nccgroup
freedom from doubt

Social Engineering

Techniques, Methods, Tools & Mitigation

Panagiotis Gkatziroulis, Security Consultant

Agenda

- **Social Engineering Methodology**
- **Attacks & Techniques**
- **Demos**
- **Tools of the trade**
- **Prevention Methods and Advice**

What is Social Engineering?

nccgroup
freedom from doubt

Invest in Products…

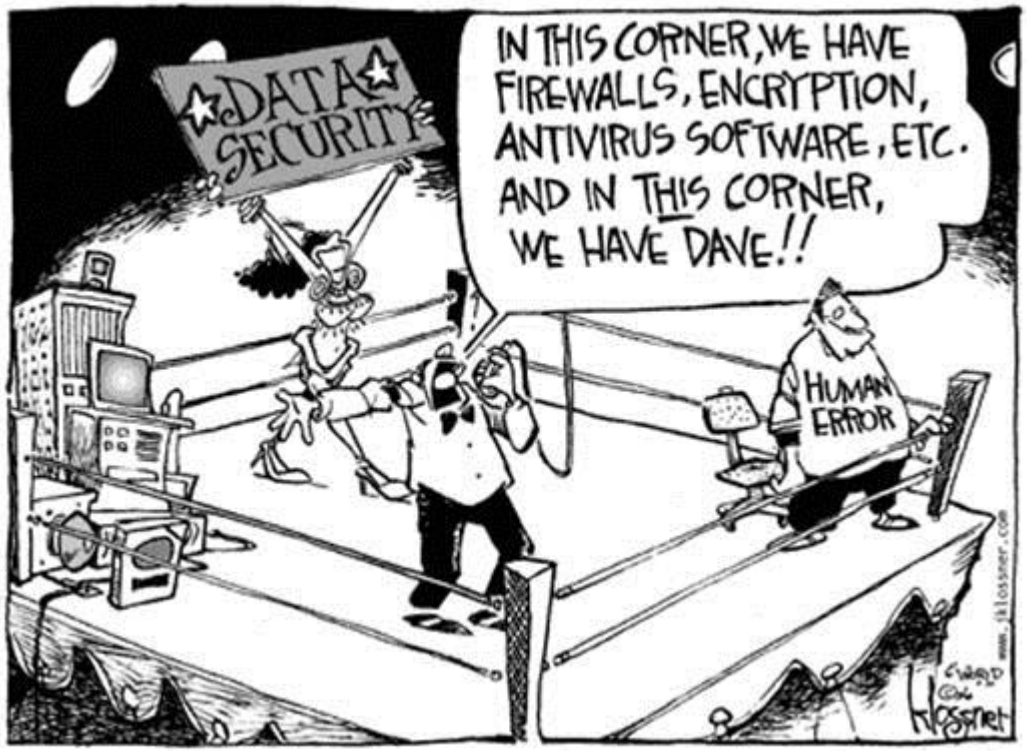
nccgroup
freedom from doubt

Is Our Security Focus Wrong?

nccgroup
freedom from doubt

Why Security Fail???

nccgroup
freedom from doubt



Who Are The Threat Actors?

- Aggrieved ex-employees
- Internal Employees
- Activists
- Corporate Espionage
- Blackhat Hackers

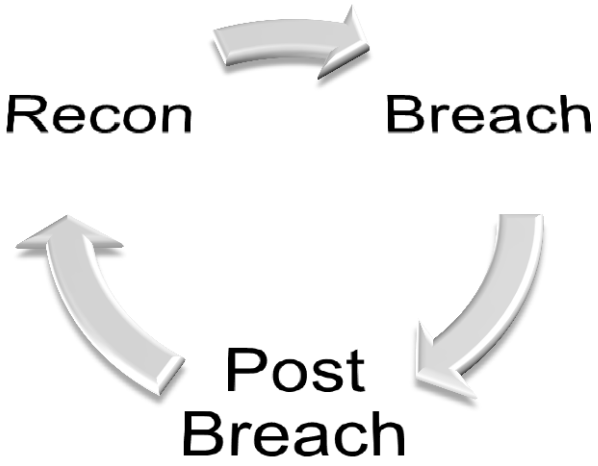
Who Are The Targets?

