



ecsc

more secure

Social Engineering

The Human Aspects of

Information Security

ISACA

Wednesday 22 November 2006

HBOS

Ian Mann

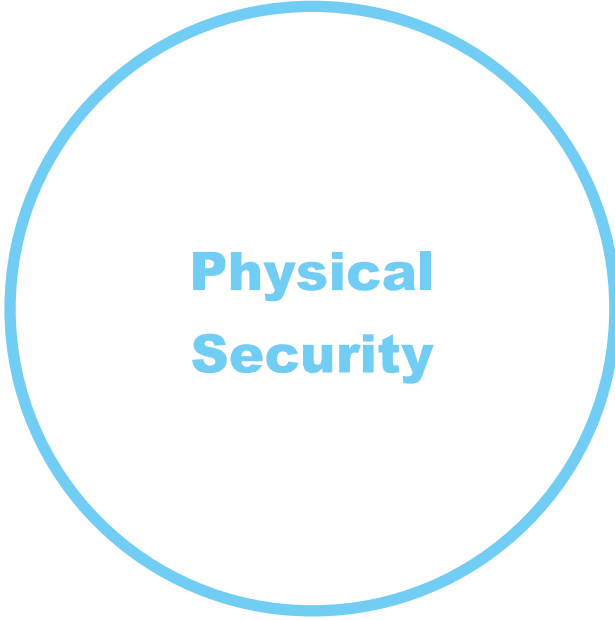
MBA BEng CLAS CISSP
Senior Systems Consultant
ian.mann@ecsc.co.uk

- BS7799-3 Panel
- CESG Listed Advisor with GCHQ
- BS7799 Lead Auditor
- Certified Information Security Systems Professional
- UKOnline for Business - Expert Panel

Information Security



**IT
Security**



**Physical
Security**

Information Security



Definition and History

Social Engineering – manipulating people to trick them into giving out information or performing an action

First used in 1930s Europe to describe the manipulation of an entire population

Picked up by Hackers in the 1980s to describe non-technical hacking



Exploiting Human Vulnerabilities

Following instructions

Ignorance

Gullibility

Desire to be liked

Reciprocation

Being helpful



Useful Roles for the Social Engineer

New technician
Security consultant
Manager
Potential customer
Business partner
Co-worker developing rapport
Authority threatening
Remote worker in an emergency

Example (Milgram was correct!)

- 22 nurses
- Telephone instruction to administer a drug
- Drug not authorised
- Dosage 2x maximum dose
- Only 1 in 22 didn't obtain the drug and proceed to the patient

Hofling et al, 1966

Phishing

HALIFAX Always giving you extra

HALIFAX Always giving you extra

personal & business account

Security Alert

Please note that Your Halifax Online Account is about to expire. In order for it to remain active, please use the link below to proceed and restore access to Your Account.

https://www.halifax-online.co.uk/_mem_bin/formslogin.asp

HALIFAX Always giving you extra

Security Alert

Dear HalifaxBank member,

This email was sent by the HalifaxBank server to verify your e-mail address. You must complete this process by clicking on the link below and entering your account information. This is done for your protection, because some of our members no longer have access to their online access and we must verify it. To verify your e-mail address and access your bank account, click on the link below.

<https://online.halifax.co.uk/OnlineBanking/security/update/SignIn/>

Please fill in the required information.

This is required for us to continue to offer you a safe and risk free environment.

Thank you
Accounts Management

Terms & Conditions
Copyright © 2006 HalifaxBank Corporation. All rights reserved.

Dear Valued Customer,

Halifax Bank plc is committed to protecting you with the latest technology to keep your details secure. Our dedicated teams and up-to-date security systems also monitor online activities and intercept all suspicious action. We do everything we can to protect our online customers, but the steps we take can be much more effective if you work with us to protect yourself.

On the 3rd of May 2006, our security systems detected an access attempt into your online banking account from IP address **81.199.84.196**. We issued this alert because this IP address, which is also in our blacklist, does not correspond with your default IP address registered with us.

