

Keeping out of harm's way in cyberspace

Martin Smith MBE FSyl

Chairman and Founder

The Security Company (International) Limited
The Security Awareness Special Interest Group



The Security Company
International



What is Cybercrime...?

- Criminal activity done using computers and the Internet. Three main categories:
 - those that use the computer as a weapon;
 - those that use the computer as an accessory to a crime;
 - those that make the computer a target of a crime.
- Most crimes are traditional in nature and use a computer or the Internet to break the law.
- Cybercrime is an international challenge, depriving online users of billions of dollars a year. It demands an international response.



What is Cybercrime...?

- Spam
- Fraud
- Cyber-bullying/cyber stalking
- Cyber-terrorism
- Piracy
- Identity theft
- Electronic funds transfer fraud
- Illegal interception of telecommunications
- 'Stranded Traveller' and other scams
- Phishing
- Pharming
- Credit card fraud
- Pornography/Dissemination of offensive materials
- Electronic money laundering and tax evasion
- Online payment and banking fraud
- Electronic vandalism
- ...and many more



We need to work the problem

- Our secure systems are built to perfection but are being subjected to massive external attack.
- Cybercrime is rapidly increasing, Advanced Persistent Threat is on everyone's lips and IP is at grave risk.
- Privacy is considered as “something of the past”.
- National infrastructures are under direct threat of attack from other nation states.

