NHS

Mersey Internal Audit Agency

Cyber Security: Hacks, Attacks and Abuse

CIPFA NW Audit Risk & Governance Group - Autumn Seminar

Friday 21st October 2016

Tony Cobain

Assistant Director – Informatics & Infrastructure

T: 0151 285 4510 M: 07770 971 006 E: tony.cobain@miaa.nhs.uk

MIAA

Cyber: New threat or rising tide?

1903 - demonstration of Marconi's purportedly secure wireless telegraphy technology, disrupted by Morse code messages through the auditorium's projector

1940 - Alan Turing and team break the enigma code

1980 - the FBI investigates a breach of computer security at NCSS

1986 - first recorded conviction for hacking in the UK but later overturned

1989 - first politically motivated attack recorded

1999 - first coordinated attacks on a state by "Legion of the Underground"

2000 - the "I Love You" worm infects millions of computers world wide

2001 - first significant denial of service attacks (against Microsoft) and release of the Anna Kournikova virus

2002 - Gary McKinnon accused of hacking NASA, his extradition to the USA was eventually blocked in 2012

2003 - Anonymous formed

2007 - first high profile spear phising attack

2009 - Conflicker worm released infecting millions of pc's worldwide

2010 - Stuxnet identified - worm targeting Iranian nuclear facilities allegedly created by US & Israeli military

2011 - Sony's PlayStation network attacked exposing details of 77m accounts

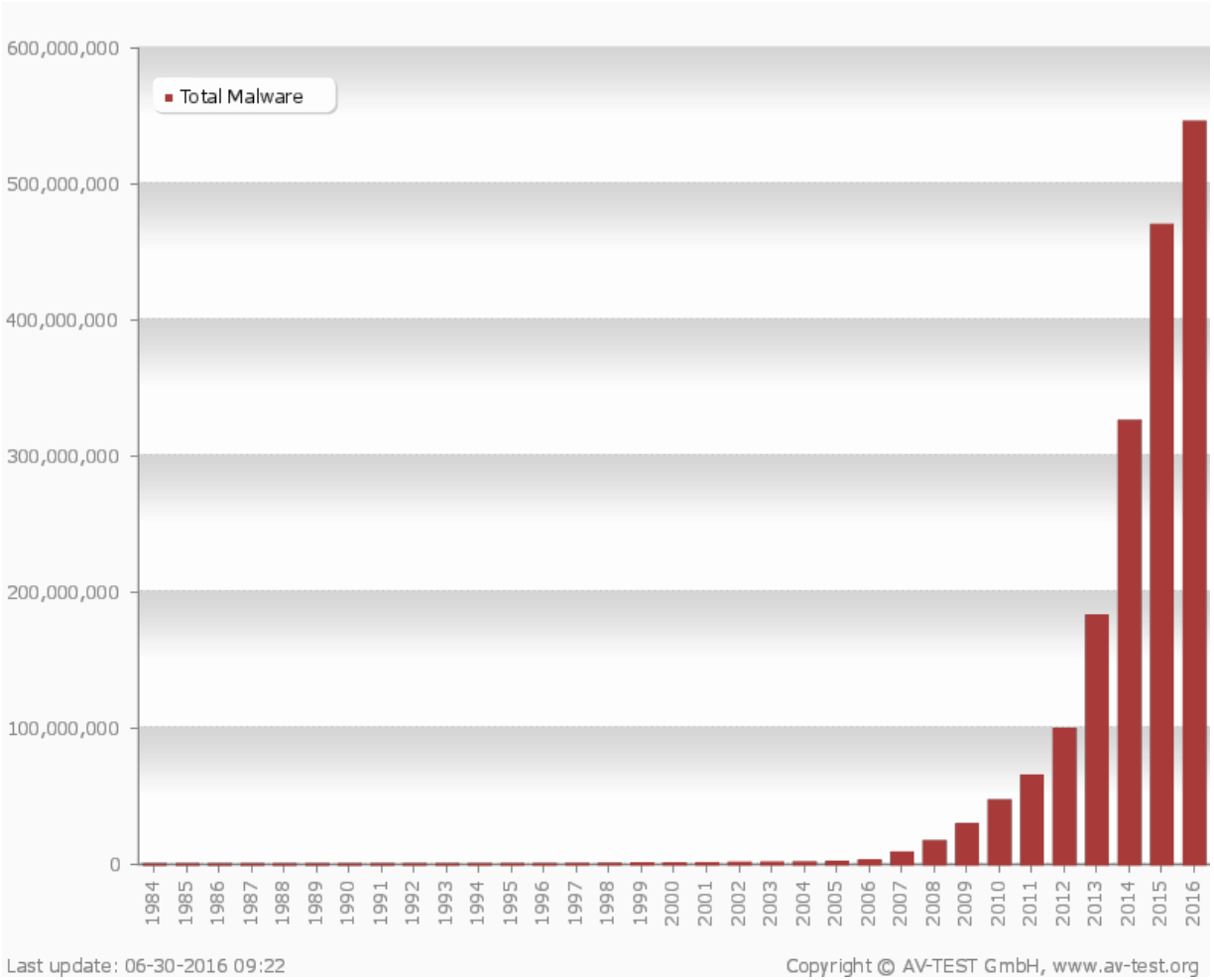
2012 - Julian Assange goes in to exile to prevent extradition to the USA over WikiLeaks

