COMMERCIAL BANKING

Fraud Guidance

Helping to protect you and your business

For your next step

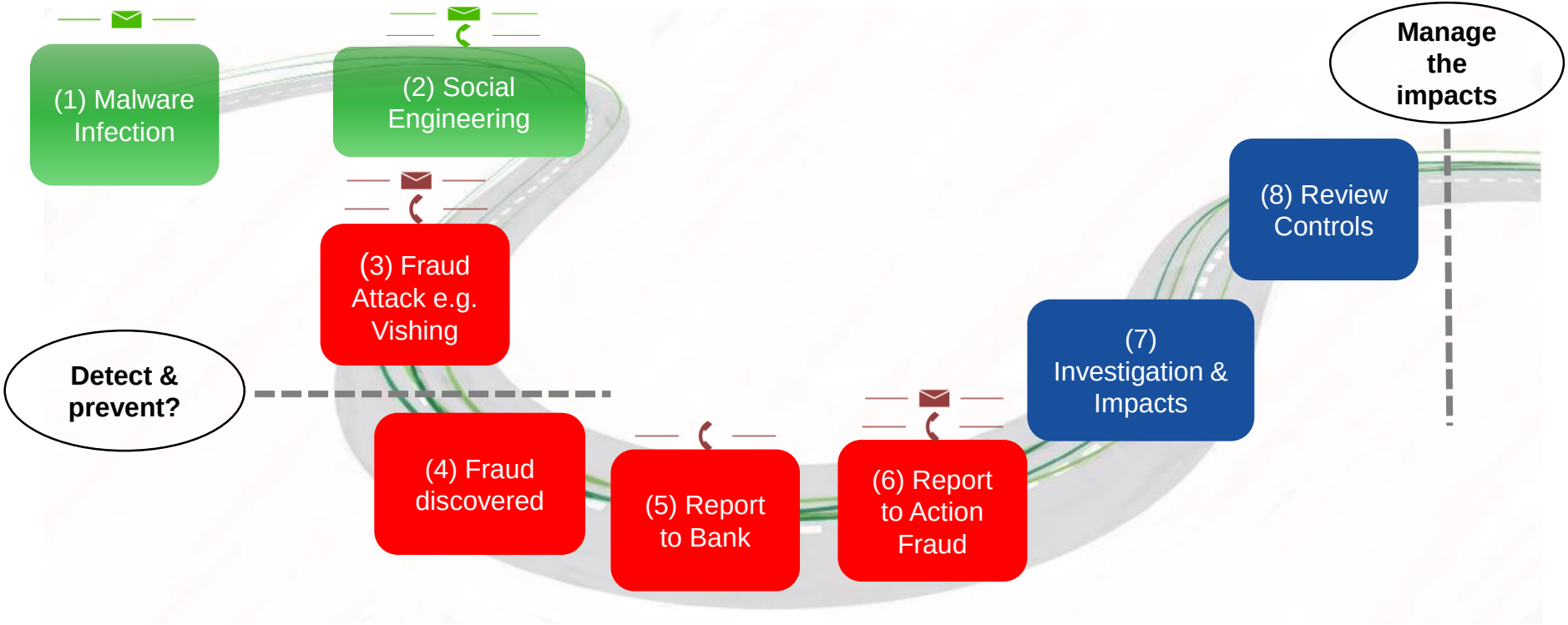
LLOYDS BANKING GROUP


EVERY
15 seconds
THERE IS AN INCIDENT OF
FINANCIAL FRAUD IN THE UK
Can you say with
certainty that you or your
business have never
been a victim?
Source: Financial Fraud Action UK (FFA UK) September 2016

THE JOURNEY OF A FRAUD EVENT CAN TAKE MONTHS FROM INCEPTION TO CONCLUSION

LLOYDS BANKING GROUP

Organised Fraud Groups are prepared to wait until the optimum time to strike.



THE TRUE COST OF FRAUD TO VICTIM ORGANISATIONS

Implications can be wide ranging and far reaching.

Amount stolen	• TYPICAL MID SIZED BUSINESS FRAUD - £35,000
Reputation	• £???
Time to investigate	• £???
Staff morale	• £???
Disruption	• £???
Total cost	• £££££ (Significantly more than the amount stolen!)

KEY FACTORS INFLUENCING VULNERABILITY

There are some key factors that influence the extent of an organisation's vulnerability.

