AMNT: CYBER SECURITY TRAINING
5 OCTOBER 2017

Elisabeth Storey, Associate Director

To discuss

Question 1

Why the increase in risk?

Your cyber footprint

Question 2

Fraud risks

Question 3

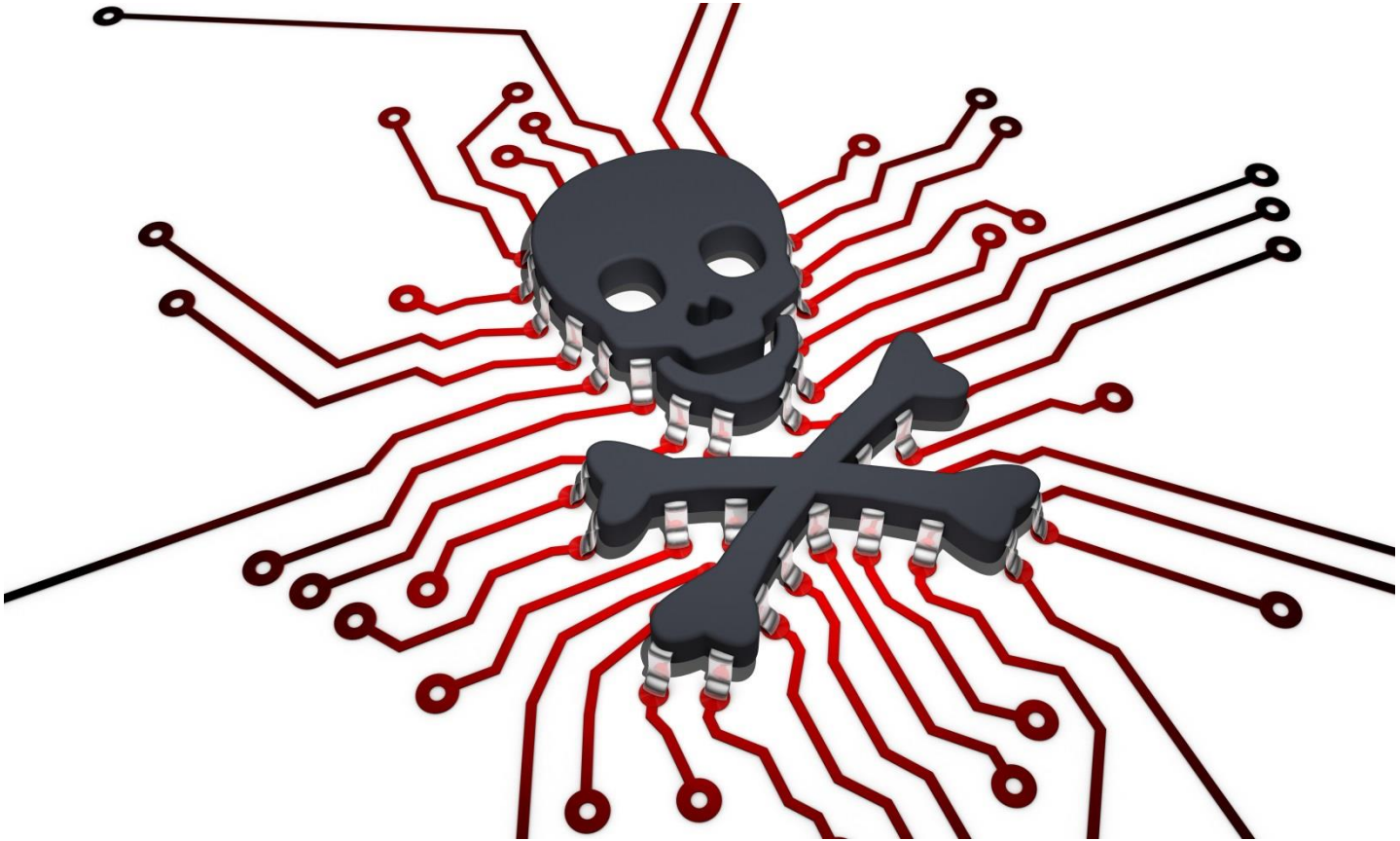
Phishing and whaling

Question 4

Good practice at work and home

Next steps and close

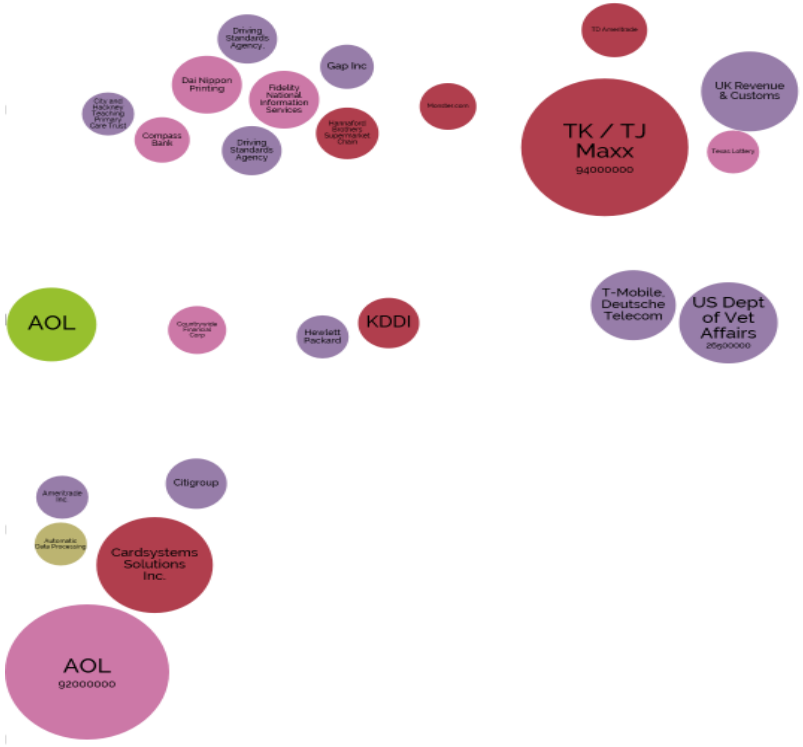
Question 1: Are you concerned about cyber risks?