2013 – Yahoo hacked, 500m account details exposed – not acknowledged publicly until 2016

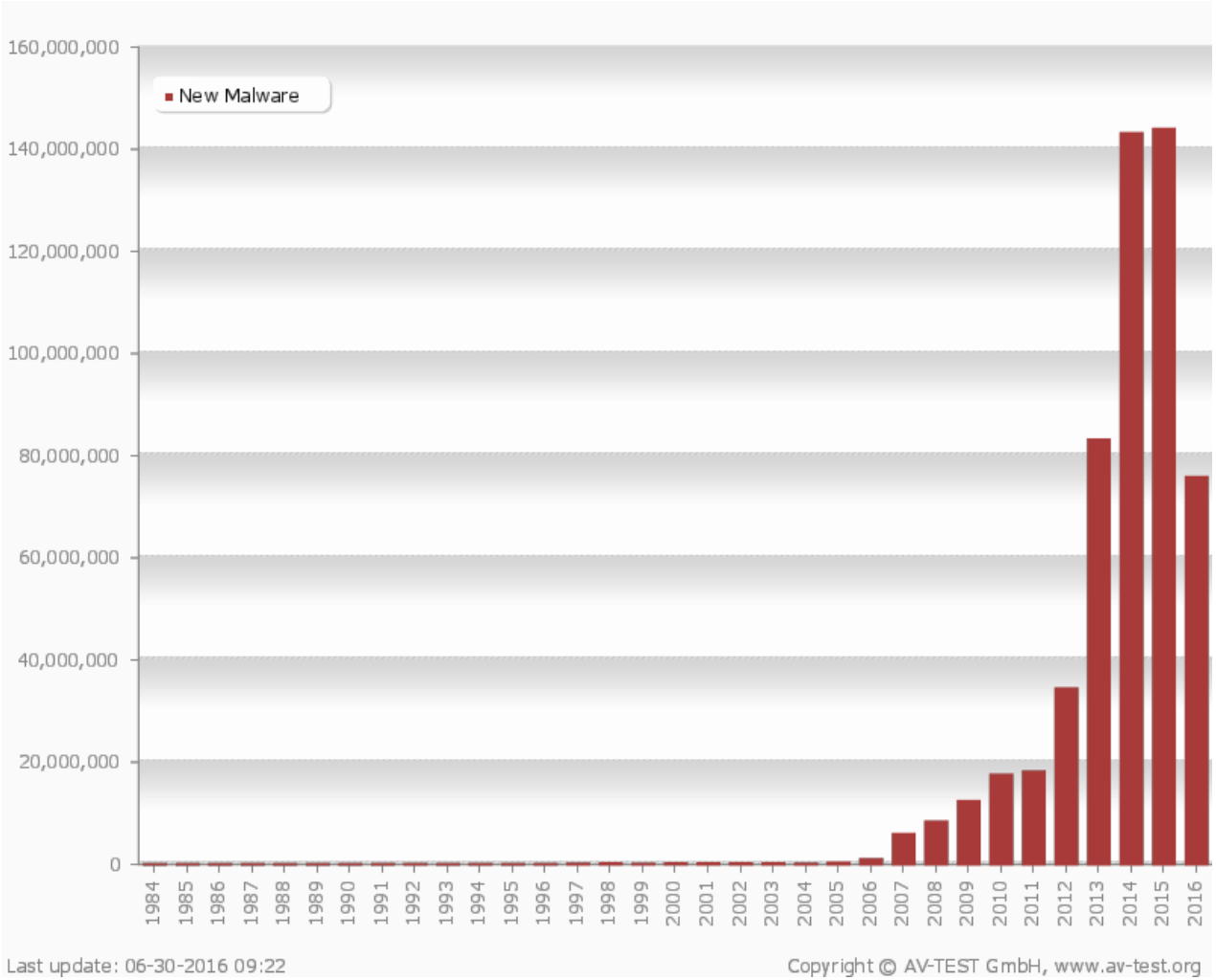
2013 - Edward Snowden goes in to hiding having extracted and released sensitive information from the NSA

