RBS Group

Fraud Awareness & Prevention

Derek Cooke
CIPFA Scottish Treasury Management Forum
28th February 2014

Agenda

1. **Introduction**
2. **Spotlights**
   - Banking malware & Trojans
   - Social engineering
   - Invoice Fraud
   - Insider Fraud
   - Cheque Fraud
3. **Summary**
4. **Q&A**

Criminal HQ !

The ‘Facts’

30%

Victim of fraud over last 12 months …
… and rising.

£4k

Average annual cost to small businesses of fraud and online crime

73%

Have **not** been a victim of Online fraud …
… or Have they?

20%

Have staff training to minimise + prevent fraud … What about other 80%?

Source: FSB Cyber Security & Fraud – Impact on small businesses

Cost of Fraud - NFA Annual Fraud Indicator

Figure 1: Identified fraud loss estimates by victim

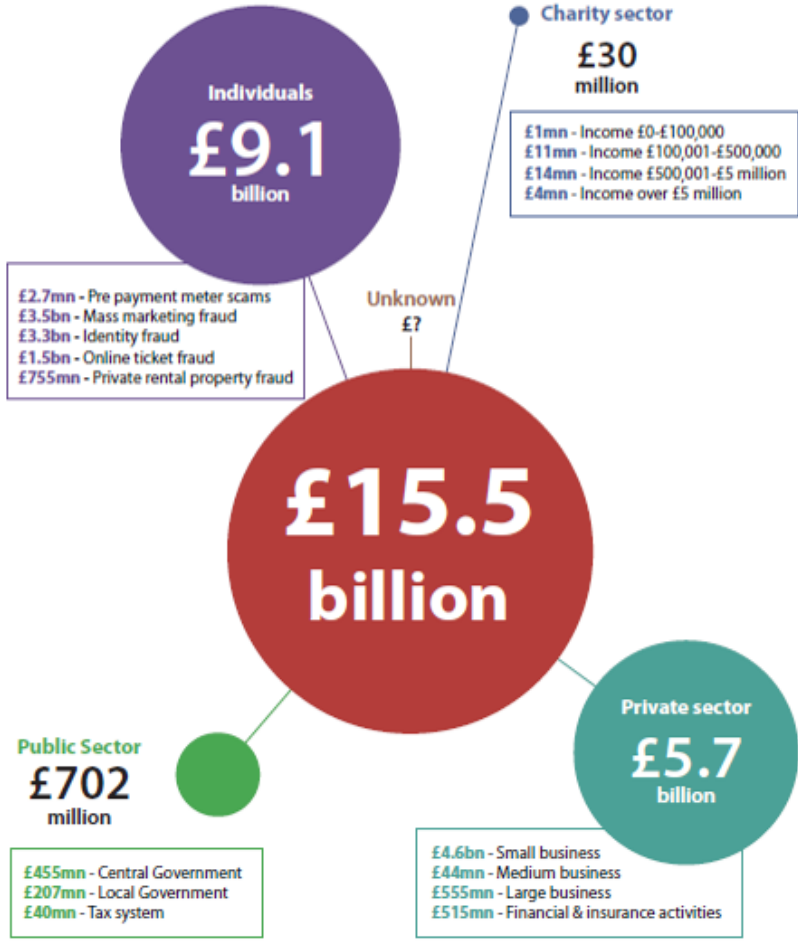
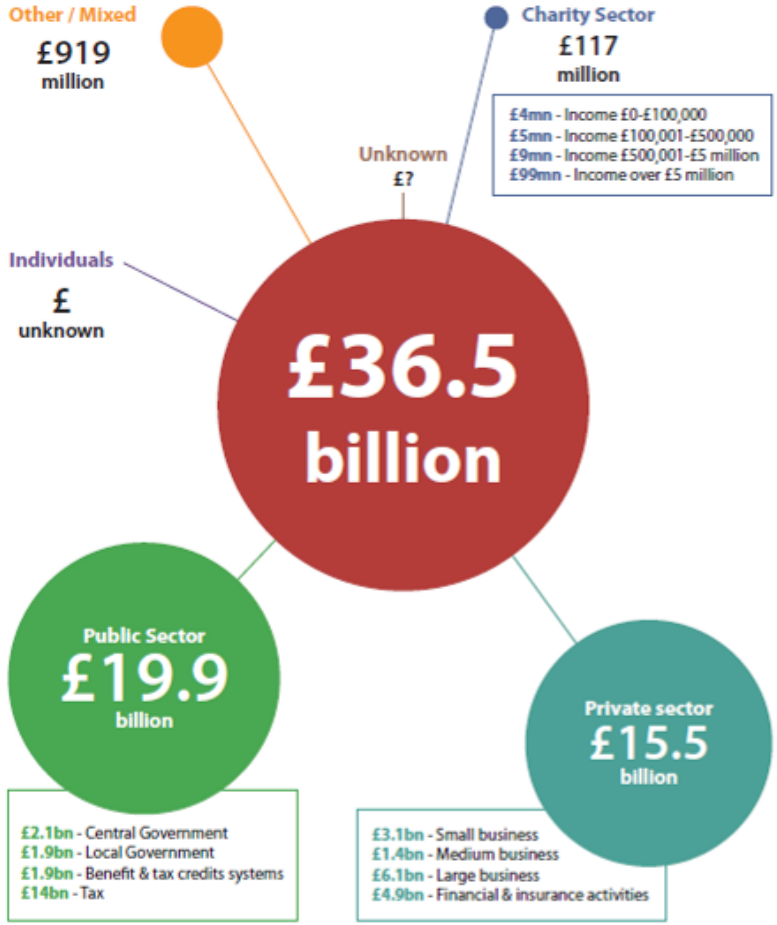