Consequently, we require that you confirm your current IP address with us. Confirming your current IP address with us will enable us protect your online banking account from unauthorized access. **Please click here to confirm or change your current IP address***

IMPORTANT:

If you do not confirm your current IP address until 14th of May 2006, your account will be SUSPENDED for security reasons and we will send you a new Access Code by post which you will need to reactivate your online banking service access. You will receive this within seven days if your current IP address is not confirmed. **Please click here to confirm or change your current IP address***

Best wishes



Nigel Ridgeway
Online Security Advisor
Halifax Bank plc.

*This private and confidential e-mail has been sent to you by Halifax Bank plc (reg no 106048). Registered in England and Scotland. Registered offices: 1 Waterhouse Square, 138-142 Holborn, London EC1N 2NA.

This e-mail is confidential and for use by the addressee only. If you are not the intended recipient of this e-mail and have received it in error, please return the message to the sender by replying to it and then delete it from your mailbox. Internet e-mails are not necessarily secure. The Halifax group of companies do not accept responsibility for changes made to this message after it was sent.

Whilst all reasonable care has been taken to avoid the transmission of viruses, it is the responsibility of the recipient to ensure that the onward transmission, opening or use of this message and any attachments will not adversely affect its systems or data. No responsibility is accepted by the Halifax group of companies in this regard and the recipient should carry out such virus and other checks as it considers appropriate.

This communication does not create or modify any contract.

If you would prefer not to receive information about other products and services from us, please reply to this e-mail with 'opt-out'

Phishing

 Always giving you extra

[Home](#)

[Help](#)

New User

- ▶ [Register my existing account for the service](#)
- ▶ [Apply for a new account](#)
- ▶ [Find out how to use the online service](#)
- ▶ [View demonstrations](#)

 [More information](#)

Existing User - Sign in

Username

Password

Your place/town of birth?

▶ [Forgotten your sign in details?](#)

FIGHT ONLINE FRAUD



[CLICK HERE FOR THE LATEST NEWS](#)

 Always giving you extra

[Home](#)

[Help](#)

New User

- ▶ [Register my account for the online service](#)
- ▶ [Apply for a new account](#)
- ▶ [Why use our service?](#)
- ▶ [Try our demo](#)
- ▶ [Register for Employee Share Schemes](#)

 [More information](#)

Existing User - Sign in

Username

Password

Your place/town of birth?

Problems signing in?
[Forgotten your sign in details or is your access suspended?](#)

Visit our [Security section](#) for information on what we are doing to protect you.



FRAUDULENT E-MAIL ALERT

WE NEVER ASK FOR YOUR PERSONAL SIGN IN DETAILS BY E-MAIL

If you are not a UK resident, or are trying to access this site from outside the UK, please read this [important message](#)