2015 - TalkTalk attacked

Cyber: But it is on the increase



Cyber: But it is on the increase



Cyber: The Top 13

1. Yahoo 2012 - 500m
2. MySpace 2016 - 359m
3. LinkedIn - 164m
4. Adobe 2013 - 152m
5. Badoo 2015 - 112m
6. VK 2012 - 93m
7. Sony 2011 - 77m
8. Dropbox 2013 - 68m
9. tumblr 2013 - 65m
10. iMesh 2013 - 49m
11. Fling 2011 - 40m
12. Last.fm 2012 - 37m
13. Ashley Madison 2015 - 32m

Talk Talk 2015 - 157k

Cyber: Live

Cyber: Why?

- To disrupt
- To obtain commercial or state secrets
- Political or moral motivation
- For financial gain (sale or extortion)
- For notoriety
- For fun
- Just because I can

Cyber: Types of attacks

- Brute force – running password crackers on web facing applications
- DDOS – using multiple infected computers to send traffic and overwhelm web facing servers
- Exploiting known vulnerabilities in systems and applications
- Rogue updates to get users to run malicious script
- Phishing to acquire credentials or introduce malware (spearing, whaling, cold calling etc)

Cyber: What's the payload

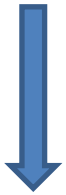
- System unavailability
- Data extraction
- Encryption (eg Ransomware like cryptolocker)
- Botnets
- Remote access (RATs)

Cyber: Phishing

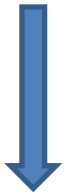
- +200bn emails are sent every day
- 39% of attachments contain some form of malicious code
- 34% of links embedded in emails are malicious
- 77% of malware is installed via email
- 23% of people receiving a phishing email will click on the link or the attachment

Cyber: Man-in-the-middle (1)

Innocent individual goes into Starbucks with PC
(other coffee shops are available)



Turns on PC and sees ”Starbucks Free WiFI”. Makes connection



Browses internet while sipping skinny latte

Cyber: Man-in-the-middle (1)

Innocent individual goes into Starbucks with PC
(other coffee shops are available)

Turns on PC and sees ”Starbucks Free WiFI”. Makes connection

Hacker goes into Starbucks with PC
(other coffee shops still available)

Turns on PC and access point. Sees “Starbucks Free WiFi” and creates a stronger access point to mimic the original.

Happily watches user traffic while allowing pass through to internet

Cyber: Man-in-the-middle (2)

Innocent individual goes into Starbucks
(other coffee shops are available)

Leaves phone in handbag while reading paper and sipping skinny latte

Phone connects because it thinks its at home

Hacker goes into Starbucks with PC
(other coffee shops still available)

Scans coffee shop to identify networks that devices have connected to.