Types of cyber risk

E-mail safety	Phishing and whaling	Social engineering	Online safety
Personal information	Social media	BYOD	Removable data
Information handling	Remote working	Mobile working	Password safety

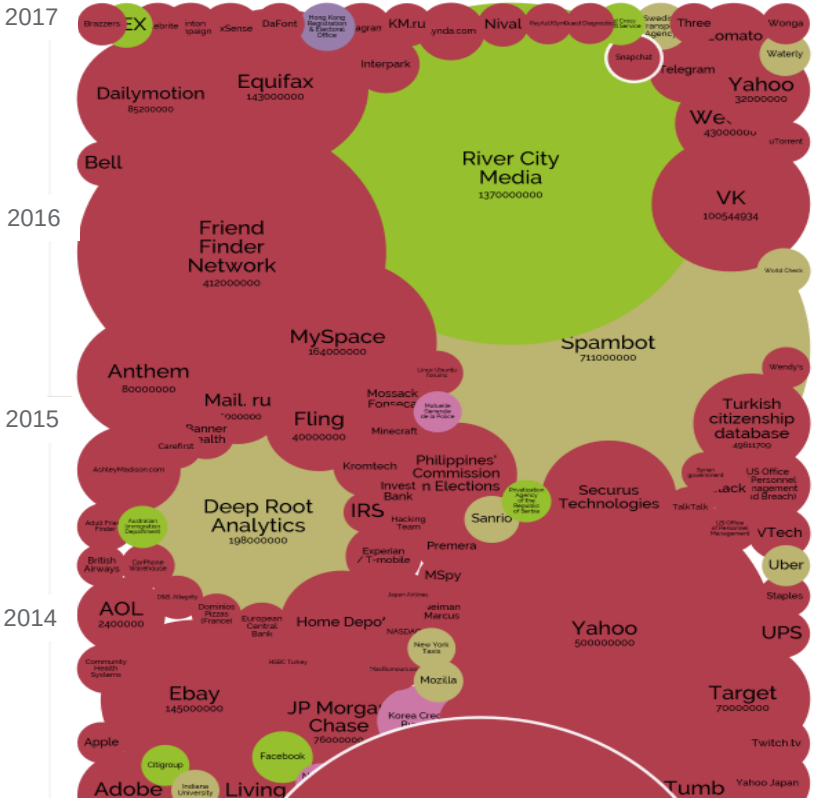
World’s biggest data breaches – 10 years ago



- accidentally published
- hacked
- inside job
- lost/stolen device or media
- Poor security

- Source: Information is Beautiful

World’s biggest data breaches – now



- accidentally published
- hacked
- inside job
- lost/stolen device or media
- Poor security

- Source: Information is Beautiful

Why the increase in risk?

Cybercrime has surpassed all other forms of crime in the UK – cyber enabled crime **36%** and computer misuse **17%**

(NCA's Cyber Crime Assessment 2016)

61% of data breach victims employed 1000 employees or less. **43%** of all attacks were social attacks.

(Verizon Data Breach Investigations Report 2017)

Human error is involved in more than **95%** of security incidents

(IBM's 2015 Cyber Security Intelligence Index report)

75% of data breaches were by external actors but **25%** were perpetrated by internal actors.

(Verizon Data Breach Investigations Report 2017)

There were approximately **5.6 million reported** incidents of fraud and cybercrime in the UK in 2016

(UK Office of National Statistics)

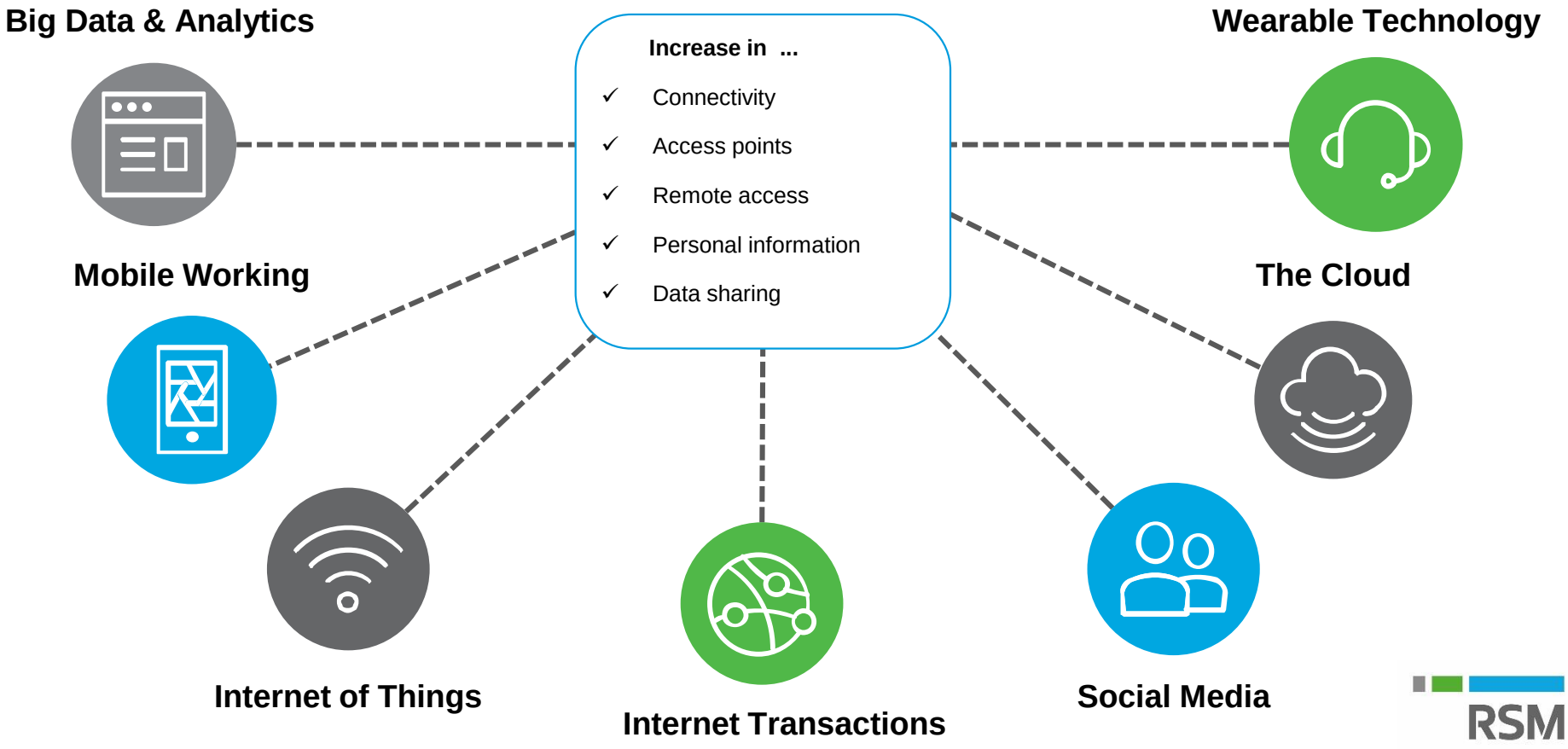
"Within the last year, **65%** of large UK firms detected a cyber security breach or attack."