HR department

It Only Needs One…

nccgroup
freedom from doubt

Social Engineering Methodology



Social Engineering - Recon

nccgroup
freedom from doubt

Digital

- Search Engines
- Email Harvesting
- DNS Records
- Social Medial
- Metadata
- Public Records

Physical

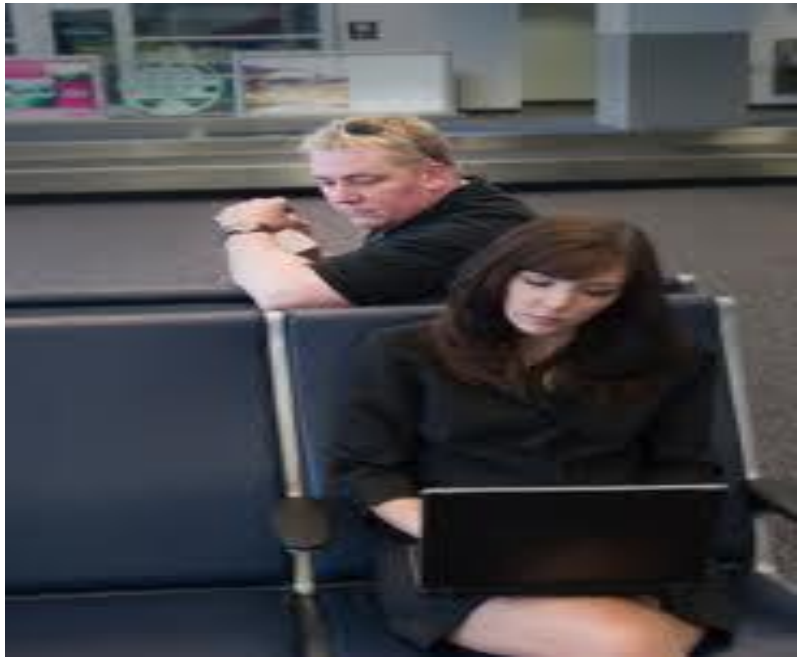
- Physical Walk
- Dumpster Diving
- Tailgate Employees to Lunch Breaks

Social Engineering - Breach

- Obtain Domain Credentials via Phishing Attacks
- Obtain Network Level Access via Spear Phishing Attacks
- Bypass Physical Security Defences and Obtain Corporate Documents

Attack Vectors

- Physical
- Phishing
- Telephone
- Shoulder Surfing
- Tailgating



Social Engineering Tactics

- Impersonation (Spoofed Emails, Telephone Attacks, Scenario-based attacks)
- Urgency
- Obligation
- Authority
- Flattering
- Fear

Do you recognize the signs?

nccgroup
freedom from doubt

Dear client,

Please find attached your invoice number 241-28195

If you have any queries with this invoice, please email us at accounts@cdsgroup.co.uk or call us on 020 8752 8040

The CDS Group of Companies, Passenger Car Services Same Day UK Couriers TV Support Units Overnight & International

Tel: 020 8752 8040
Email: accounts@cdsgroup.co.uk

Please consider the environment before printing this email.

Do you recognize the signs?

nccgroup
freedom from doubt

cds group

telephone: +44 (0) 20 8752 8040
email: enquiries@cdsgroup.co.uk

cds group

Dear client,

Please find attached your invoice number 241-28195

If you have any queries with this invoice, please email us at accounts@cdsgroup.co.uk or call us on 020 8752 8040

The CDS Group of Companies, Passenger Car Services Same Day UK Couriers TV Support Units Overnight & International

Tel: 020 8752 8040
Email: accounts@cdsgroup.co.uk

Please consider the environment before printing this email.