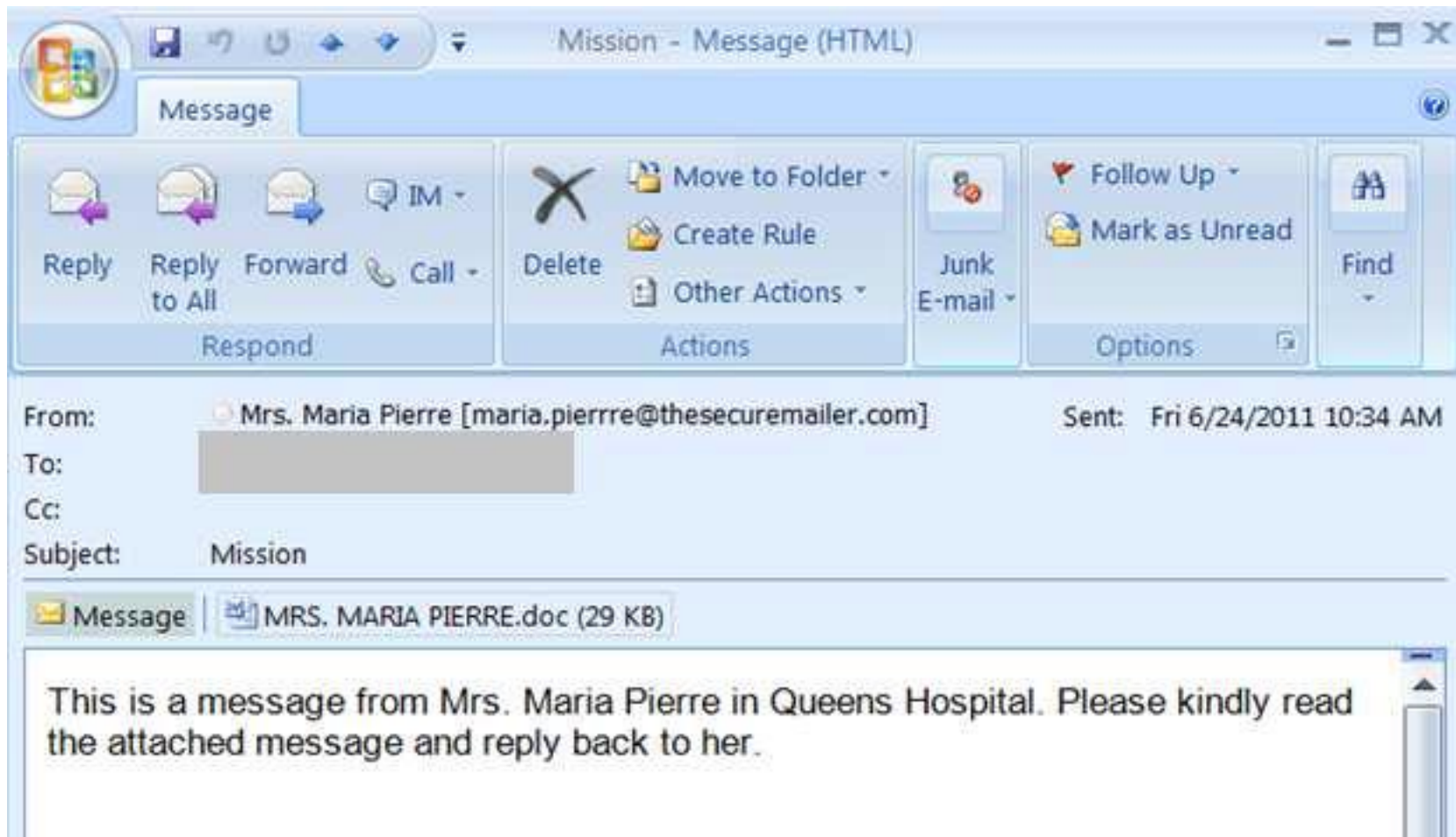


Examine the evidence

- The vast majority of breaches and security events occur at the most basic levels of our defences.
- Most attacks succeed by subverting physical security, by exploiting sloppy housekeeping and errors in systems operations and patching, and by directly targeting people.
- Social media makes social engineering easy.
- BYOD is emasculating our technical defences.
- Human error and ignorance amongst our workforces present a gap in our fortification.



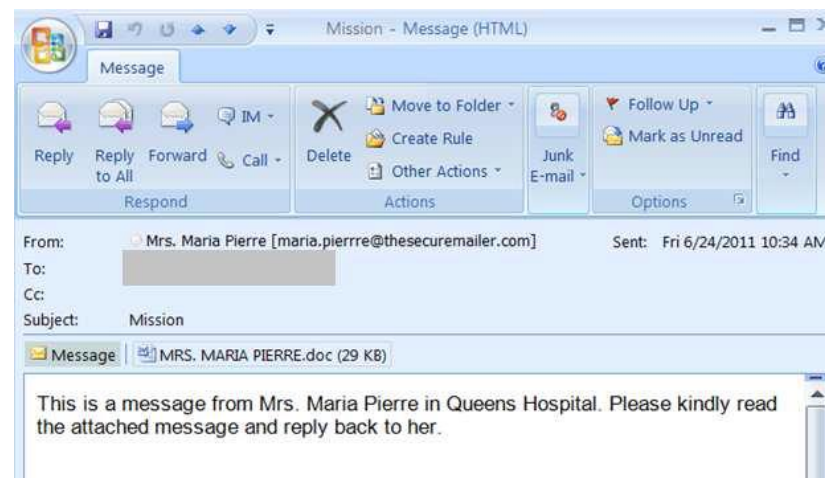
It starts with an email...