(UK National Crime Agency and National Cyber Security Centre, March 2017)

"Why would they attack us?!"

RSM

Why the increase in risk?

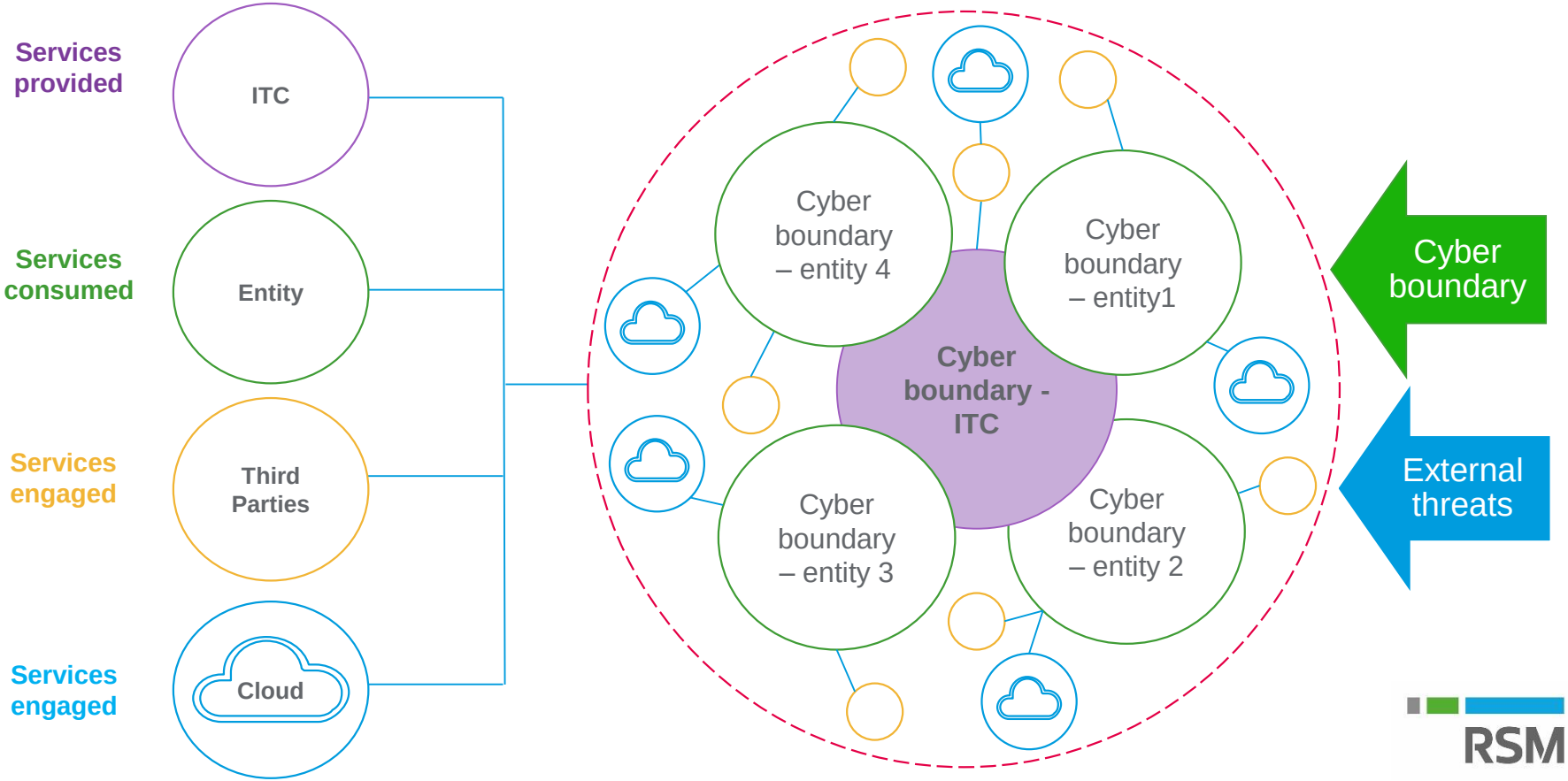


Cyber crime is increasing – why?