Figure 2: Hidden fraud loss estimates by victim



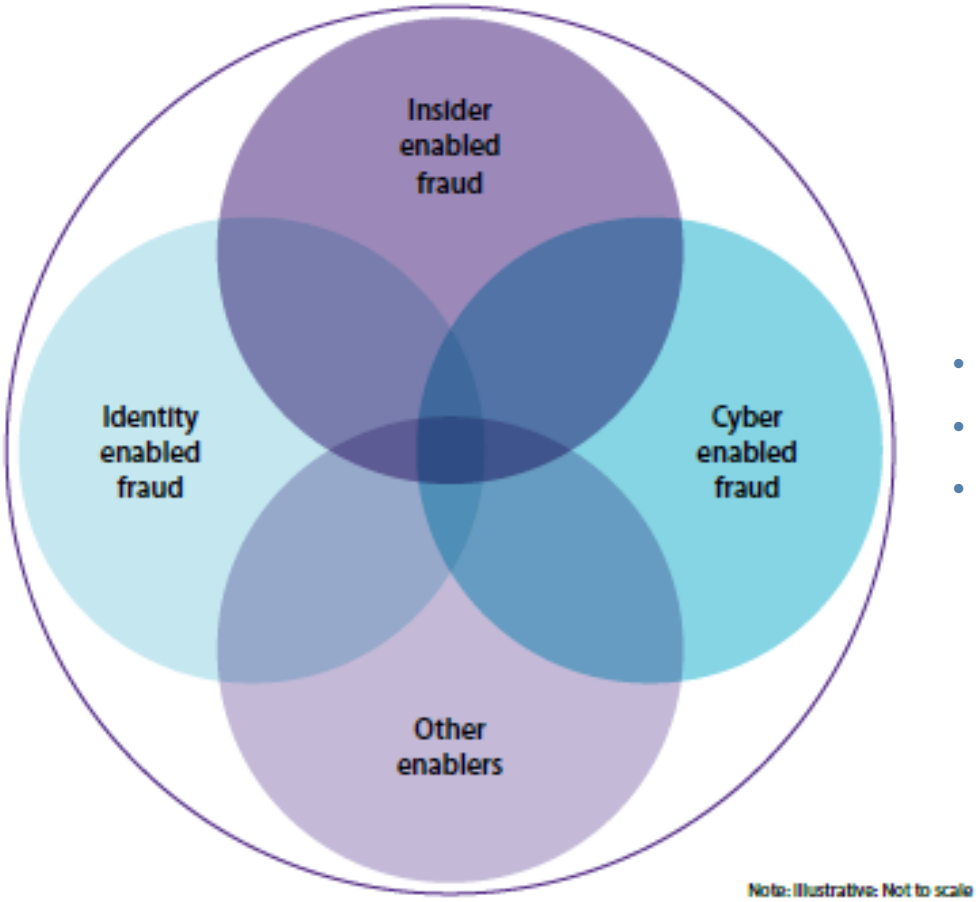
“Hidden” cost of Fraud

Terrorism. Human Trafficking. Organised Crime. The Drugs Trade.