Sets up dummy network

Hacker watches as phone polls gmail etc
Harvests passwords and has "an in"

Cyber: Who?

- State sponsored?
- Hacktivist groups (Anonymous etc)?
- Commercial competitors?
- Criminals?
- Kids?

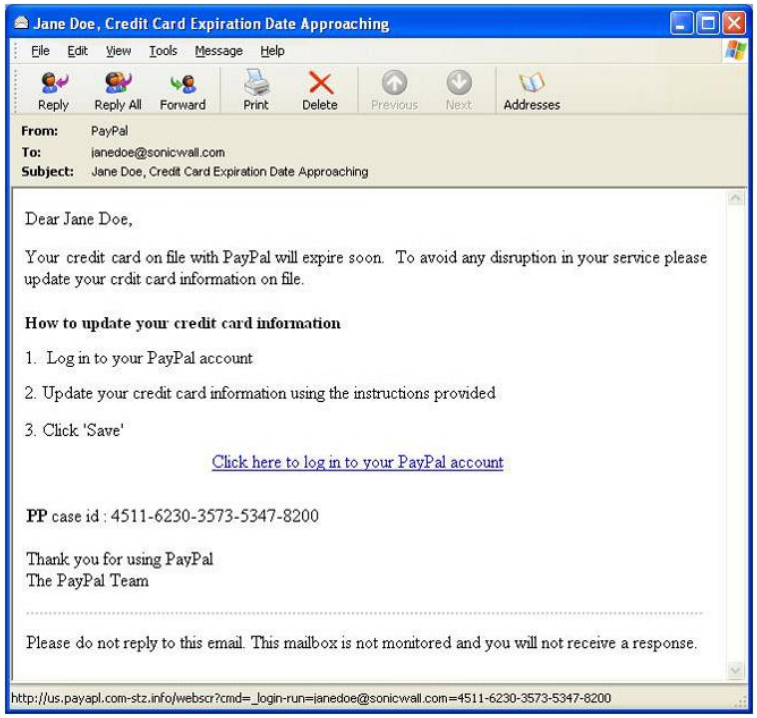
Cyber: Surely not the NHS though?

- Absolutely yes
- NHS websites have been hacked
- NHS pc's and servers have been infected
- NHS systems have been ransomwared

- NHS Digital now operating CareCERT to promoted good practice, monitor traffic and disseminate alerts.

Cyber: An exercise

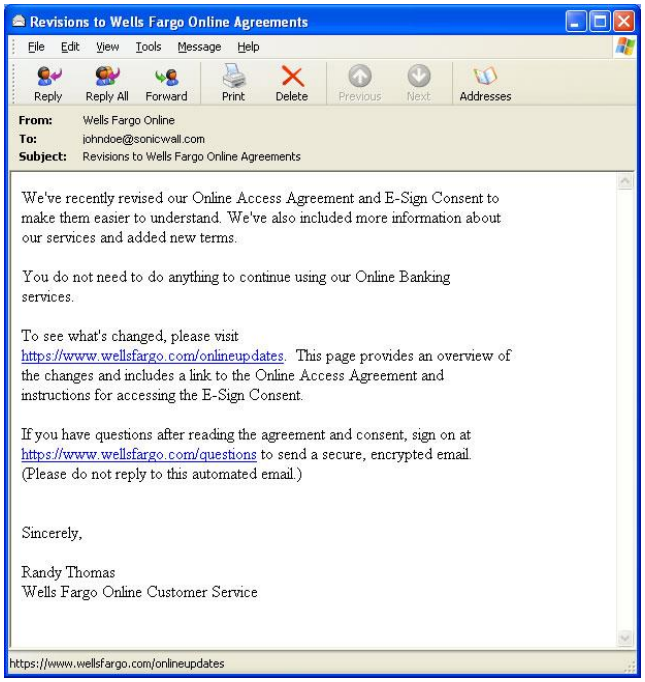
Cyber: Exercise answers (1)