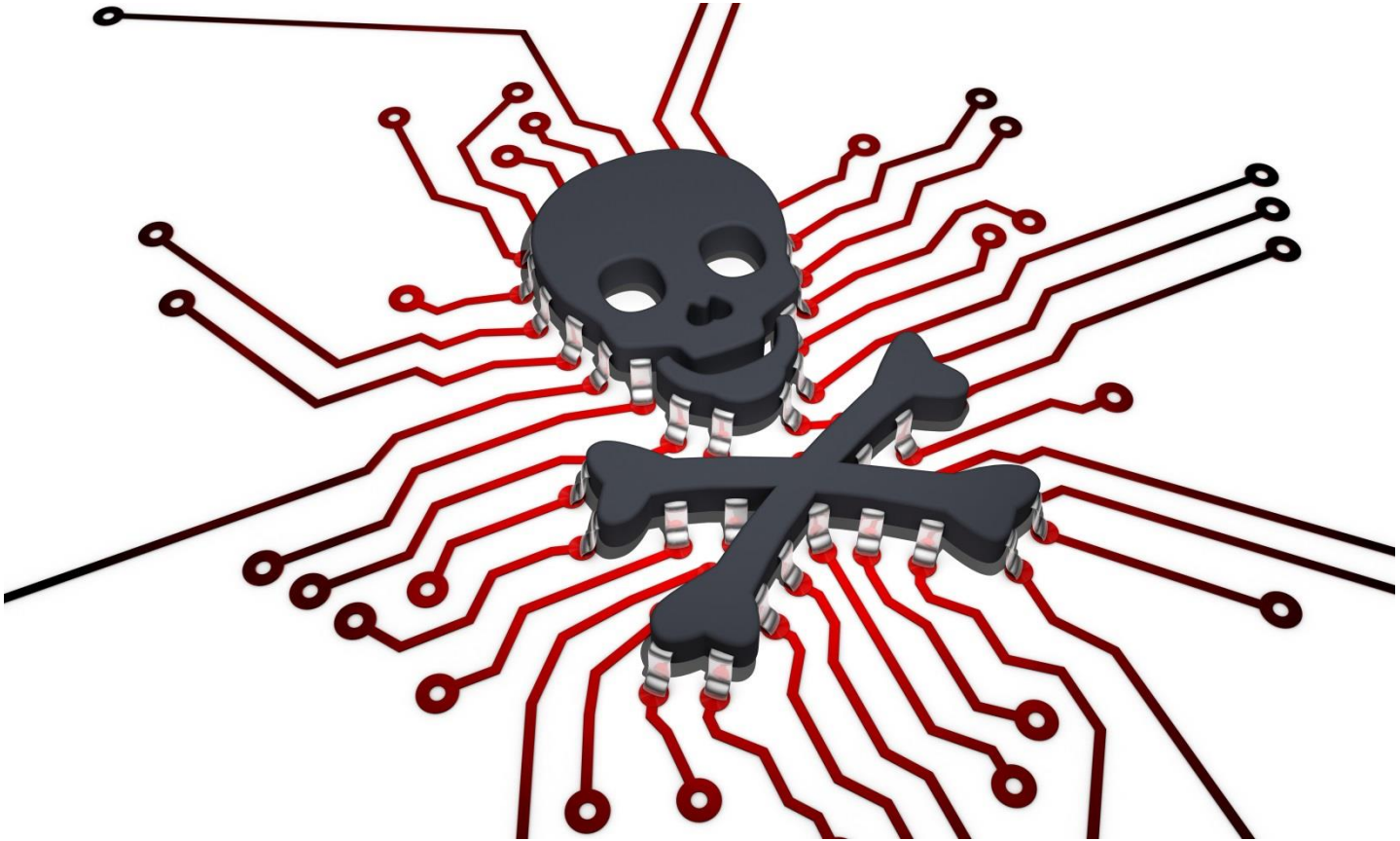
The inherent risks

- Increasing digitisation of information, network connections, dependencies, and trust relationships
- Increasing sophistication of attackers
- Increased processing power and decreasing cost means increasing attack frequency
- Staff have the information the attackers want – so they need to be educated
- Growth of the dark web as a market
- Rapid growth of social media
- Under reporting
- Lack of understanding of the entity's cyber footprint

Your cyber footprint



Question 2: Do you know your cyber footprint?



Types of fraud – how many do you know about?

…and the list goes on

ActionFraud
National Fraud & Cyber Crime Reporting Centre
0300 123 2040

Identity fraud can be described as the use of a stolen identity in criminal activity to obtain goods or services by deception. Stealing an individual's identity details does **not**, on its own, constitute identity fraud. But using that identity for criminal activities does.

Action Fraud

Web Site

RSM

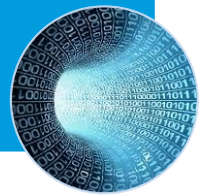
Typical examples

- Transfers – commission scams
- Transfers – bogus investments

Scams

- Pensions
- Lump sums
- Transfers

National Insurance numbers



- Pensions
- Death benefits

Impersonation

Example

This is MONEY.co.uk
FINANCIAL WEBSITE OF THE YEAR

Criminals gained remote access to his computer

They called his bank and by using his stolen online details got his address and contact numbers changed

They hacked his BT account on his PC and emailed BT to redirect his home address to theirs in Manchester

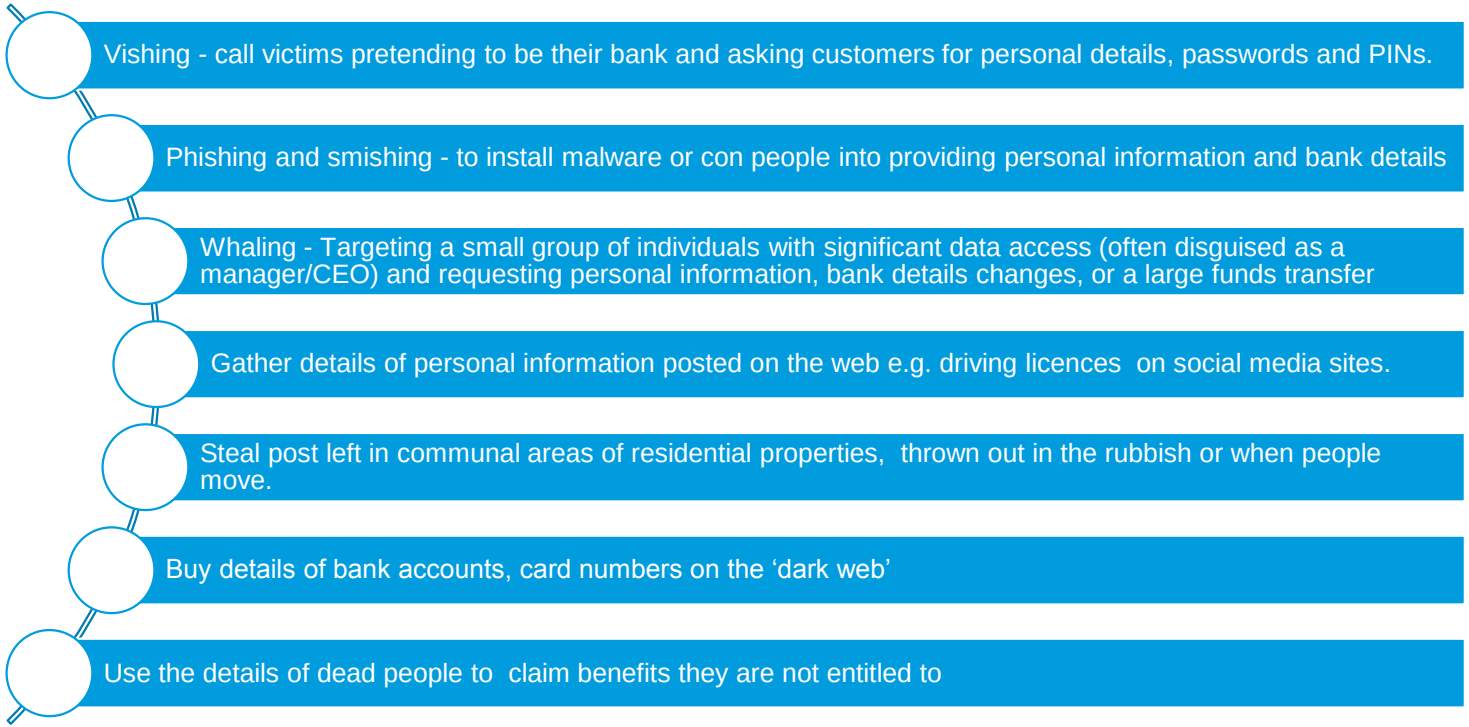
They hacked his Facebook and asked his friends via direct messages for money. One transferred £900 to a bank account