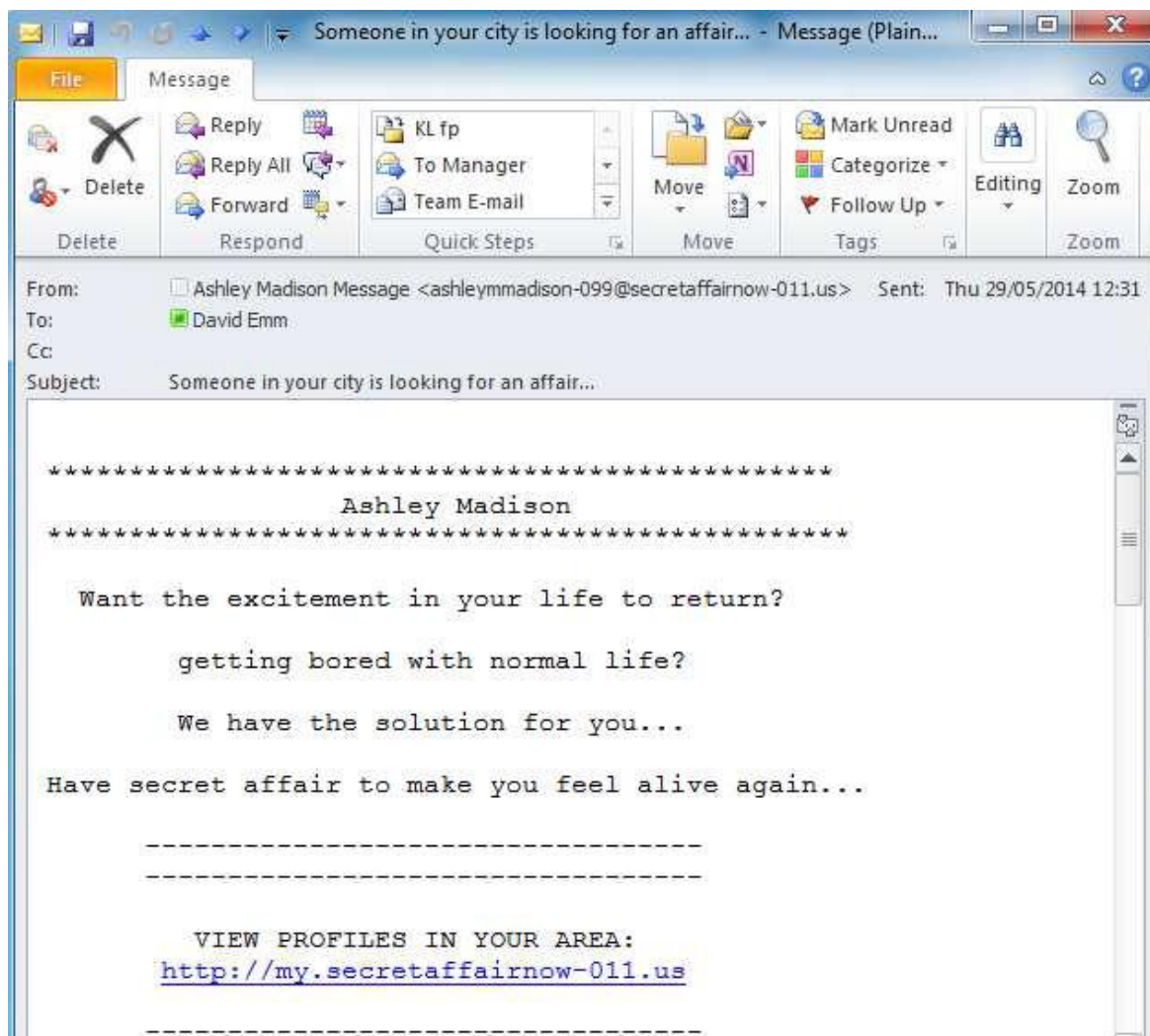
What would you do...?

- Open the attachment – it might be interesting
- Save the attachment to disk and open it
- Save it to disk, scan it and only open it if it's clean
- Just delete it

Your choice...?



Another example...

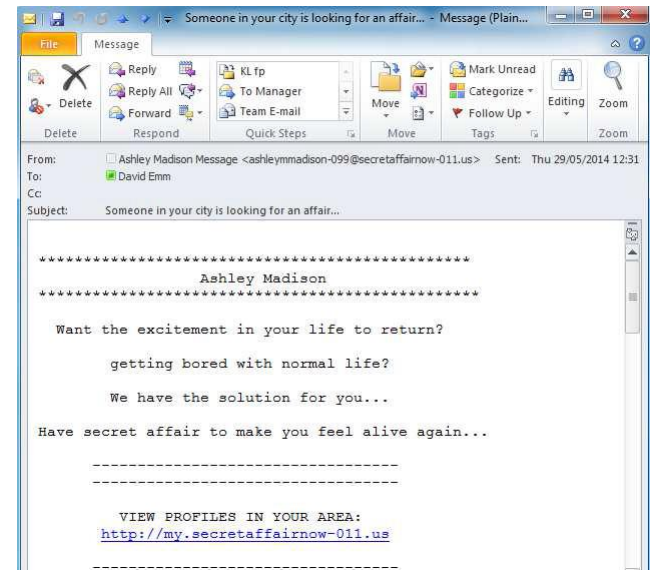


@MartinSmith_TSC

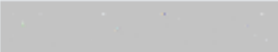
What would you do...?




- Click on the link – I might get a date
- Send a reply asking for more information
- Just delete it

Your choice...?



But what about this...