Convergence

- Invoice related fraud
- Use of public information
- Data compromise

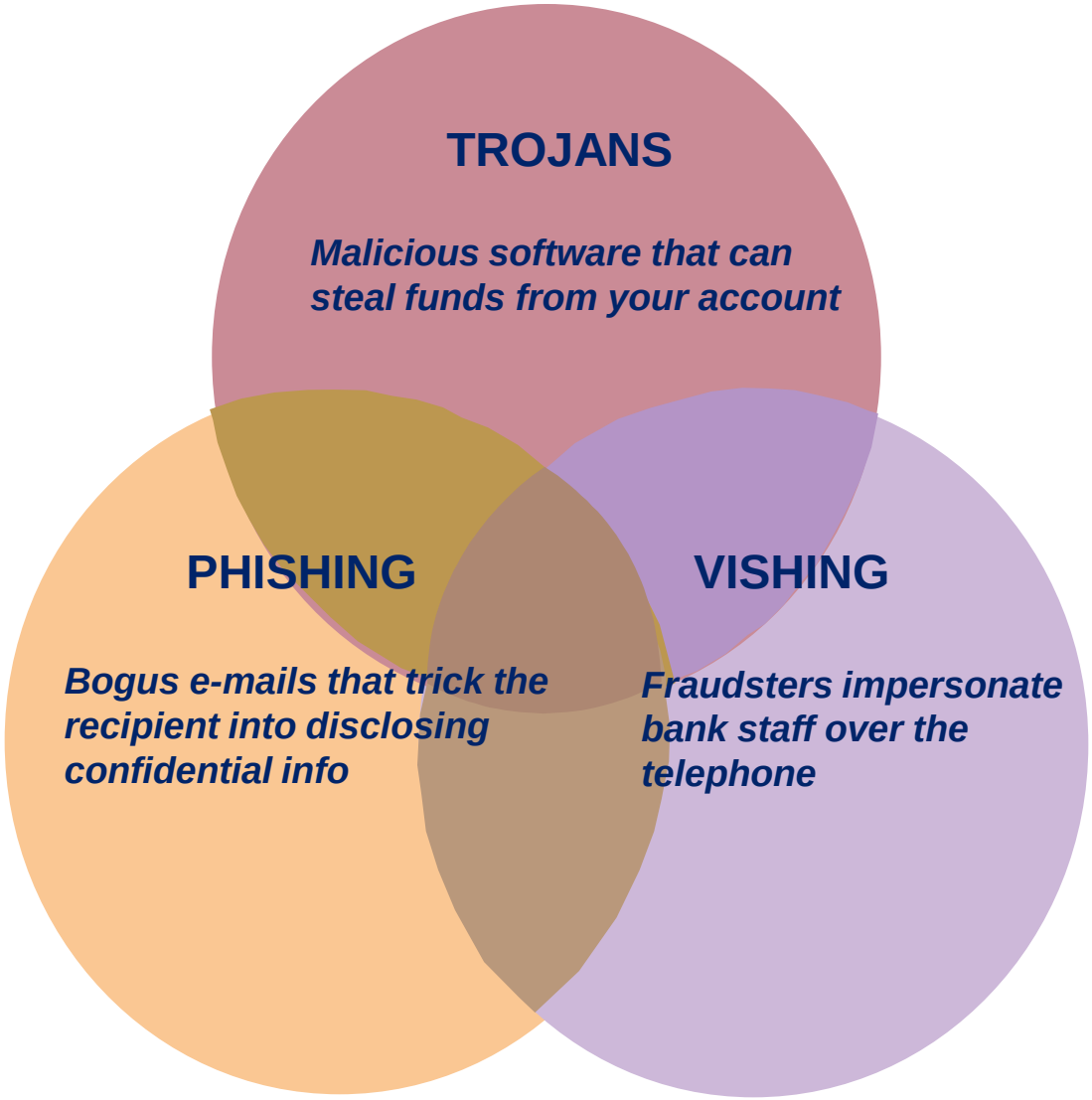
Figure 3: Key fraud enablers



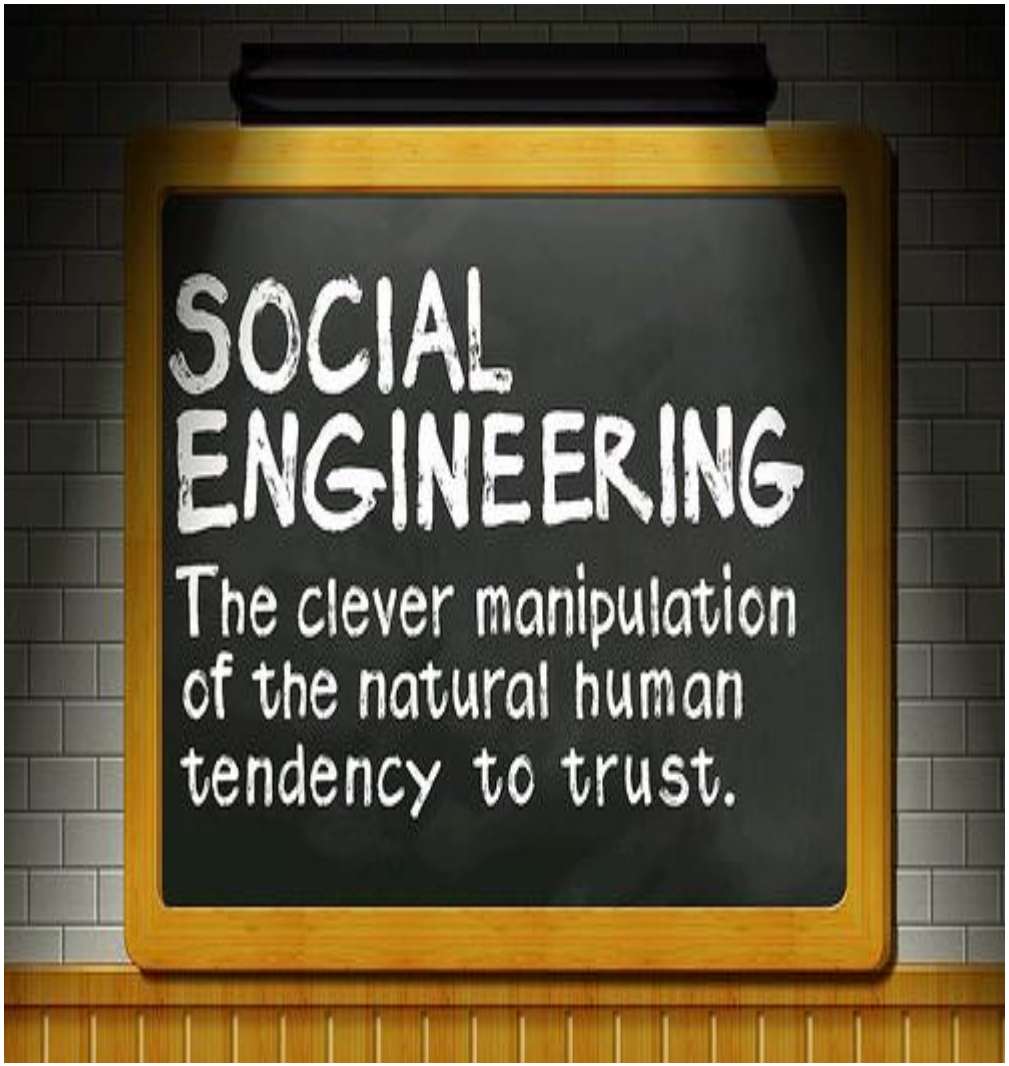
- Malware & Phishing
- Device Convergence
- Cloud Computing