He personally lost £2,400 over the counter and £300 from a cashpoint.

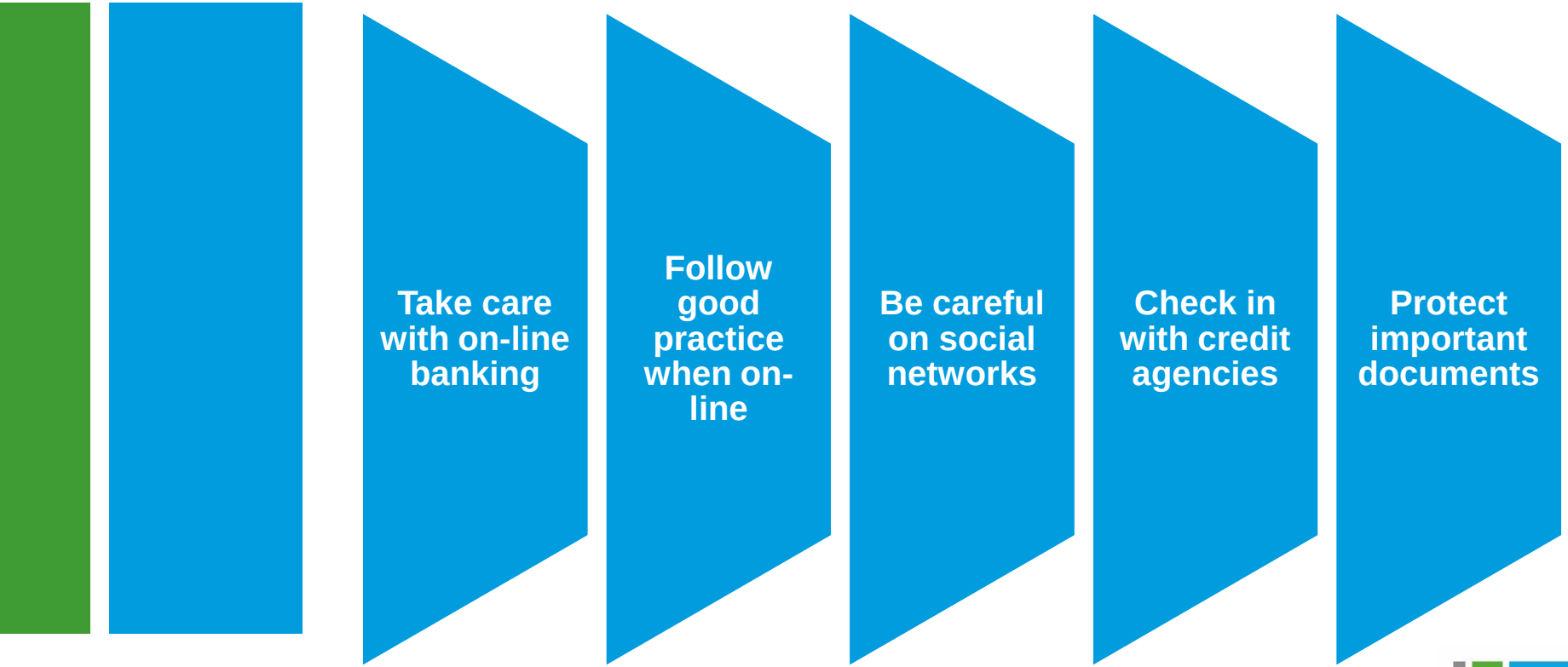
The case of a victim known only as Chris, who had thousands stolen by fraudsters who simply rang his bank to gain details and also conned his Facebook friends into sending money too, is highlighted by Get Safe Online.