From: ☐ noreply@taxreg.hmrc.gov.uk Sent: Fri 16/05/2014 11:04
To: 
Cc:
Subject: HMRC taxes application with reference Y4K9 JVJ4 GYCT 0T2T received

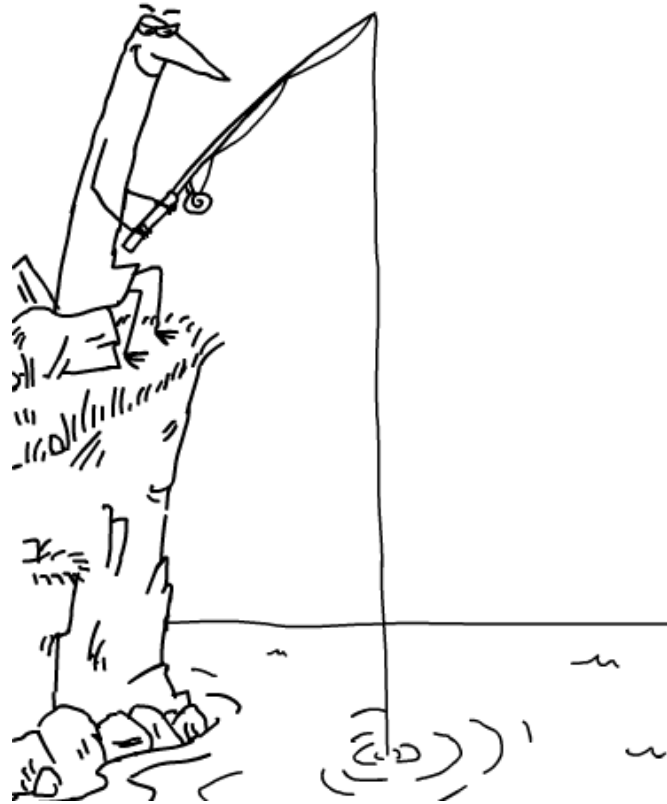
 Message  HM Revenue & Customs - TAX.zip (8 KB)  ATT00001.txt (224 B)

The application with reference number Y4K9 JVJ4 GYCT 0T2T submitted by you or your agent to register for HM Revenue & Customs (HMRC) taxes has been received and will now be verified. HMRC will contact you if further information is needed.

The original of this email was scanned for viruses by the Government Secure Intranet virus scanning service supplied by Vodafone in partnership with Symantec. (CCTM Certificate Number 2009/09/0052.) On leaving the GSi this email was certified virus free.

Communications via the GSi may be automatically logged, monitored and/or recorded for legal purposes.