- Social Engineering

Trojans, Phishing & Vishing



Phishing, Vishing & Trojans = Social Engineering



- **The banks' own systems have proven difficult to attack**
- **Fraudsters therefore focus on the individual users of Internet Banking services**
- **Securing your browser is key to staying safe online**
- **Staying vigilant for bogus phone calls is also essential**

Phishing

- **The practice of sending e-mails at random, purporting to come from a bank or other genuine company**

- **Purpose can be either:**

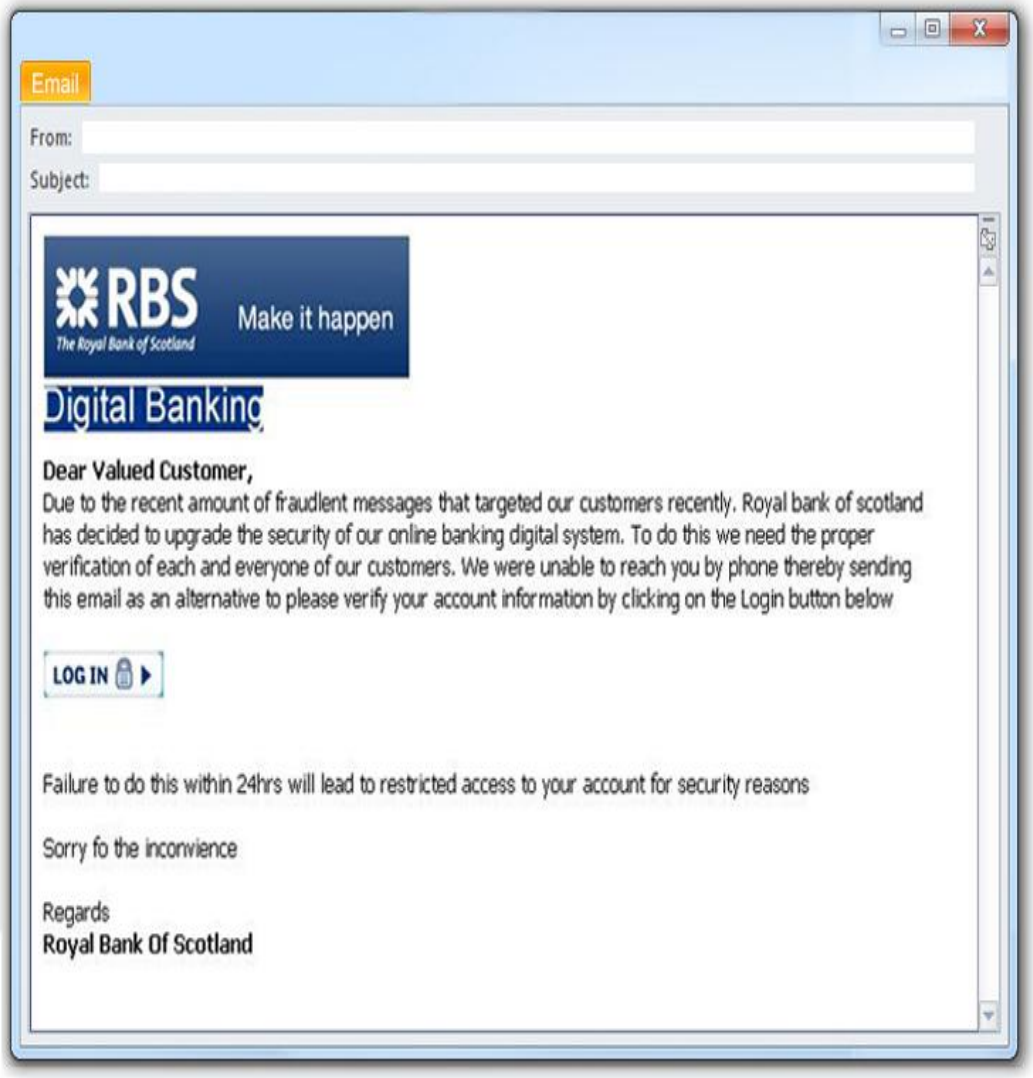
  - to trick users into clicking a link to a bogus web page, where they disclose their confidential details