RSM

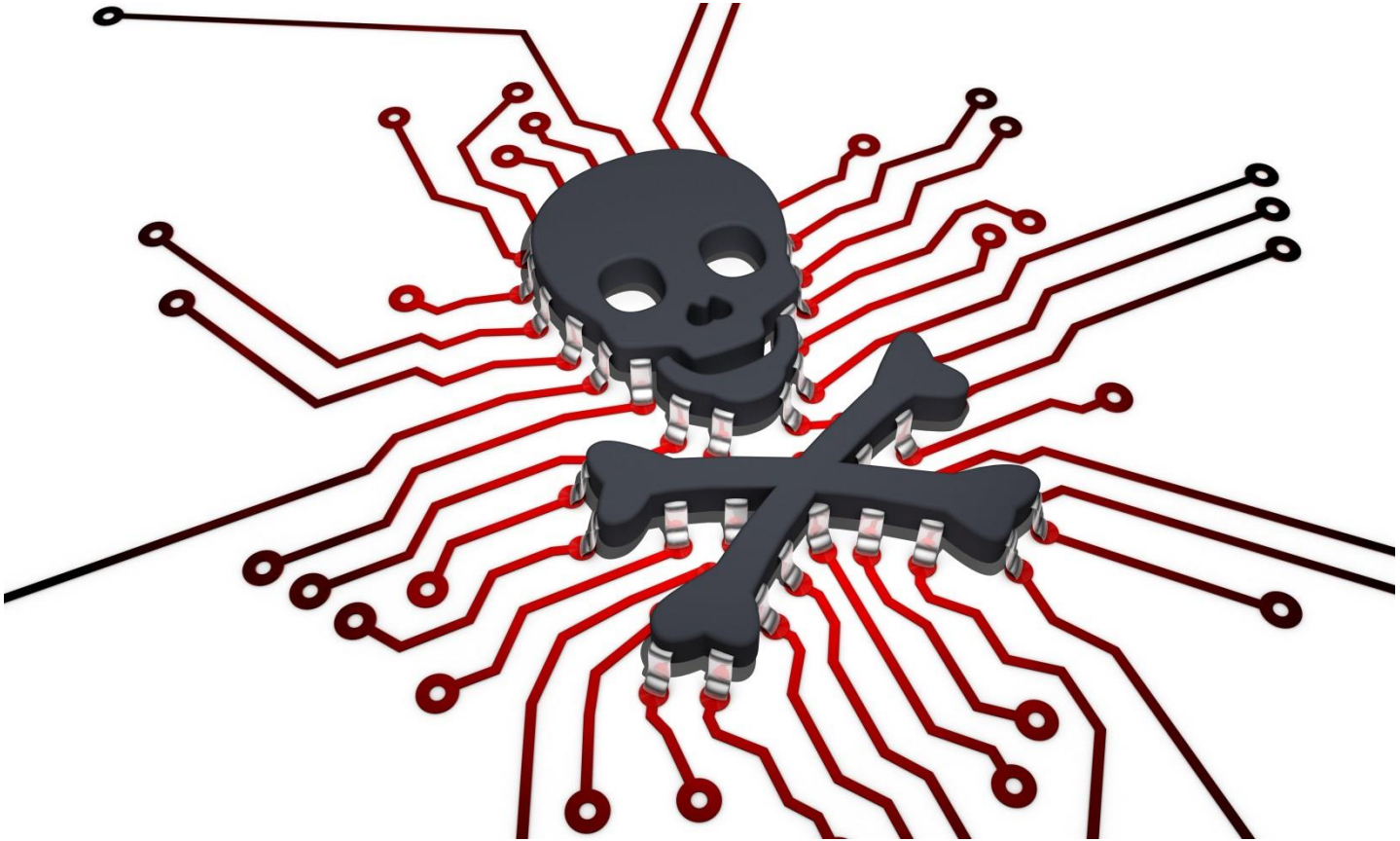
What do identity fraud thieves do?



Prevention advice



Question 3: Would you recognise a malicious email?



What is phishing and whaling?

Phishing

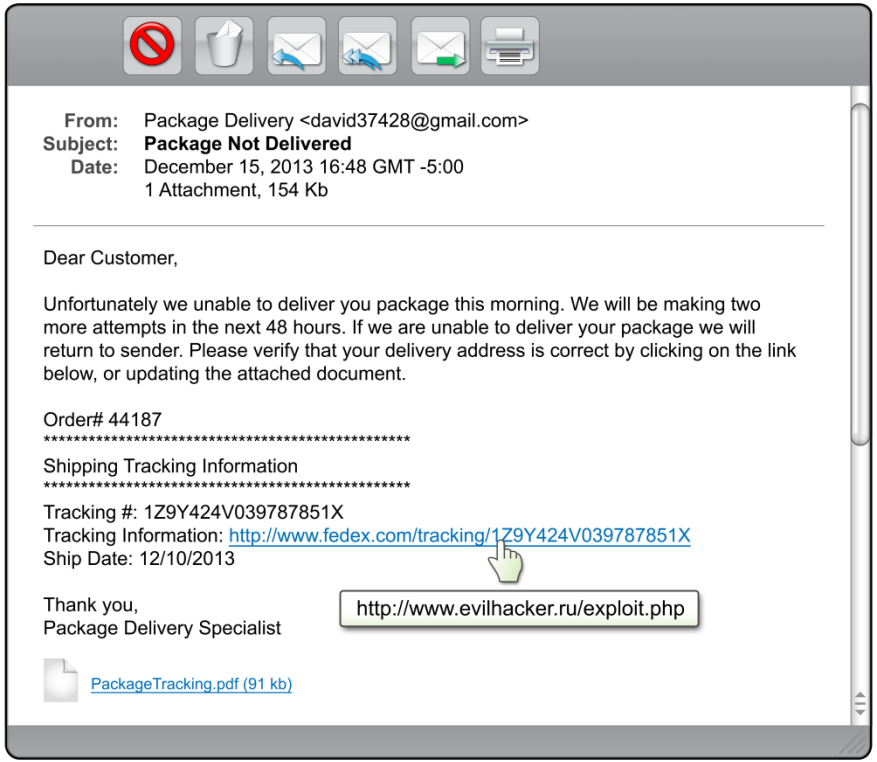
- Targeting many individuals, mainly with blanket e-mails, and hoping that some will follow links, open attachments, reply with information, or transfer funds

Whaling

- Targeting a small group of individuals with significant data access (often disguised as a manager/CEO) and requesting personal information, bank details changes, or a large funds transfer

RSM

Malicious content - ransomware



From: Package Delivery <david37428@gmail.com>
Subject: **Package Not Delivered**
Date: December 15, 2013 16:48 GMT -5:00
1 Attachment, 154 Kb

Dear Customer,

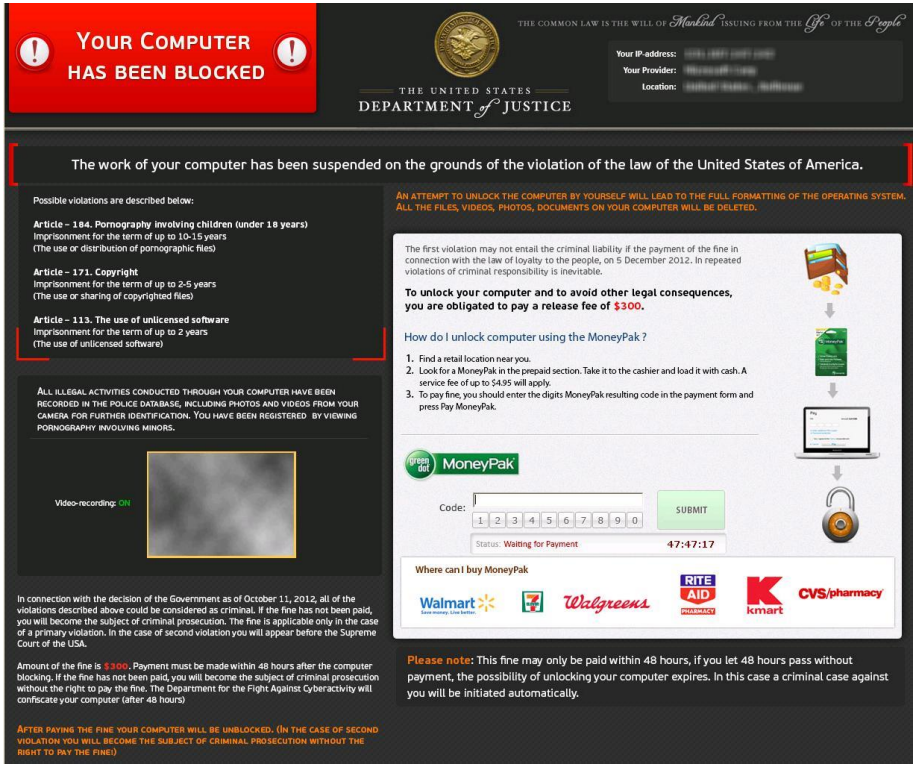
Unfortunately we unable to deliver you package this morning. We will be making two more attempts in the next 48 hours. If we are unable to deliver your package we will return to sender. Please verify that your delivery address is correct by clicking on the link below, or updating the attached document.

