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?

SOCIAL ENGINEERING
The clever manipulation of the natural human tendency to trust.
Invest in Products…
Is Our Security Focus Wrong?
Why Security Fail???

IN THIS CORNER, WE HAVE FIREWALLS, ENCRYPTION, ANTIVIRUS SOFTWARE, ETC. AND IN THIS CORNER, WE HAVE DAVE!!
Who Are The Threat Actors?

- Aggrieved ex-employees
- Internal Employees
- Activists
- Corporate Espionage
- Blackhat Hackers
Who Are The Targets?
It Only Needs One…

WHY PHISHING SCAMS KEEP WORKING
Enter your bank account number.
SCAM.

WAIT FOR IT
Enter your bank account number.
SCAM.

THERE IT IS
Enter your bank account number.
OKEY-DOKEY.
Social Engineering Methodology
Social Engineering - Recon

**Digital**
- Search Engines
- Email Harvesting
- DNS Records
- Social Media
- 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
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.

This message and any attachment are confidential and may be privileged or otherwise protected from disclosure. If you are not the intended recipient, please telephone or email the sender and delete this message and any attachment from your system.

If you are not the intended recipient you must not copy this message or attachment or disclose the contents to any other person. This e-mail or any attachments are for information purpose only and does not form any part of an agreement, contract or fact.

The contents of an attachment to this e-mail may contain software viruses, which could damage your own computer system. Whilst The CDS Group has taken every reasonable precaution to minimise the risk, we do not accept liability for any damage, which you sustain as a result of software viruses. You should carry out your own virus checks before opening any attachment to this e-mail.
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.

This message and any attachment are confidential and may be privileged or otherwise protected from disclosure. If you are not the intended recipient, please telephone or email the sender and delete this message and any attachment from your system.

If you are not the intended recipient you must not copy this message or attachment or disclose the contents to any other person. This e-mail or any attachments are for information purpose only and does not form any part of an agreement, contract or fact.

The contents of an attachment to this e-mail may contain software viruses, which could damage your own computer system. Whilst The CDS Group has taken every reasonable precaution to minimise the risk, we do not accept liability for any damage, which you sustain as a result of software viruses. You should carry out your own virus checks before opening any attachment to this e-mail.
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.

This message and any attachment are confidential and may be privileged or otherwise protected from disclosure. If you are not the intended recipient, please telephone or email the sender and delete this message and any attachment from your system.

If you are not the intended recipient you must not copy this message or attachment or disclose the contents to any other person. This e-mail or any attachments are for information purpose only and does not form any part of an agreement, contract or fact.

The contents of an attachment to this e-mail may contain software viruses, which could damage your own computer system. Whilst The CDS Group has taken every reasonable precaution to minimise the risk, we do not accept liability for any damage, which you sustain as a result of software viruses. You should carry out your own virus checks before opening any attachment to this e-mail.
Outlook migration

support@NCC.com

Sent: Tue 22/04/2014 14:17
To: NCC Support

All,

As part of NCC’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://ncc.com/owa/auth/logon.aspx?logon= 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....
Do You See These Stuff Often Internally?
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.)
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!!!
Any Questions???

DONE WITH MY PRESENTATION

NOW I HAVE TO ANSWER QUESTIONS
Website: trustforum.nccgroup.com
Twitter: @NCCTrustForum
Email: trustforum@nccgroup.com
UK Offices
Manchester - Head Office
Cheltenham
Edinburgh
Leatherhead
London
Thame

European Offices
Amsterdam - Netherlands
Munich – Germany
Zurich - Switzerland

North American Offices
San Francisco
Atlanta
New York
Seattle

Australian Offices
Sydney