The social engineer's profile



@MartinSmith_TSC



Phishing attacks

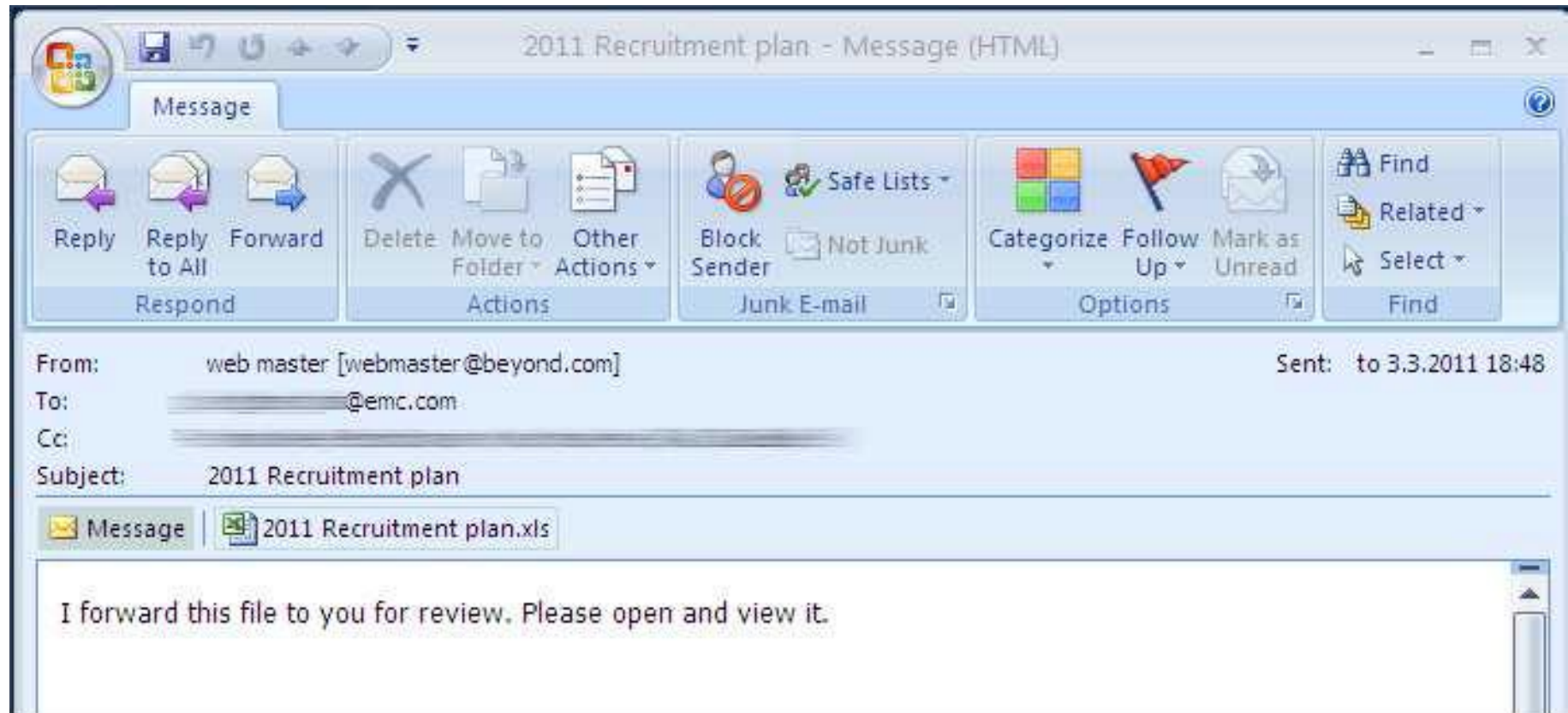


It can happen to the best of us...

- RSA is one of the world's leading computer security companies, inventors of the RSA public key cryptographic algorithm, sold to EMC in 2006 for \$21bn
- On 17 March 2011 RSA announced that it had been hacked



It can happen to the best of us...



Oops, I've clicked on it...

DON'T panic!

DON'T switch off your computer

DON'T delete anything

DO disconnect from the network (wired and wi-fi)