- The level of fraud risk awareness by payment clerks/teams
- Quality of cyber security, hygiene and ongoing critical patch management
- Multiple access to applications and data
- Effectiveness of controls, procedures and processes and how well they are embedded
- Staff training and testing

SOCIAL ENGINEERING

Social engineering refers to psychological manipulation of people into performing actions or divulging confidential information.
A type of confidence trick for the purpose of information gathering, fraud, or system access.

HOW PRIVATE IS YOUR INFORMATION?

How secure is the information posted by your employees and is reference to your organisation appropriate?

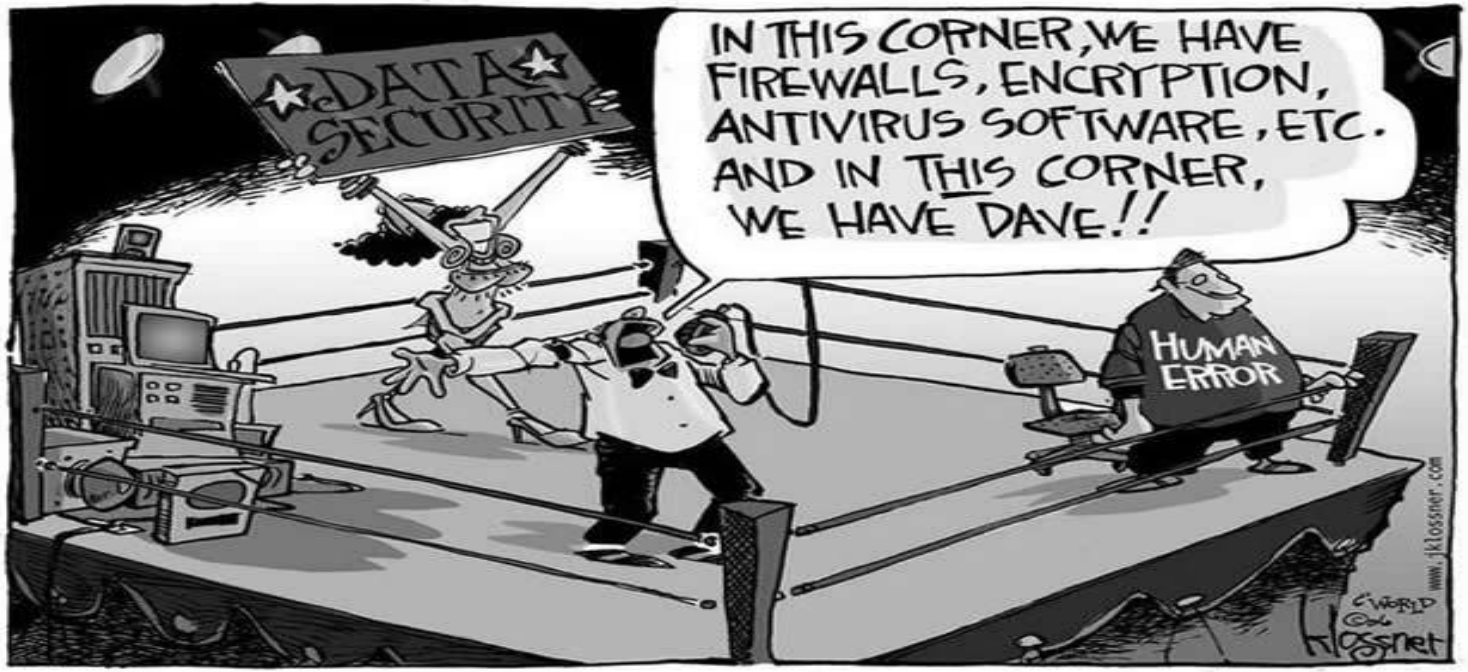
- CIFAS pop-up coffee shop experiment
- https://www.youtube.com/watch?v=yrjT8m0hcKU

TYPES OF APPROACH

Social engineering attacks can come via email, social media, phone, text and through planted hardware