Do you recognize the signs?

nccgroup
freedom from doubt

cds group

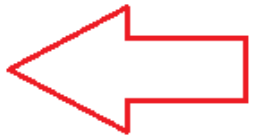
telephone: +44 (0) 20 8752 8040
email: enquiries@cdsgroup.co.uk

cds group

Dear client,

Please find attached your invoice number 241-28195

If you have any queries with this invoice, please email us at accounts@cdsgroup.co.uk or call us on 020 8752 8040



The CDS Group of Companies, Passenger Car Services Same Day UK Couriers TV Support Units Overnight & International

Tel: 020 8752 8040
Email: accounts@cdsgroup.co.uk

NCC Test Case

nccgroup
freedom from doubt

Outlook migration

support@[redacted]

Sent: Tue 22/04/2014 14:17

To: [redacted]

All,

As part of [redacted]'s migration to a new IT infrastructure we request that all users confirm that they are able to login to the email portal by 29/04/2014. Any accounts that have been dormant for over 2 months will be disabled.

Go to http://[redacted]/owa/auth/logon.aspx?logon=[redacted] and enter your username and password. These will be the same as your regular Windows credentials.

Thanks in advance for your assistance regarding this matter.
Kind Regards,

IT Helpdesk

Why This Attack Was Successful?

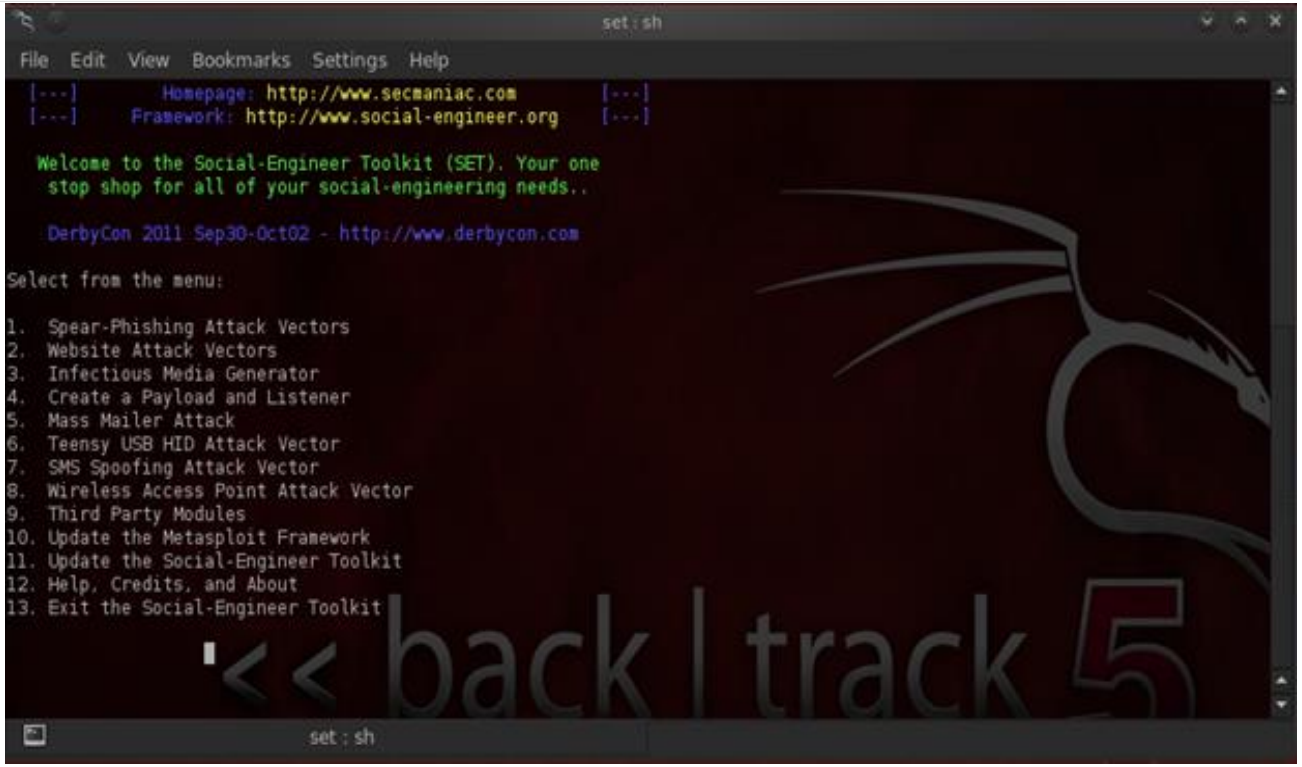
1. Trusted Source // IT Helpdesk
2. Promotes Fear // Accounts will be disabled

Lesson Learned?