Order# 44187
****
Shipping Tracking Information
****
Tracking #: 1Z9Y424V039787851X
Tracking Information: http://www.fedex.com/tracking/1Z9Y424V039787851X
Ship Date: 12/10/2013

Thank you,
Package Delivery Specialist

http://www.evilhacker.ru/exploit.php

PackageTracking.pdf (91 kb)



Example

This is MONEY.co.uk
FINANCIAL WEBSITE OF THE YEAR

HOW ONE GANG SWIPED $1BN FROM GLOBAL BANKS

Up to US$1billion - £650million - has been stolen in approximately two years from financial institutions worldwide.

The fraud was detected by cyber security firm Kaspersky Lab in February 2015.

Gained entry into an employee's computer through 'spear phishing' – infected it with malware called Carbanak.

↓

Sent authentic-looking emails from his account that other staff clicked on, spreading the malware through the bank.

↓

Found the administrator account for the CCTV equipment

↓

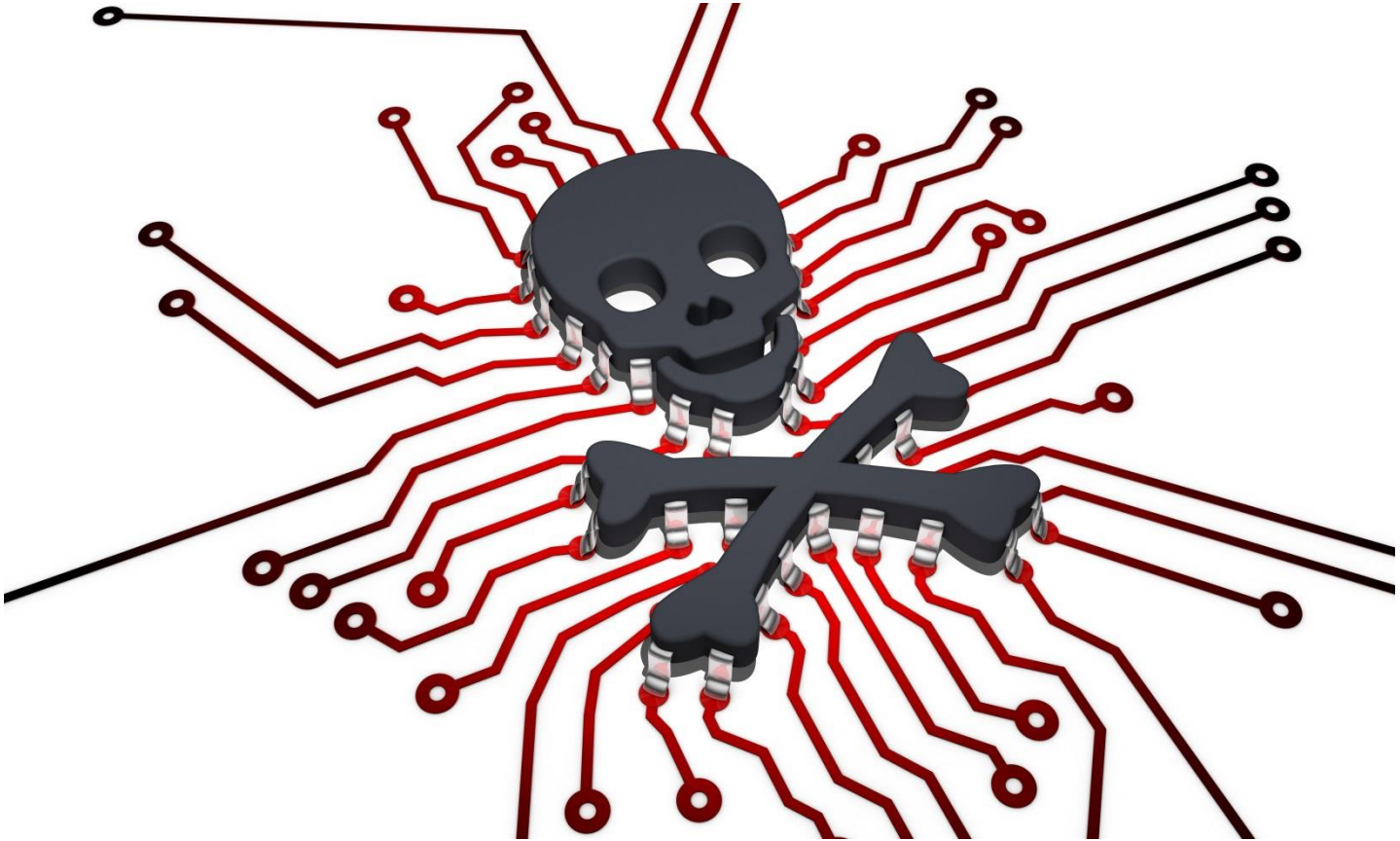
They used the CCTV to record everything that happened on the screens of staff who serviced the cash transfer systems.