  - to deliver a Trojan file

- **In 2012, fraudsters created approximately 257k phishing websites targeted against the customers of UK banks***

Source = Financial Fraud Action UK

Phishing e-mails - Common Features



- Credible originating e-mail address
- Illicit use of trusted logos
- Demands immediate action
- May have a topical theme
- Bogus hyperlinks or action buttons
- Unfamiliar telephone numbers
- ZIP file attachments

Vishing = Impersonation

- **Vishing involves the fraudster calling the customer and pretending to be from the bank**
- **The fraudster may already know who you bank with – perhaps as a result of responding to an earlier phishing e-mail**
- **The fraudster may already have harvested user details such as log-in PINs & passwords**
- **What they don't have in their possession are your smartcards or other relevant security devices – they therefore call to trick you into using them**

Security warning:

We will **never** ask for PINS, passwords or smartcard security codes over the telephone in any circumstances.

If in doubt, call the Bankline Helpdesk.

Only individuals who have authorised access to NatWest Bankline should proceed beyond this point. For the security of customers, any unauthorised attempt to access customer bank information will be monitored and may be subject to legal action.

Vishing & The Public Domain

- **Although often linked with phishing e-mails, vishing can occur on a 'stand alone' basis**

- **Criminals can make exploratory phone calls, posing as a new supplier or new customer:**

  - they may, for example, try to find out who has responsibility for banking, payments or some other key role,

  - they can cross-reference this with information that is in the public domain to build up a detailed profile of your organisation,

  - this helps them to sound convincing when they subsequently try to impersonate the bank over the telephone

Vishing – It Takes 2 to Disconnect

- **If you receive a suspicious call from someone purporting to be from your bank:**
  - hang-up immediately,
  - call your bank using a telephone number that you know to be genuine,
  - DO NOT use any contact details given to you by the suspicious caller

- **When you call the bank, use a different phone to that which received the suspicious call:**
  - fraudsters will not necessarily terminate their half of the call after you put your own phone down,
  - a line can be kept open for several minutes in this way,
  - if you use the same phone, there is a risk that you will reconnect to the fraudster

Vishing / Phishing Case Study

- **Customer responded to a phishing e-mail**
- **They gave away their full Customer ID, User ID, PIN & password**
- **The customer was then contacted by the fraudster, who posed as a member of bank staff**
- **He told the customer that all of their accounts were locked and…**
- **They could only be reinstated by disclosing smartcard security codes**
- **Multiple codes were disclosed, allowing numerous domestic and international payments to be executed**

Trojan Overview

- **A form of malicious software that is installed without the user's knowledge**
- **It opens a backdoor into your PC or network**
- **Its presence is often only felt when you connect to a banking website**
- **Customers of every UK bank have been targeted (1 Trojan can target multiple banks)**
- **Anti-virus software has a poor track record at detecting Trojans**
- **Circa 1 in 750 PCs in the UK is infected with a Trojan at any given time***

Source = Trusteer, 2012

Trojan Capabilities

- **What they can do**
  - divert you to a fake ‘look-a-like’ site controlled by the fraudster
  - insert bogus web pages
  - tamper with genuine web pages
  - log key-strokes & harvest confidential info
  - video web sessions
  - trick the genuine user into authorising fraudulent payments

Trojans – Infection Routes

- **How you become infected:**
  - opening attachments to phishing e-mails
  - visiting compromised web sites (via pop-up boxes & advertising banners)
  - leaving software un-patched
  - Trojans can also masquerade as genuine software

Trojan Infections are primarily spread by phishing & spam e-mails

The e-mails misappropriate well known brands & logos, and have credible originating addresses

Social Media	“A Facebook friend has sent you a picture”
Mobile Networks	“A multi-media message is available to view”
Travel & Hotels	“Confirmation of your hotel booking is attached”
Logistics	“We could not deliver a parcel to you”
Government	“Receipt of Online VAT Submission”

Trojans – beware phishing e-mail attachments

- **The Trojan is wrapped in a ZIP file**

- **The ZIP file will contain a file ending .EXE**
  - the file name could be designed to make the attachment seem harmless, e.g. invoice.pdf.exe

- **The Trojan is installed when the .exe file is clicked**

Trojan Case Study

- **Customer was infected by inadequate information security controls:**
  - **Staff allowed to access personal e-mails from their work desktops,**
  - **Browsing / web filtering controls were also relaxed**
- **PCs used to access Bankline were infected with Trojan malware**
- **Significant funds were fraudulently transmitted overseas**
- **Luckily, the funds were retrieved as it was a bank holiday in the receiving country**
- **The customer subsequently updated their information security and software maintenance policies**