Phishing

From: BankX **Identity Theft Protection Team**

To: You

Subject: IMPORTANT: Identity Theft **Incident Alert**

Dear You

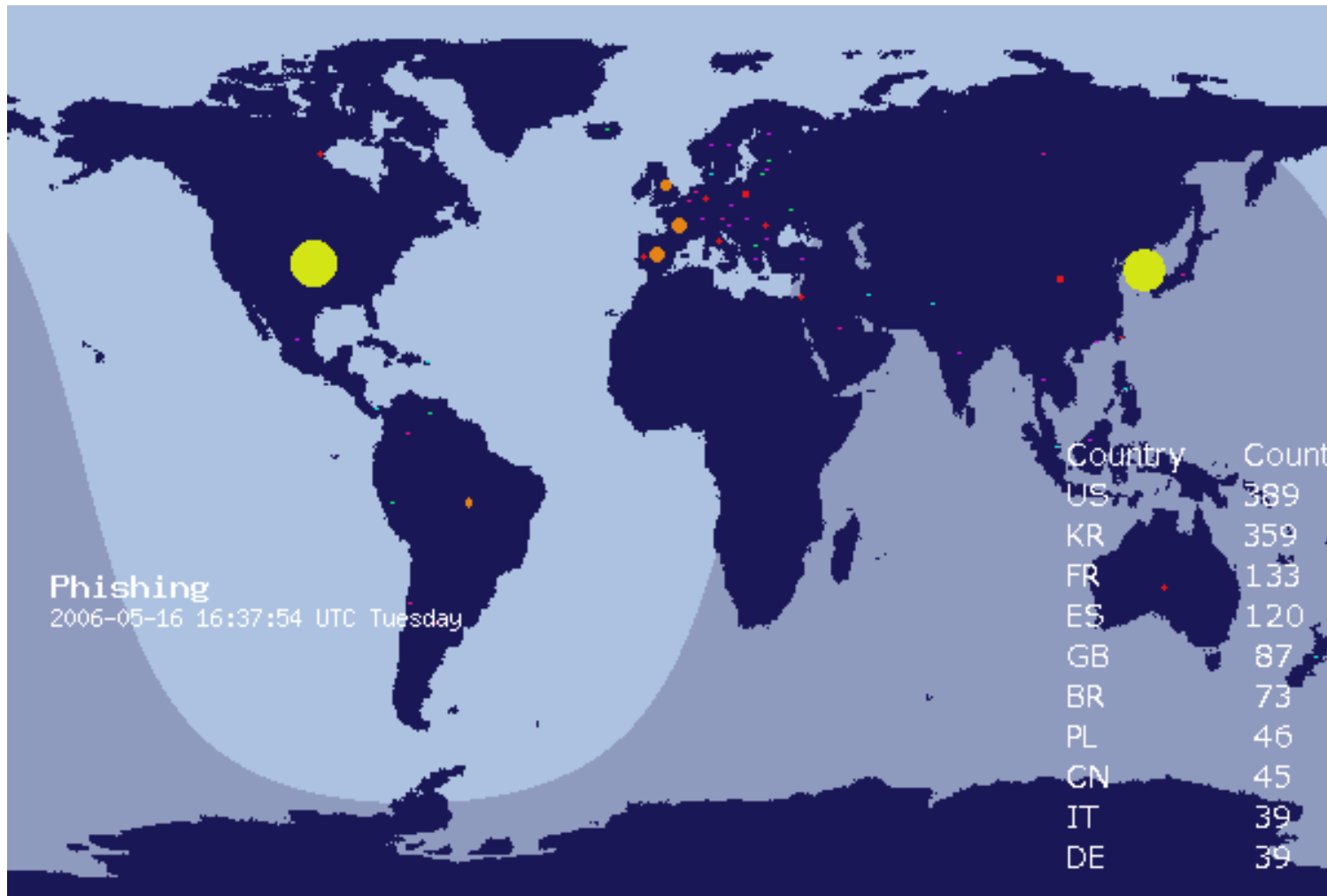
Our protection systems have detected an **ongoing** identity theft fraud on **your account**. We have **evidence** that funds are being withdrawn.

Under our **terms and conditions** **you are protected** from any losses you have suffered to date.

However, **you must act now** to change your security details **so you can stop any further theft**.

If you don't **re-activate your account now**, **you will be liable** for any further theft from your account