Phish

- Acquiring and using your name is easy so no guarantee of legitimacy
- “Credit” is misspelt
- PayPal don’t include log in links
- The website at the bottom isn’t actually PayPal

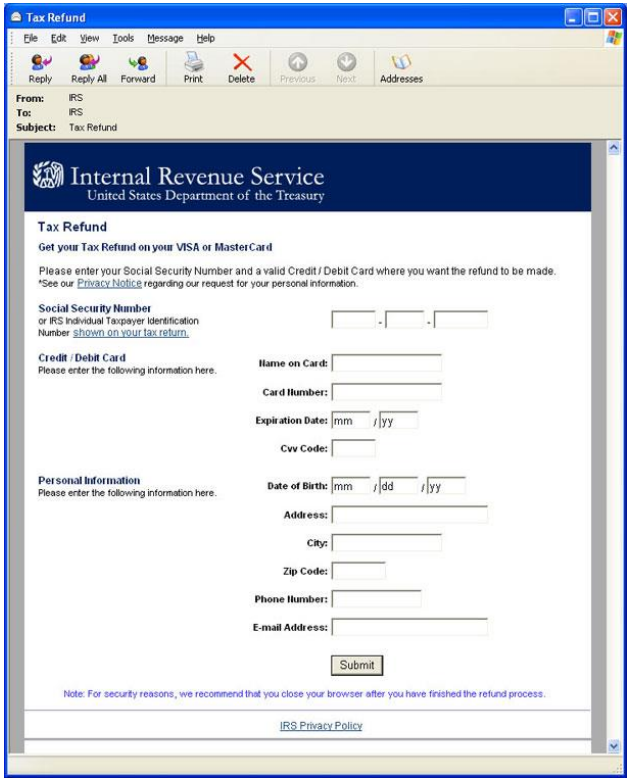
Cyber: Exercise answers (2)



Legitimate

- The email isn't asking you to do anything
- The website is legitimate
- But still beware of link and unsolicited mail

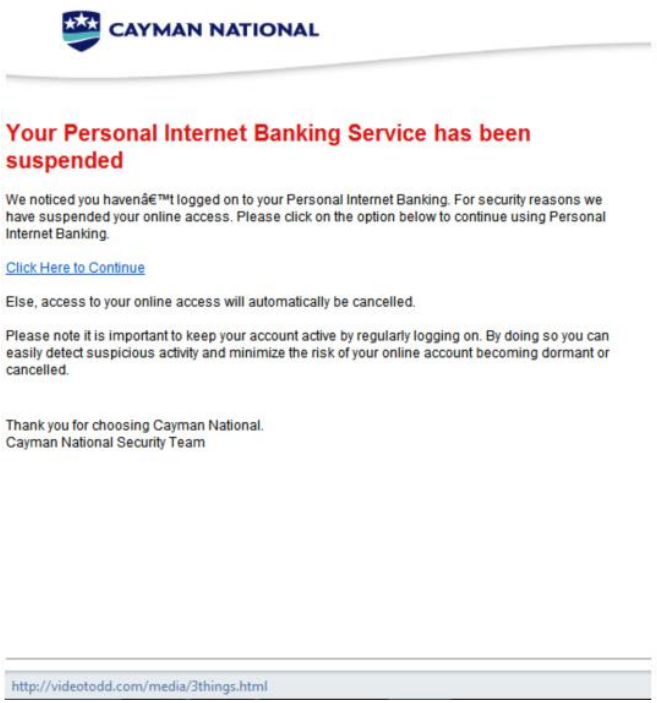
Cyber: Exercise answers (3)



Phish

- IRS/HMRC etc would not request such personal information
- A CVV code is only needed for purchases not refunds
- This is a clear attempt at identity theft and credit card abuse

Cyber: Exercise answers (4)



CAYMAN NATIONAL

Your Personal Internet Banking Service has been suspended

We noticed you havenâ€™t logged on to your Personal Internet Banking. For security reasons we have suspended your online access. Please click on the option below to continue using Personal Internet Banking.