Trusteer Rapport defends against Trojans

- **Hardened browser solution**
- **Adds extra layer of encryption when you connect to the bank**
- **Ensures you are connected to the genuine bank site**
- **Stops Trojans from installing themselves**
- **Disables any Trojans that are already present in your browser**
- **Automatically updates in the background to defend against new strains**
- **Available free to all RBSG customers**
- **Complements, but does not replace, anti-virus and firewall controls**

Trusteer Rapport – Protecting Vulnerable & Infected devices

Keystroke Lockdown

Keystrokes are encrypted from the keyboard to the browser.

Communication Lockdown

Bankline, the destination website, is authenticated and the SSL connection is enforced.

Browser Lockdown

All browser interfaces are blocked during a secure session. External code inside the browser is quarantined.

Keep your software up to date to reduce infection risk

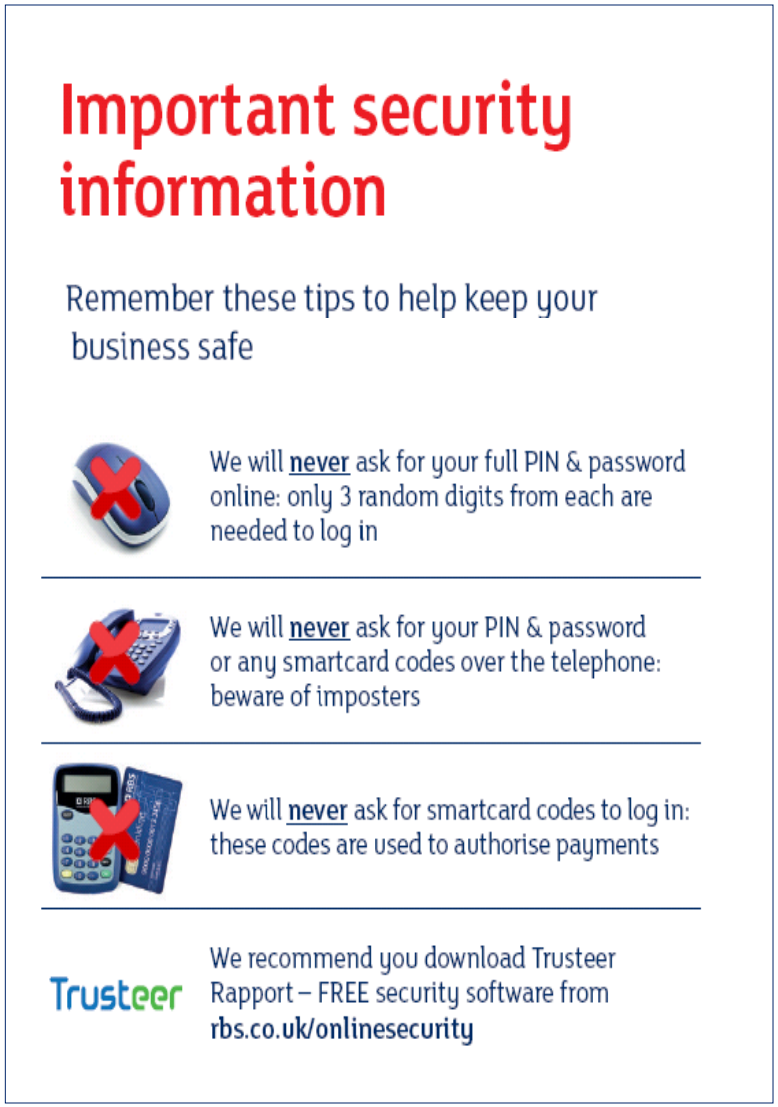
Always set software to update automatically

- **Browsers – Internet Explorer, Firefox, Chrome etc.**
- **Operating Systems – Windows, MAC OS etc.**
- **Media Players, e.g. Adobe Flash**
- **PDF Readers, e.g. Adobe Reader**
- **Productivity Tools, e.g. Microsoft Office Suite**
- **Java Software**

Online Banking Best Practices

- **Regularly change log-in passwords**
- **Don’t allow staff to share log-in credentials / keep credentials safe**
- **Dual authorisation of payments**
- **Apply payment limits**
- **Disable functionality and payment options that you don’t normally use**
- **Regularly review user roles and privileges**