↓

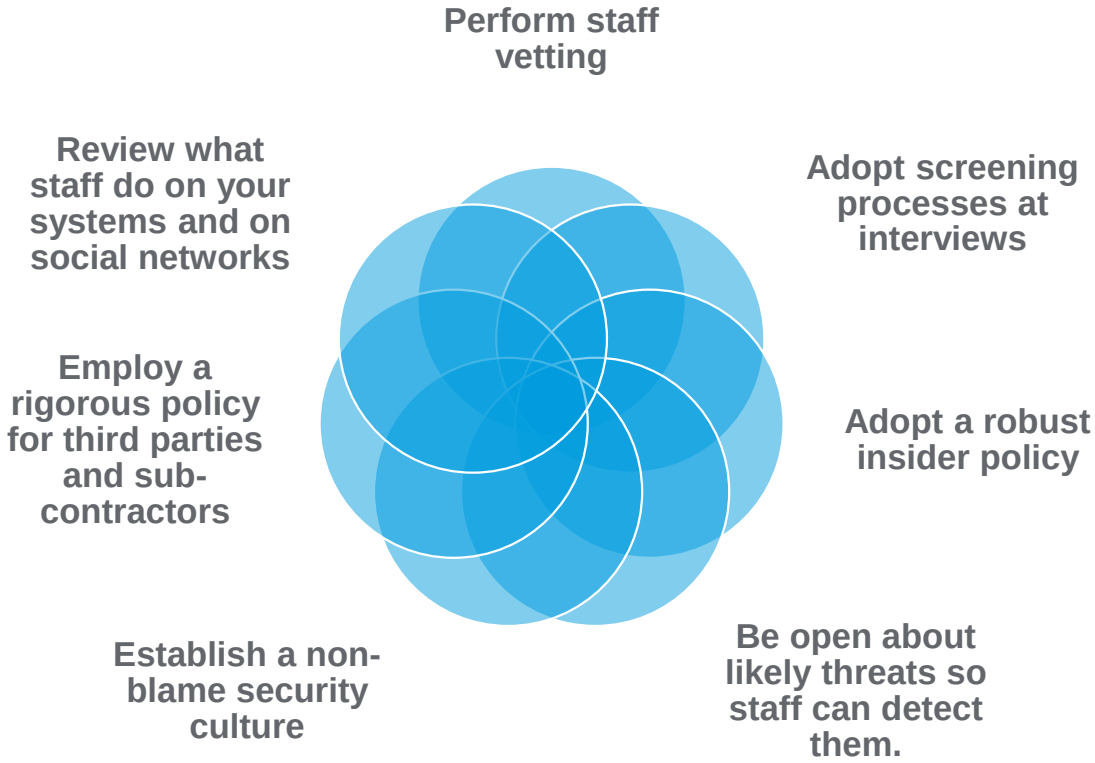
They mimicked the activity of these staff activity in order to transfer money out.

RSM

Question 4 – What action can you take?



Good practice at work – Board level



What do Trustees need to do?

Translating cyber risk management into practical next steps:

- make this a board level issue;
- consider your risks: both your people and third party risks;
- consider data scrubbing;
- implement good IT general controls in depth;
- review your policies and procedures;
- ensure you will be GDPR ready by May 2018;
- provide rolling education and training e.g. on the use of social media;
- foster a no-blame culture;
- keep your firewalls, operating systems, virus engines up-to-date;
- password protect the Wi-Fi;
- have a formal Incident Management Plan for **when** the worst happens;
- consider compliance with Cyber Essentials;
- consider cyber insurance;
- check physical site controls;
- review controls against social engineering generally; and
- penetration tests.

Good practice: people in your cyber footprint

Every person in your cyber footprint should:

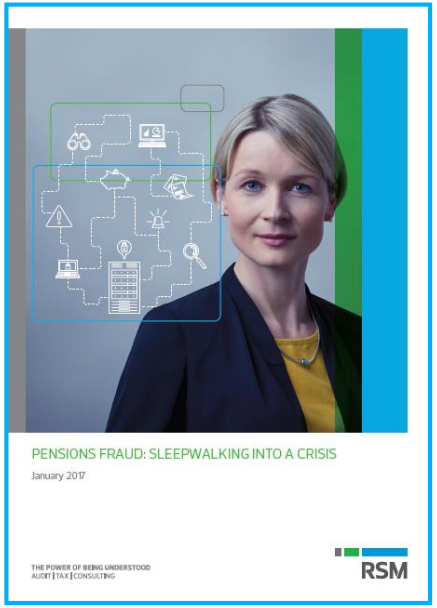
- Read policies and procedures
- Keep up-to-date with education and training
- Be aware of unusual phone calls, e-mails or texts
- Verify contacts
- Take care with requests to change bank details
- Accept all security up-dates to your PC as soon as possible
- Don't click on links – type in the URLs to verify authenticity
- Report anything suspicious to management immediately
- Be careful on social media
- Change passwords regularly
- Have strong and different passwords for different accounts
- Be careful with portable media
- Check security certificates, especially for payment websites

If it doesn’t smell right, it probably isn’t right!

Questions for Trustees

Areas for consideration:

- Is cyber security on the risk register and in what guise?
- Has the risk been appropriately assessed and has it been rigorously tested?
- Do trustees use portable devices to access board papers?
- Do trustees use home computers? How secure are they?
- Have trustees been given sufficient training in order to understand and assess risks?
- Does the administrator have an internal controls report and does it sufficiently detail IT risk?
- If a breach occurs, would the administrator have to tell the trustees? What is covered in the contractual arrangements and when were they last reviewed?
- What controls are in place to check a member's identity when benefits are being claimed?
- Do Trustees have an Incident Management Plan?
- Are Trustees in a position to report personal data security breaches to the ICO within 72 hours (with a risk management review)?



RSM

Next steps and close

Summary

5 principles

Remember the worth of your data to others

Establish what good practice looks like for you

Staff remain the weak link

Strength in depth for IT controls: don’t ignore importance of good basic controls

Effective incident management is key to maintaining reputation

RSM

Further information

Some useful sites

- **Action Fraud** - www.actionfraud.police.uk
- **UK Cyber Security Forum** - www.ukcybersecurityforum.com
- **Information Security Forum** - www.securityforum.org
- **National Crime Agency** - www.nationalcrimeagency.gov.uk/crime-threats/cyber-crime
- **Cyber UK** - www.cyber.uk

Questions and answers?

Contact details

Elisabeth Storey

Associate Director, London

elisabeth.storey@rsmuk.com

0203 201 8314

For more information visit www.rsmuk.com