APOLOGIES TO ALL DAVES

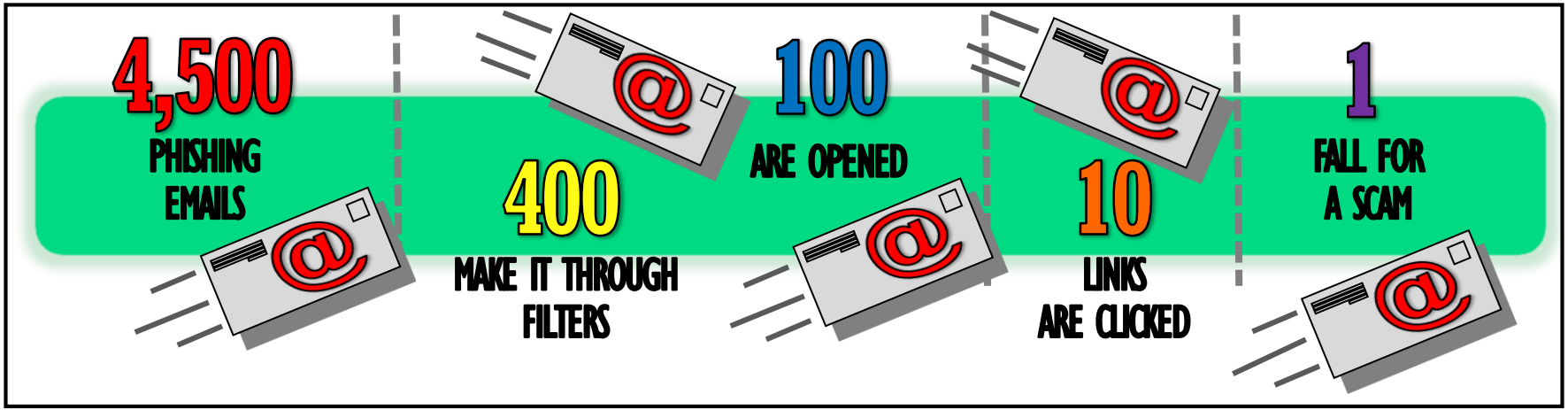
Education & Awareness is Important



THE MOST COMMON FORM OF MALWARE DISTRIBUTION IS THROUGH PHISHING EMAILS

LLOYDS BANKING GROUP

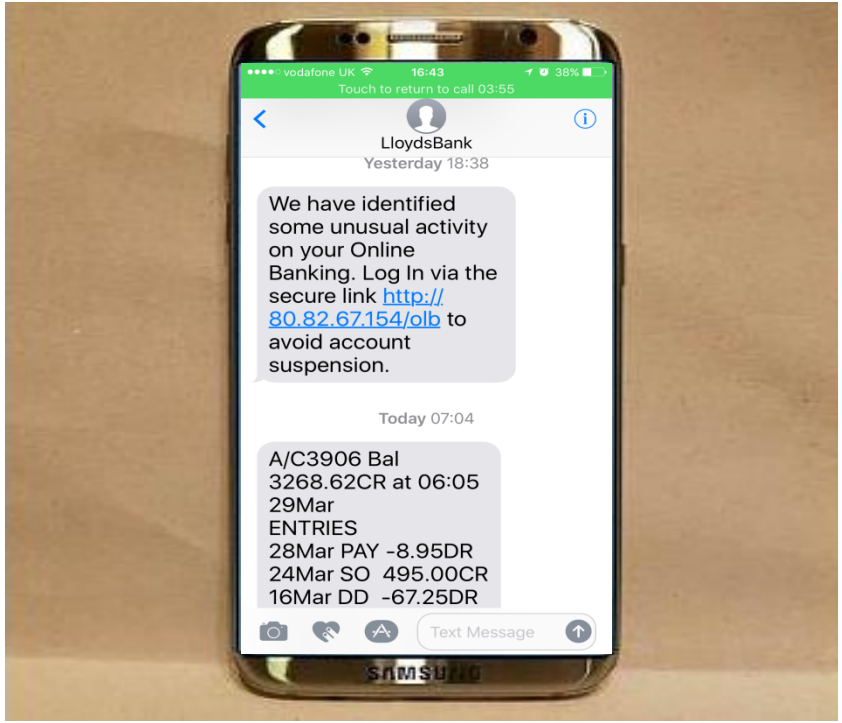
It's essential to make sure that staff are alert to the threat.



- Distribution also via malvertising; external media devices; macros
- Quality of cyber security, hygiene and ongoing critical patch management
- Staff awareness, training and testing. Repeat, repeat, repeat!