We Use a Variety of Media to Inform Customers About Fraud

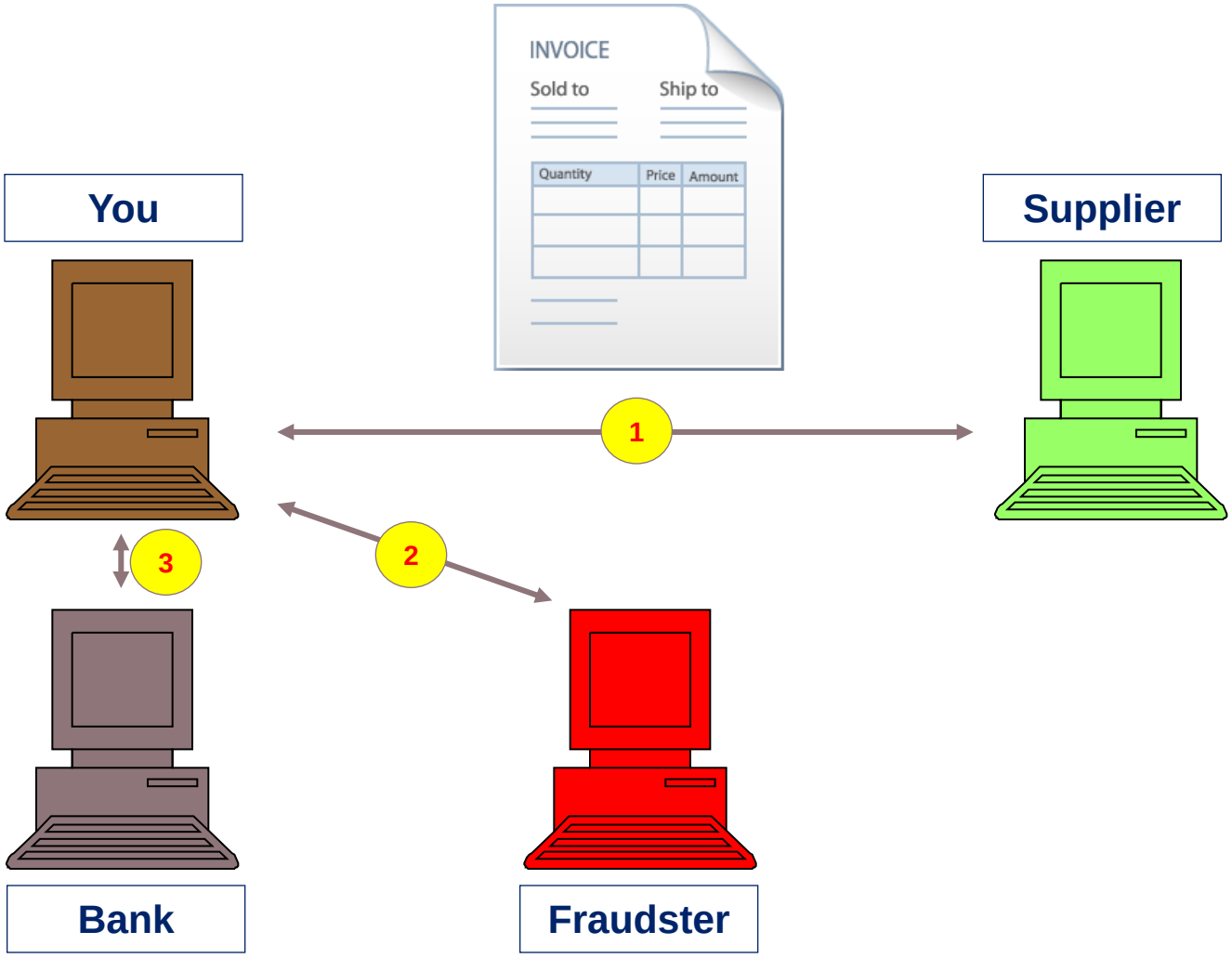


- Letters
- e-mail
- Roadshows
- Videos
- Dedicated web content
- In-application messaging
- Webinars & conference calls
- Statement inserts & physical collateral

Summary of how to stay safe online

- Anti-virus software & firewalls
- Download Trusteer Rapport
- Information security and web browsing policies
- Keep your key software up-to-date
- Beware unsolicited e-mails & attachments
- Beware unsolicited phone calls purporting to be from the bank
- Enable ‘dual authorisation’ and other controls for online banking
- Read all fraud communications from your bank

Invoice Fraud



Invoice Fraud

Mitigants

1. Confirm change of bank account requests with the Supplier.
2. Single Points of Contact (and/or Dual Authentication for Account changes) with Suppliers.
3. Check invoices for irregularities – Verify with the genuine Supplier as this will help both Parties.
4. Generate confirmation emails each time a payment is made to a Supplier.
5. Proactive review of recent and pipeline Change of Account requests made by Suppliers and Contractors.

Insider Fraud

ChronicleLive

HOME | NEWS | SPORT | WHAT'S ON | LIFESTYLE | IN YOUR AREA | BUY, S

Hot Topic: Crime - Northumbria Police - Trinity Square, Gateshead - Sunday Sun

Follov

News » North East News » East Coast

By Rob Kennedy | 4 May 2013 09:39

Train company boss's free rail ticket scam is exposed

Railway boss Trevor Watt has been given a suspended prison sentence after admitting fraud where he dished out free rail tickets

Tweet

BBC News Sport Weather iPlayer TV Rad

NEWS MANCHESTER

Home World UK England N. Ireland Scotland Wales Business Politics Health Education Sci/Envir

24 August 2012 Last updated at 15:38

Share

Bingo addict Graham Taylor stole £1.5m from Nema Ltd

A financial director who stole about £1.5m from his employers to feed his internet bingo addiction has been jailed for five years.