CLICK HERE



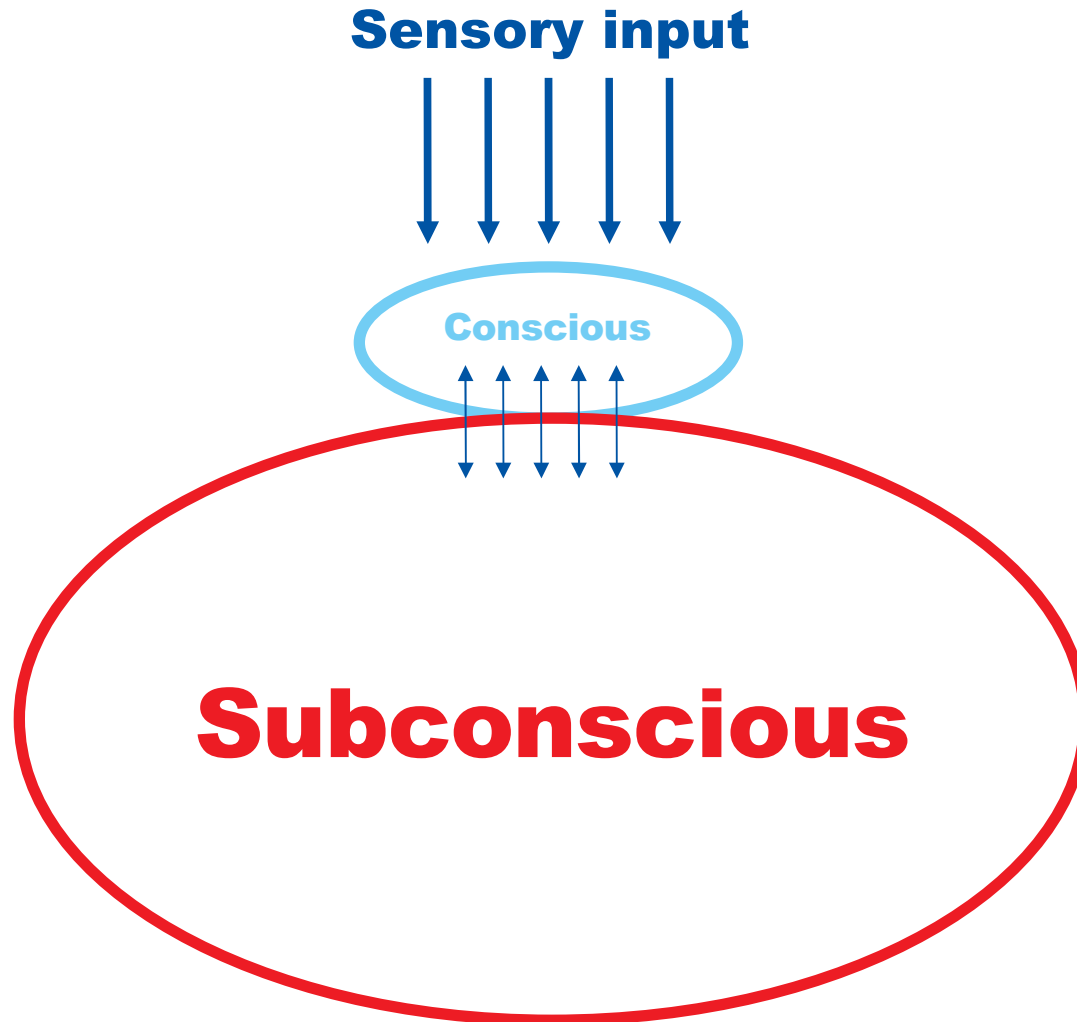
**INTERNET
DEFENCE**

**MAKING IT
more secure**

What Next?

- Spear Phishing
 - Targeted attacks
- Pharming
 - Redirecting traffic through a DNS compromise
 - “a marketing neologism designed to convince banks to buy a new set of security services”
Anti-Phishing Working Group
- Tickling

The Human Mind



The Human Mind

Conscious

- Believes it is in control
- Very slow
- Thinks, applies logic
- Limited multi-tasking
- No decisions

Subconscious

- In control (but can be 'easily' led)
- Fast
- Decides and acts
- Multi-tasking
- Remembers

Premature Evaluation

- Child - “Don't drop that”
- Politician - “A moment of madness”
- “Tell me, what is your current password?”

Instant Mind Control

It is all in the handshake

- Interrupt during a subconscious activity
- Instant access to the subconscious

Be careful!

Easy Targets

- Security Guards
 - Operate 99% in the subconscious due to hours of boredom and repetition
- Helpdesk Operations
 - Trained to be helpful
- Example
 - The **PEN** is mightier than the sword
 - Running a 'mind script'

If they can do it?



Understand your Human Vulnerabilities

- Vulnerability assessment and testing
- Risk assessment
- Incident reporting and analysis
- Raise staff awareness

Risk Assessment Process

- Information
- Information Assets
- Impact
- Threats
- Vulnerabilities
- Existing Countermeasures
- Probability
- Risk Level

Vulnerability Testing

- Risk assessment
- Adequate resources
- Combination attacks
 - Technical
 - Physical
- Realistic attacks
- Use of an insider?
- Dealing with alarms

Countermeasures

- Systemic
 - Minimise the impact of human vulnerabilities
 - Move employees into conscious processing
- Staff Awareness and Training
 - Trigger points
 - Incident procedures