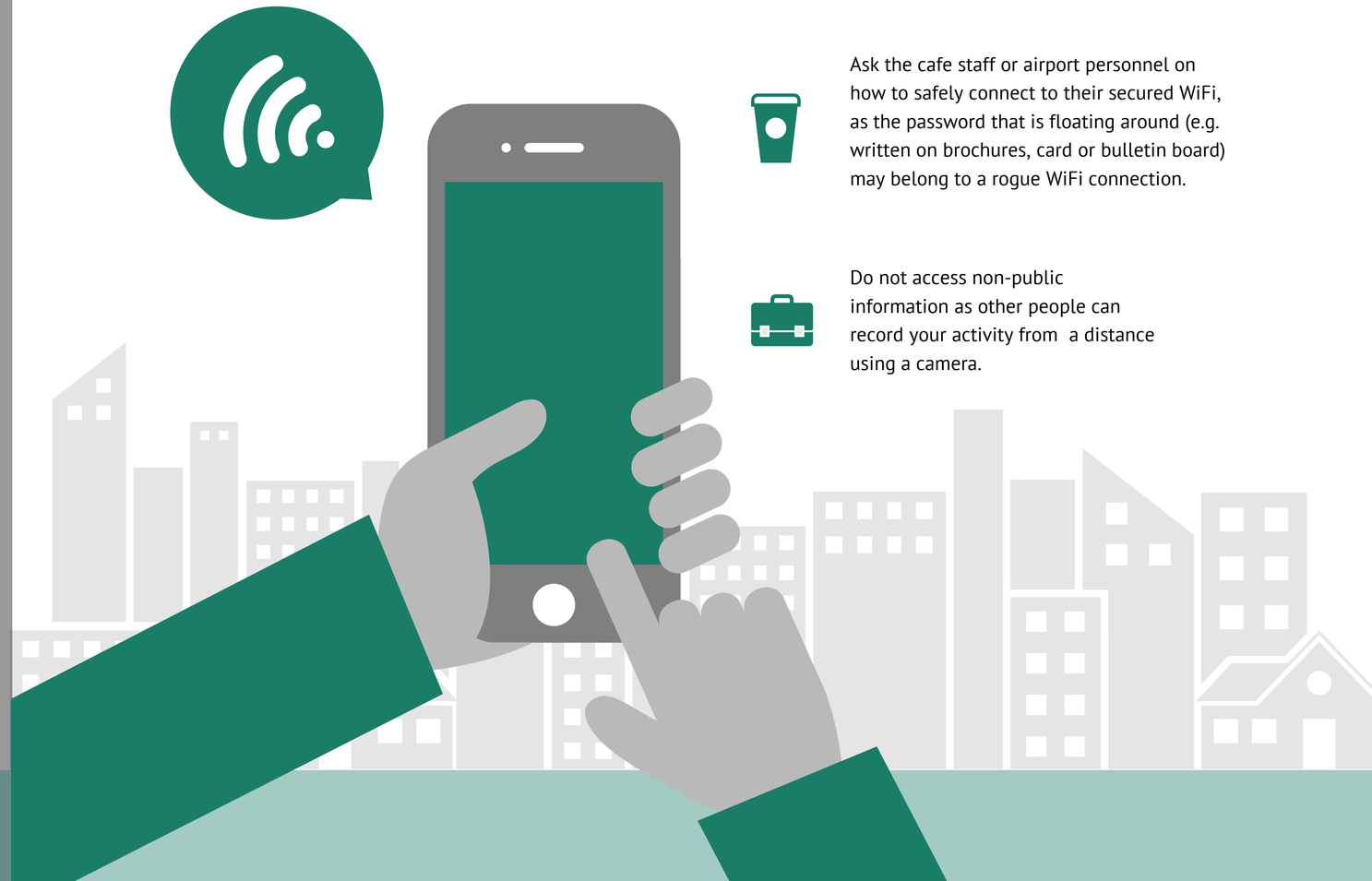
THINGS TO CONSIDER BEFORE CONNECTING TO A PUBLIC WIFI AND ACCESSING SENSITIVE INFORMATION

Do not connect to unsecured WiFi. Public places such as parks, airport terminals, buses and cafés, do offer free Internet access but are often targeted by criminals. Hackers can scan your Internet traffic by allowing you to connect to infected unsecured WiFi.

Never leave your laptop/mobile phone unlocked or unattended as criminals can transfer a virus to your device in seconds to record your future digital activities.

Ask the cafe staff or airport personnel on how to safely connect to their secured WiFi, as the password that is floating around (e.g. written on brochures, card or bulletin board) may belong to a rogue WiFi connection.

Do not access non-public information as other people can record your activity from a distance using a camera.

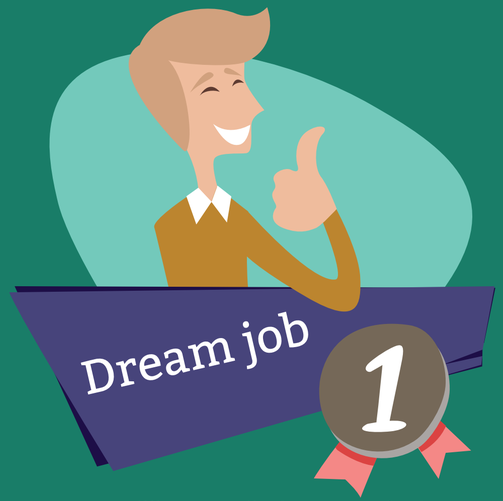


Need help? Call IT Service Desk on +44 (0)1202 9 65515.

Click Wisely

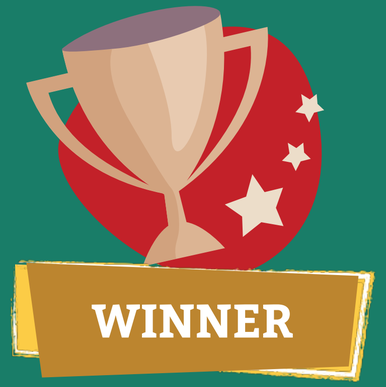
What to look out for

Can you really trust that link you're about to click on?



... offers of dream jobs,

Offers discounts and freebies,



... winning money or holiday trips,

or losing money or having your bank accounts closed.