Click Here to Continue

Else, access to your online access will automatically be cancelled.

Please note it is important to keep your account active by regularly logging on. By doing so you can easily detect suspicious activity and minimize the risk of your online account becoming dormant or cancelled.

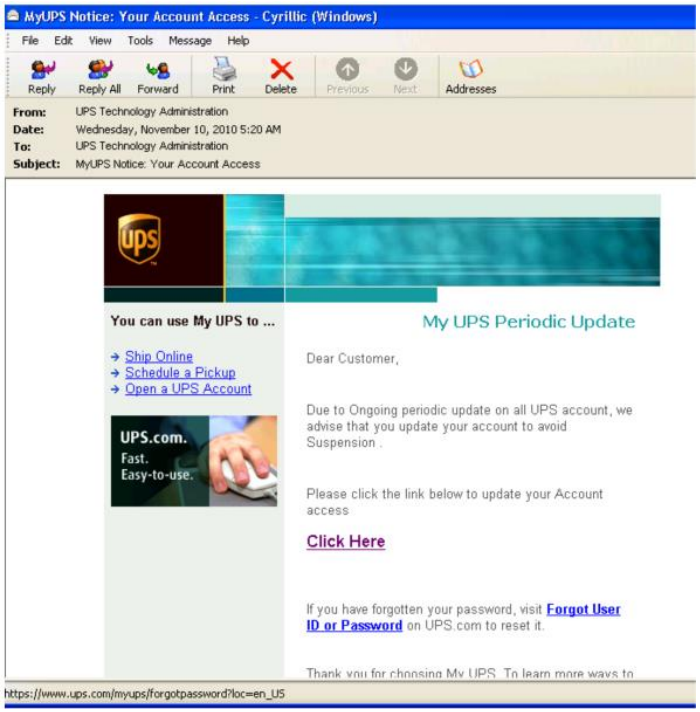
Thank you for choosing Cayman National.
Cayman National Security Team

http://videotodd.com/media/3things.html

Phish

- Notice the spelling of “else”
- The web address that the link points to is not the bank’s

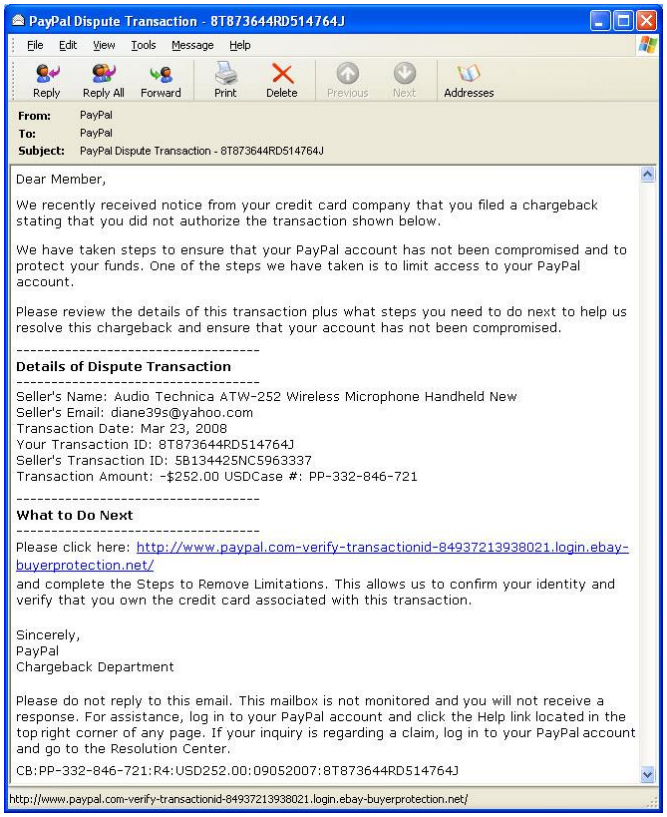
Cyber: Exercise answers (5)