SMISHING (SMS SCAM) IS A RECENT FRAUD TARGETING UK ENTITIES

The fraudster's objective is to harvest credentials to be able to access the victim's bank account



VISHING (TELEPHONE SCAM) – HOW A FRAUDSTER APPROACHES HIS TARGET

Be alert to the tricks:-

- Spoofing technology
- Open line

PRACTICAL STEPS THAT YOU CAN IMPLEMENT TO PROTECT YOUR BUSINESS FROM VISHING

Raising awareness and effectively training your staff is critical to strengthen your fraud defence against these attacks

- Raise awareness with all staff. Have clear procedures for staff to follow
- Independently authenticate calls
- Don’t assume it is the bank, regardless of what they know!
- Dual authorisation to set up and authorise payments
- Remind all staff that the Bank will never ask for:-
  - full password or full memorable information log on details
  - card & reader authentication codes

RANSOMWARE HAS INCREASED EXPONENTIALLY IN THE PAST 12 MONTHS

It's proving to be a very lucrative and attractive fraud type attacking businesses across all sectors and sizes.

No guarantee if the ransom is paid

Visit 'No More Ransom!' website

Disruption caused by the need to forensically clean or rebuild system

HAVING A RANSOMWARE PREVENTION STRATEGY IS VITAL

A robust contingency plan will help your business avoid having to face the dilemma of deciding whether to pay a ransom or not.

- No guarantee of recovery if the ransom is paid
- Back up your files regularly to an independent source
- Forensic cleansing required post incident & prior to running data recovery
- Effective IT boundary security management & staff awareness. ‘Think Before You Click’!
- System/application access – point of least privilege!

CONNECTING TO FREE WI-FI CAN BE CONVENIENT, BUT ALSO VERY DANGEROUS!

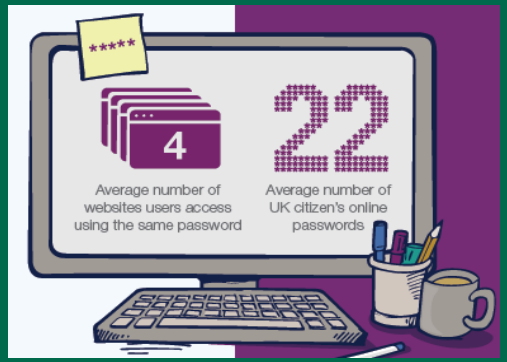
It’s not difficult for hackers to eavesdrop into your internet session.

Password Security – attackers use a variety of techniques to discover passwords

Providing advice and guidance for your users will help to improve your system security

- Train staff to avoid using easy to guess/predictable passwords
- Encourage use of pass phrases
- Never re-use passwords between home and work
- Only change on indication of suspicion of compromise

- Don’t store passwords in plain text format



INVOICE FRAUD AND BUSINESS EMAIL COMPROMISE (CEO) FRAUD

These types of fraud are very lucrative.

Invoice Fraud accounts for:

37% of reported fraud losses borne by business customers.

Business Email Compromise (CEO) Fraud accounts for:

35% of reported fraud losses borne by business customers.

SIGNIFICANT INCREASE IN BUSINESS EMAIL COMPROMISE/CEO FRAUD

Police issue warning asking all UK businesses to be on alert.

- Impersonation by hacking into or spoofing a business owner or senior executive's email account.
- Instruction to invoice clerk or payments team. Urgent payment to specified account.
- Take advantage of employee's instincts of trust, fear and obedience.
- Replicating terminology the sender would ordinarily use.
- Unable to contact the sender to verify.

MANDATE/INVOICE SCAMS

Mandate/invoice scams are very active frauds targeting all industry sectors.

- Instruction from supplier to change bank account details.
- Research and pre-attack phone calls to add legitimacy.
- Build trust/relationship with the invoice clerk or Finance team.
- Redirection of all future payments. Delay before fraud is discovered.
- Time to move the money. Slim chance of recovery.

EMAIL INTERCEPTION COMPROMISING ELECTRONIC INVOICES IS EMERGING

Intelligence to date indicates activity initially instigated by West African fraud ring compromising businesses domiciled in the Far East is spreading.

- Email system compromise. SMTP DNS poisoning.
- Attacker monitors email traffic looking for pre order correspondence.
- Email between buyer and seller containing invoice intercepted.
- Beneficiary bank account details altered.
- Spoofs seller/vendor email address to send amended instruction.

STAFF AWARENESS IS A VITAL CONTROL IN PREVENTING A BUSINESS FALLING VICTIM

Well trained staff significantly increase the chances of an attack being detected and prevented.