Always Validate the Origin of the Information!!!

Tools of The Trade

- SET
- TheHarvester
- Recon-NG
- Phishing Frenzy
- PwnPlug Devices

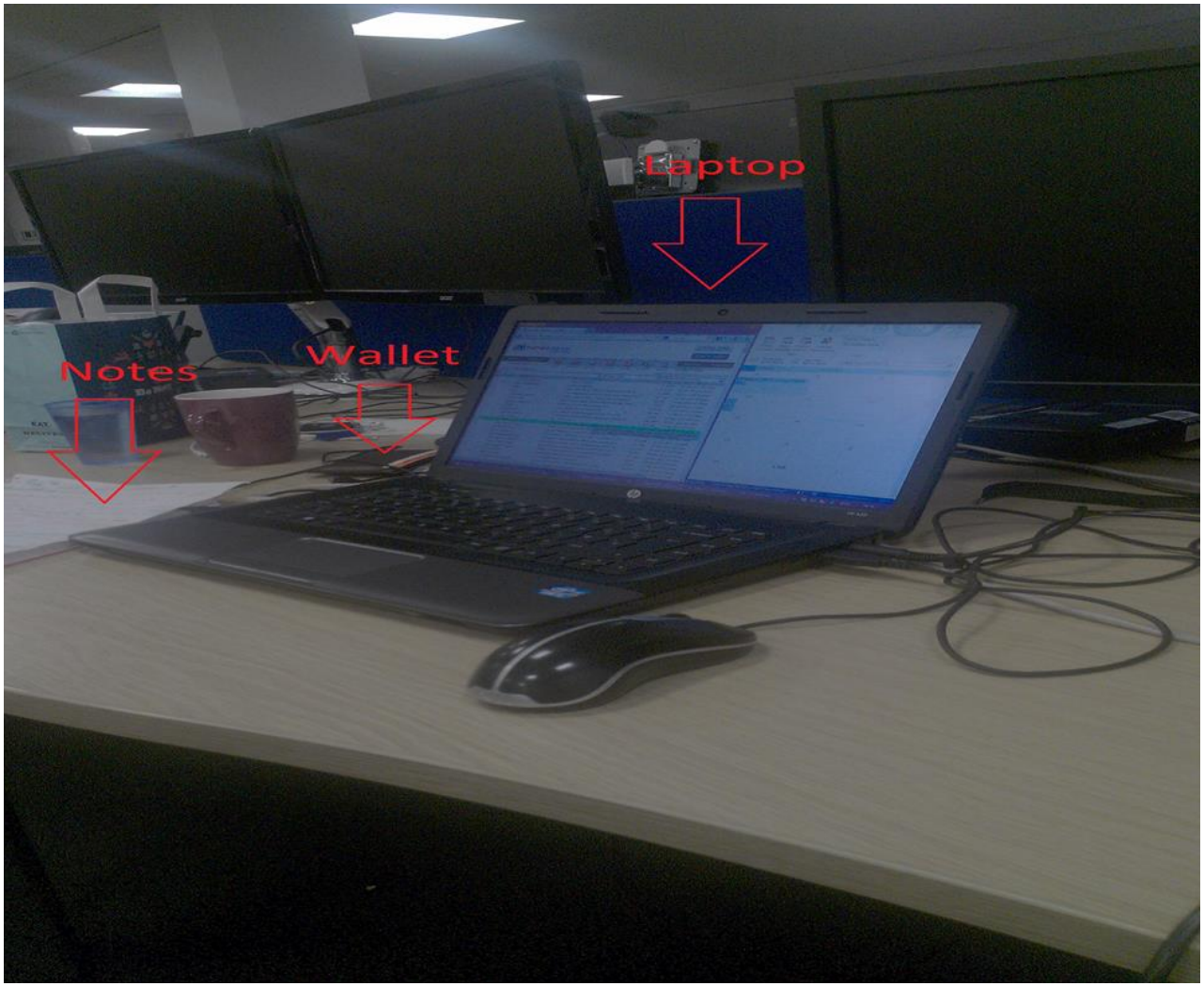


Physical to Cyber is Just One Port Away….