Graham Taylor, 66, of Hanover Street, Castleton, Greater Manchester, siphoned off the money from engineering firm Nema Ltd over a four-year period.

Three colleagues lost their jobs due to his actions.

He pleaded guilty to four theft offences and two of fraud by abuse of position at Bolton Crown Court.

Former colleagues were given the day off on full pay to go to court to see him sentenced on Thursday, Greater Manchester Police said.

Graham Taylor admitted theft and fraud

'Desperate gambler'

Taylor had worked for the firm, based in Chichester Street, Rochdale, for 12 years when the company, which had previously been turning over £3m a year, began to make a loss.

Bosses put it down to the general economic downturn and s

The Northern Ec

News Sport Business What's On Lifestyle Features Info Announcements

National Local News Crime Education NHS & Health Council Public Notices Galleries

The Northern Echo » News »

NEWS SEND YOUR NEWS, PICTURES & VIDEOS

North Yorkshire supermarket worker jailed for stealing hundreds of thousands of pounds of Asda gift vouchers

8:53pm Friday 7th June 2013 in News

A NORTH Yorkshire supermarket worker who was today (June 7) jailed for stealing hundreds of thousands of pounds of Asda gift vouchers amassed a fortune which she spent on luxury holidays, artwork and lavish ornaments, police said.

Jennifer Margaret Ward, 49, of Wigginton Road, York and her partner Alistair Gordon Lobban, 52, of the same address, were sent to prison for a total of three years following what North Yorkshire Police described as a "bizarre and

BBC Sign in News Sport Weather iPlayer TV Radio

NEWS LIVE BBC NEWS CHANNEL

News Front Page
World
UK
England
Northern Ireland
Scotland
Wales
Business
Politics
Health
Education
Science & Environment
Technology
Entertainment
Also in the news

Video and Audio

Have Your Say
Magazine
In Pictures
Country Profiles

Page last updated at 19:41 GMT, Friday, 20 November 2009

E-mail this to a friend Printable version

Ex-policeman jailed in fraud case

A former policeman and an insurance company manager who funded a lavish lifestyle with money obtained from a £1.4m fraud, have been jailed.

The court heard the men spent the money on holidays and hotels

John Taylor, 35, and Stephen Spellacy, 36, who served with Humberside Police, admitted the theft and laundering of the money from Norwich Union in York.

Taylor, of York, was jailed for five years. Spellacy, from Pocklington, was jailed for eight-and-a half-years.

They were among seven men jailed at Leeds Crown Court.

Police said the thefts from Norwich Union - now Aviva Plc - took place over several years.

BBC News Sport Weather iPlayer TV Rad

NEWS LANCASHIRE

Home World UK England N. Ireland Scotland Wales Business Politics Health Education Sci/Envir

20 June 2012 Last updated at 15:38

Share

Bride jailed for stealing £200,000 towards wedding

A bride who stole £200,000 from her employers to pay for a lavish wedding has been jailed.

Part-time accounts assistant Kirsty Lane, 30, transferred the funds from Pure AV's bank account into that of her and her future husband, Graham.

The fraud was discovered shortly after the pair's wedding at the Great Hall at Mains, near Blackpool in January 2011.

Police said Lane "abused her position of trust to steal from her employer and fund a lavish lifestyle"

Lane, of Lewis Close, Adlington, Lancashire was sentenced to 20 months in prison at Preston Crown Court.

She stole about £122,000 from the Leyland company, which installs audio -visual equipment, by putting in fake invoices, marking them as paid and then depositing the money into her own account.

Insider Fraud

Opportunity + Rationalisation = Loss

Warning Signs

1. **Behavioural & Lifestyle Changes / Holiday Pattern / Supplier relationships**

Mitigants

1. **Check, Check + Check !**
    1. Validate right to work
    2. Social Networking sites
    3. Verify Qualifications
2. **Zero tolerance policy / Culture & Awareness**
3. **Control Framework**

Cheque Fraud

Source: UK Payments

- *" … in the past year the Banking Industry successfully identified over 90% of all fraudulent cheques as they went through the cheque clearing process".*

Cheque Fraud

Simple steps to prevent

1. Storage – ‘Lock and key’
2. Condition – Middle of book
3. Preparing – Avoid gaps
4. Sending – Recorded
5. Reconcile – Frequency
6. Dual Review – Prevent Insider
7. Follow up / Stop – Missing

Recap

30%

Victim of fraud over last 12 months …
… and rising.

£4k

Average annual cost to small businesses of fraud and online crime

73%

Have **not** been a victim of Online fraud …
… or Have they?

20%

Have staff training to minimise + prevent fraud … What about other 80%?

Source: FSB Cyber Security & Fraud – Impact on small businesses

Next steps

✗ ✓

Visit Security Centre on www.rbs.co.uk / www.natwest.com