- Be cautious, remain vigilant. Hover over the email address
- Staff awareness, training, repetition and testing
- Authenticate the instruction using a different channel. Especially for new payments. Documented procedure. **CULTURE!**
- Raise stakeholder awareness
- Report to the bank and Action Fraud

Are they really who they say they are?

THE ‘TAKE FIVE’ CAMPAIGN PROVIDES VERY PRACTICAL FRAUD PREVENTION TIPS

It is strongly recommended that all employees are familiar with these basic principles.

- Never disclose security details such as your PIN, full Password or Card/Reader codes
- Don’t assume an email request, letter or caller is genuine
- Don’t be rushed – a supplier or genuine organisation won’t mind waiting to give you time to stop and think
- Listen to your instincts
- Stay in control

FRAUD PREVENTION – ADOPTING A LAYERED APPROACH IS STRONGLY RECOMMENDED

It's prudent to work on the premise that one layer will be circumvented.

CHEQUE FRAUD

The illegal use of cheques to acquire funds.

HOW CAN CHEQUE FRAUD AFFECT YOUR SCHOOL?

Cheque fraud can happen in a few different ways. Criminals can steal cheques, create fraudulent cheques or change the name or amount on a legitimate cheque.

COUNTERFEIT CHEQUES are copy cheques, printed to look exactly like your genuine cheques.

FORGED CHEQUES are genuine cheques that have been stolen and used by a fraudster with forged signatures.

ALTERED CHEQUES are genuine cheques issued by the school. Either the fraudster will intercept the cheque and alter it in some way before they try to pay it in e.g. by altering the beneficiary's name and/or the amount, or they will be the genuine payee but might try to increase the amount payable to them on the cheque.

CHEQUE SCAMS A cheque you are not expecting, or for an amount more than you require, is paid into your account by a fraudster presenting themselves as a genuine payer. The fraudster then asks for the overpaid funds to be returned. After you have done this, the cheque is returned as fraudulent.

CHEQUE FRAUD – WHAT ACTIONS CAN YOU TAKE TO PROTECT YOUR SCHOOL

LLOYDS BANKING GROUP

ISSUING CHEQUES

- **Cross through spaces on cheques you issue e.g. after the payee name and the amounts (words and figures).**
- Use a **printer** which is recommended for cheques.
- Always use a black or blue ballpoint or a pen with **indelible ink** so that writing cannot easily be erased or altered. **Apply more pressure** with the pen tip than normal, to make the writing difficult to remove.
- E**nter ZERO** rather than NIL, which can be changed to NINE.
- Write **full payee names** rather than acronyms e.g. Department for Education rather than DfE.

CHEQUE FRAUD – WHAT ACTIONS CAN YOU TAKE TO PROTECT YOUR SCHOOL

LLOYDS BANKING GROUP

BEST PRACTICE

- Consider whether cheque is the best method for the payment. Online payments, BACS, CHAPS can be faster and more appropriate.
- **Reconcile** cheque payments to statements and report inaccuracies immediately.
- Keep cheque books **secure.**
- Make sure cheques can‘t easily be recognised in the **post** – especially if window envelopes are used.
- Look out for cheques that have been removed from the **middle or back** of your cheque book

CRIMINALS USE MONEY MULES TO PROCESS STOLEN FUNDS

The account holders who allow their bank accounts to be used for this purpose are recruited in a variety of ways

Met Police warn fraudsters are targeting child 'money mules'

Children are being targeted by criminals to act as money mules, police have warned.

SCAMSPOTTING

Video created by the students of the Sheffield Universities.

https://vimeo.com/208179201

FIND OUT MORE

For more information about how to protect your business from fraud, visit:

www.lloydsbank.com/fraud
www.lloydsbank.com/business

or contact your relationship management team.

For external support:

www.actionfraud.police.uk
www.getsafeonline.org
www.cyberaware.gov.uk

Reducing these risks – Phil's Top Tips

- On-Line Banking
  - Who has access? / Policy for changing supplier data
- No cheque books in school
- Stand alone computer for on-line banking
- Cashless School (On-Line & PayPoint Payment options for Parents)
- Care with email hyperlinks
- Care with social network content
- Frequent back-ups of data
- Keep anti-virus software up to date
- Cyber Crime Insurance?
- Check all Invoices are genuine.
- Franking machine Logos

Your Bank will **never** call you to request user name, password details or challenge/response codes