nccgroup
freedom from doubt

Do You See These Stuff Often Internally?

nccgroup
freedom from doubt



Mitigations

- **Limit Online Exposure**
- **Email and Web Gateway Solutions (URL Sandboxing etc.)**
- **Anti-tailgating Barriers**
- **Social Engineering Assessments**
- **Increase User Awareness via Trainings**
- **Policies (Escort visitors etc.)**

nccgroup
freedom from doubt

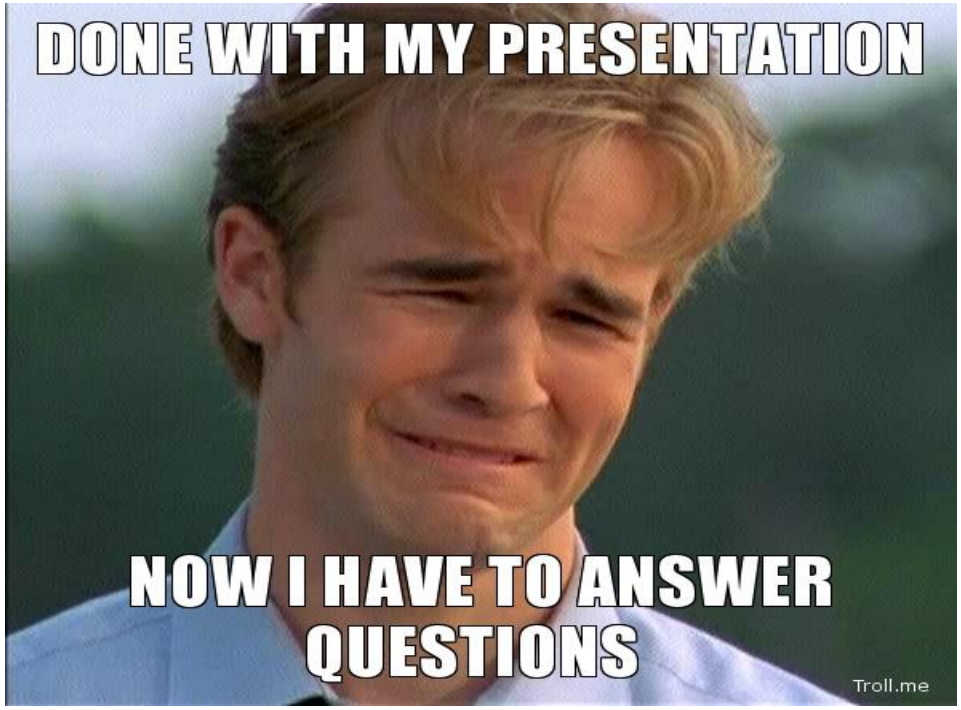
Conclusion

- **False Sense of Security (PCI DSS, Products etc.)**
- **Management People are Reactive NOT Proactive**
- **Strong Physical && Weak Human == Pwned**

- **Employees Must Feel Safe to Click Any Link Inside Their Company Environment!!!**

nccgroup
freedom from doubt

Any Questions???



trustforum
from NCC Group

The educational networking event for security professionals

nccgroup
freedom from doubt

Website: trustforum.nccgroup.com
Twitter: @NCCTrustForum
Email: trustforum@nccgroup.com

nccgroup
freedom from doubt

UK Offices

Manchester - Head Office

Cheltenham

Edinburgh

Leatherhead

London

Thame

North American Offices

San Francisco

Atlanta

New York

Seattle

Australian Offices

Sydney

European Offices

Amsterdam - Netherlands

Munich – Germany

Zurich - Switzerland