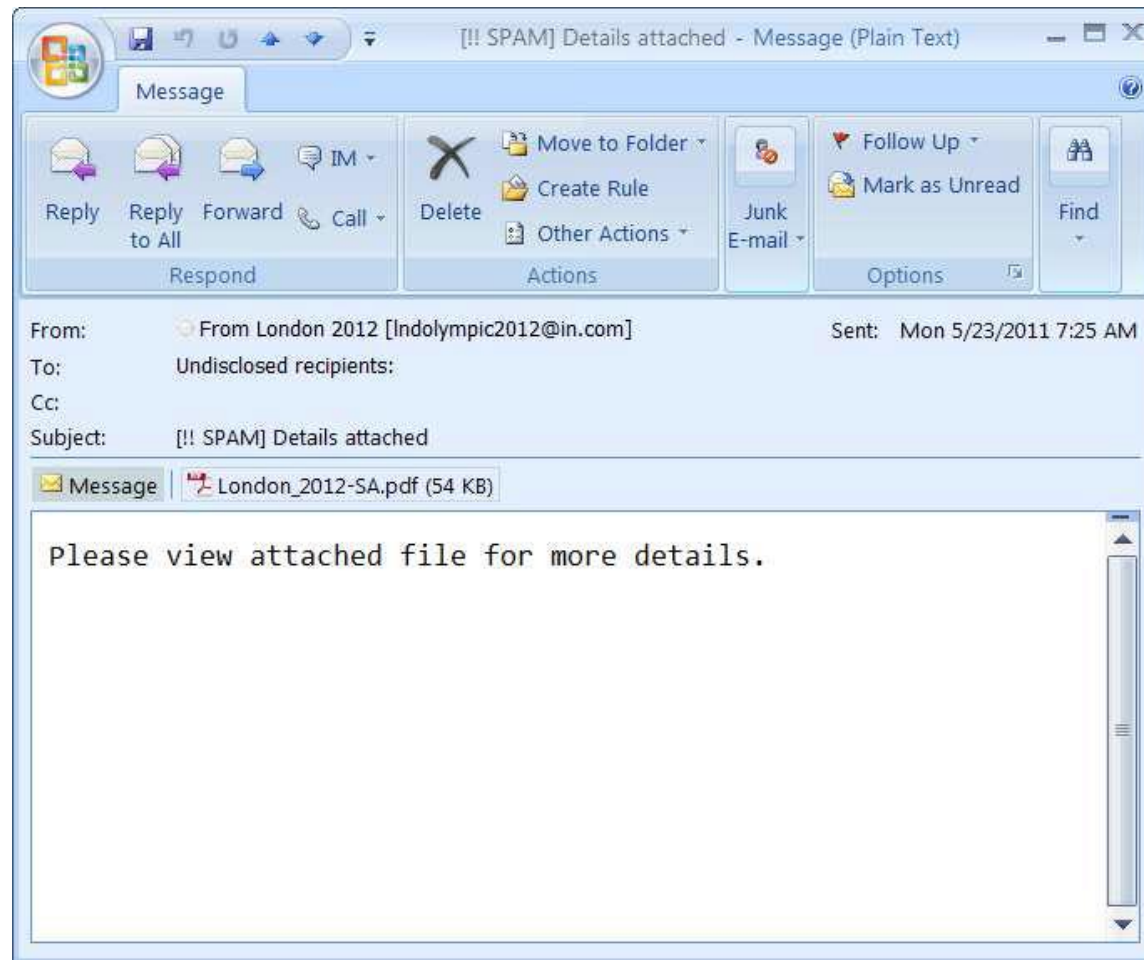
DO contact IT immediately

@MartinSmith_TSC



Staying safe – top tip...

Don't open attachments in unsolicited e-mails!



@MartinSmith_TSC

Staying safe – technical tips...

- Use Windows 7 64-bit
- Patch OS and applications
- Use Chrome for browsing
- Use KB SSL Enforcer to force 'https'
- Use VPN, especially for untrusted wi-fi hotspots
- Use complex passwords



Staying safe – mobiles and tablets...

- Don't 'jailbreak' or 'root' your device
- Use a PIN or (even better) a long passcode
- Install apps from trusted sources
- Only use trusted wi-fi for confidential transactions
- Be wary about storing sensitive data on the device



Staying safe – passwords...



The minimum requirements...

We know from our work over the years:

- **Line management understanding** – line managers must take ownership and display leadership by example of cyber security.
- **Employee behaviour online** - employees must each take ownership of their own digital footprint, and know how to shape, manage and monitor it.
- **Employee Vigilance** - employees must be vigilant to hostile cyber activity and know how to report their suspicions.
- **Social Engineering** – employees must understand the risks to them personally and the organisation, and recognise the techniques.
- **Get the basics right** – there must be good cyber-hygiene within your technical environment, and your employees must display good security practice in their daily routines and working practices.