Phish

- Wrong use of case on “suspension”
- The link for forgotten password is not a legitimate ups site – it should be “one-to-one” not “myups”

Cyber: Exercise answers (6)


PayPal Dispute Transaction - 8T873644RD514764J

File Edit View Tools Message Help

Reply Reply All Forward Print Delete Previous Next Addresses

From: PayPal
To: PayPal
Subject: PayPal Dispute Transaction - 8T873644RD514764J

Dear Member,

We recently received notice from your credit card company that you filed a chargeback stating that you did not authorize the transaction shown below.

We have taken steps to ensure that your PayPal account has not been compromised and to protect your funds. One of the steps we have taken is to limit access to your PayPal account.

Please review the details of this transaction plus what steps you need to do next to help us resolve this chargeback and ensure that your account has not been compromised.

Details of Dispute Transaction

Seller's Name: Audio Technica ATW-252 Wireless Microphone Handheld New
Seller's Email: diane39s@yahoo.com
Transaction Date: Mar 23, 2008
Your Transaction ID: 8T873644RD514764J
Seller's Transaction ID: 5B134425NC5963337
Transaction Amount: -$252.00 USDCase #: PP-332-846-721

What to Do Next

Please click here: http://www.paypal.com-verify-transactionid-84937213938021.login.ebay-buyerprotection.net/
and complete the Steps to Remove Limitations. This allows us to confirm your identity and verify that you own the credit card associated with this transaction.

Sincerely,
PayPal
Chargeback Department

Please do not reply to this email. This mailbox is not monitored and you will not receive a response. For assistance, log in to your PayPal account and click the Help link located in the top right corner of any page. If your inquiry is regarding a claim, log in to your PayPal account and go to the Resolution Center.

CB:PP-332-846-721:R4:USD252.00:09052007:8T873644RD514764J

http://www.paypal.com-verify-transactionid-84937213938021.login.ebay-buyerprotection.net/

Phish

- PayPal will always use your member name
- PayPal will always put cut and paste links in their emails
- The link isn't to PayPal but to ebay-buyerprotection.net – an illegitimate site.

Cyber: How do we prevent an attack?

- You can't – it's when not if.

There are three types of individuals /organisations

- Those who have been hacked/attacked and know it
- Those who have been hacked/attacked and don't know it
- Those who will be hacked/attacked

Cyber: Defence in depth

- **Protect against the known knowns and the known unknowns**
  - Take the Senior Information Risk Owner (SIRO) role seriously
  - Make asset ownership (IAOs) an accountable role
  - Have robust and comprehensive polcies and procedures
  - Manage the perimeter with firewalls and IPS/IDS
  - Manage user access, especially admin level
  - Build resilience and recovery

Cyber: Defence in depth

- **Protect against the unknown unknowns**
  - Effectively and robustly risk assess assets
  - Manage patches and don't use unsupported software (XP!!!)
  - Have robust up to date anti-virus
  - Keep abreast of security advisories
  - Educate, educate, educate

Cyber: And be assured

- Third party certified standards (Cyber Essentials, ISO27001 etc)
- Clarity on assurance frameworks and reporting on information assets through SIRO/IAO channels
- Ensuring that internal audit plans cover cyber risk
- Regular penetration testing and vulnerability assessment.
- Social engineering and phishing exercises.

Cyber: MIAA services and support

Protecting the core

- Security architecture design
- Security mgt assessment
- Information risk assessments
- Asset mgt documentation
- ISO27001 compliance

Protecting the perimeter

- Cyber Essentials
- Vulnerability assessment programmes
- Firewall rule ase assessment

Test, probe, assure

- Penetration testing
- Social engineering & phishing
- Web application testing
- Remote and mobile access testing
- Infrastructure reviews

Protecting the perimeter

- Real time monitoring
- Incident response
- Digital forensics

Cyber: Questions or concerns?

Watch out for the phish

I've got your email addresses!!!