@MartinSmith_TSC

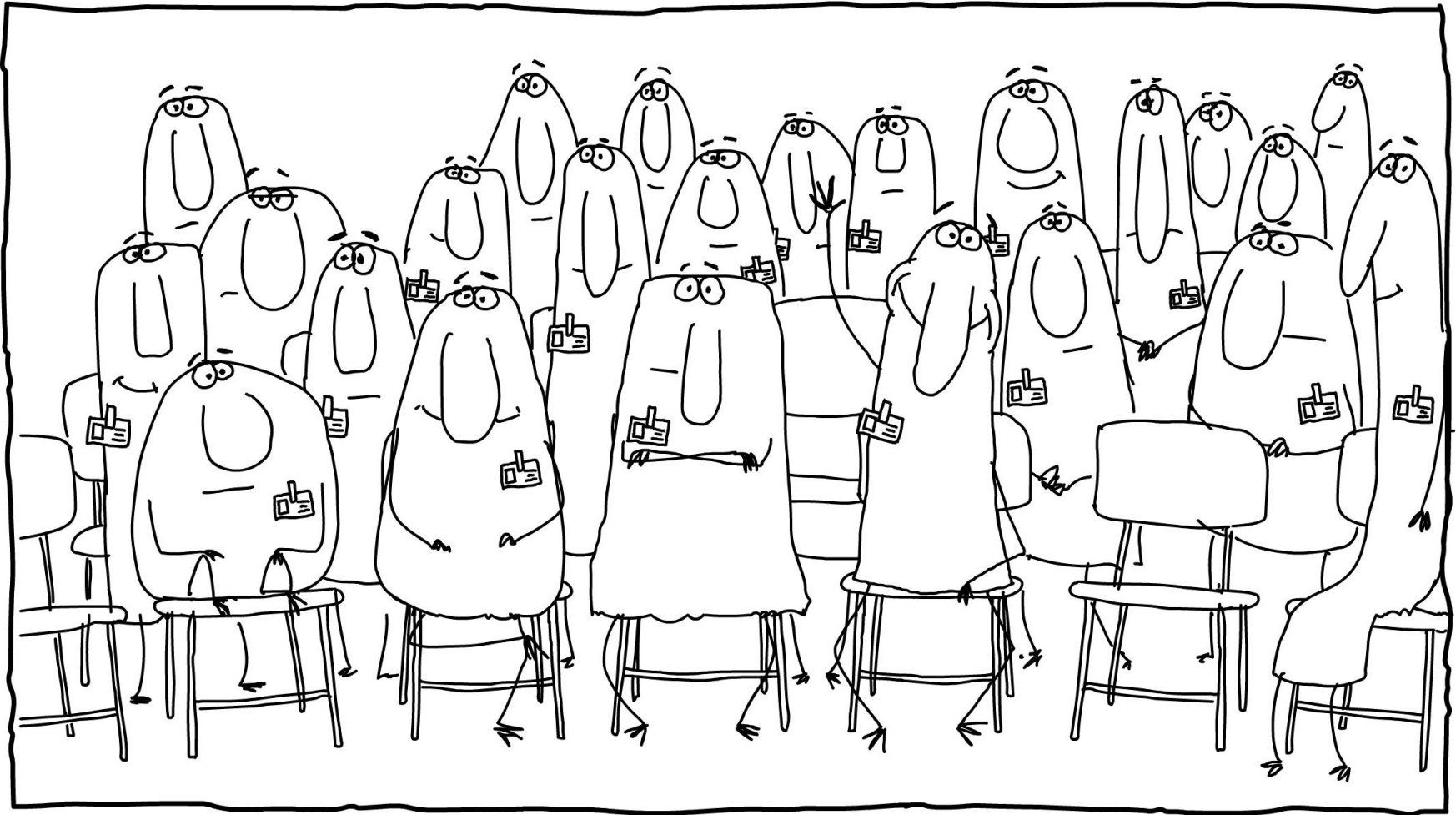


The barriers

- Too much focus on technology
- Senior managers don't see the threat
- Culture
- HR
- Fragmented reporting processes
- Not my problem...



How big is your security department?



@MartinSmith_TSC



Lock it away



Tailgating



Actually, people want to help...

- There is an enormous willingness amongst workforces to follow good cyber security practice.
- The vast majority of any workforce is intelligent, honest, hardworking and sensible.
- To win their support, we just need to tell them what it is we want them to do in language they can understand.
- We must explain the benefits of good cyber security management - “What’s in it for me?”



The elephant in the room

1. The “Mark 1 Human Being” remains the greatest and continuing weakness in the entire fraud prevention regime, but at the same time can be our greatest supporter in the fight against crime.
2. Often it is the breach of ***trust*** that we must fear, not the breach of ***security***.



Trust vs security...



An opportunity for change

- Our lack of focus on the people issues is at the heart of our current data security vulnerabilities. Yet this need not be a bad thing.
- Effort in this area will produce rapid improvements of value far in excess of any extra investment, and that will enhance and support all our other activities from the perimeter fence and beyond right down into the source code.
- It takes only a gallon of oil to make the engine run smoothly.



Questions?

Contact me:

martin@thesecurityco.com

[@MartinSmith_TSC](https://twitter.com/MartinSmith_TSC)

+44 (0) 1234 708456

www.thesecurityco.com

www.thesasig.com



The Security Company
International