

Embrace the Click

FIVE EFFECTIVE SOCIAL ENGINEERING PROTECTIONS

DAN BOUGERE

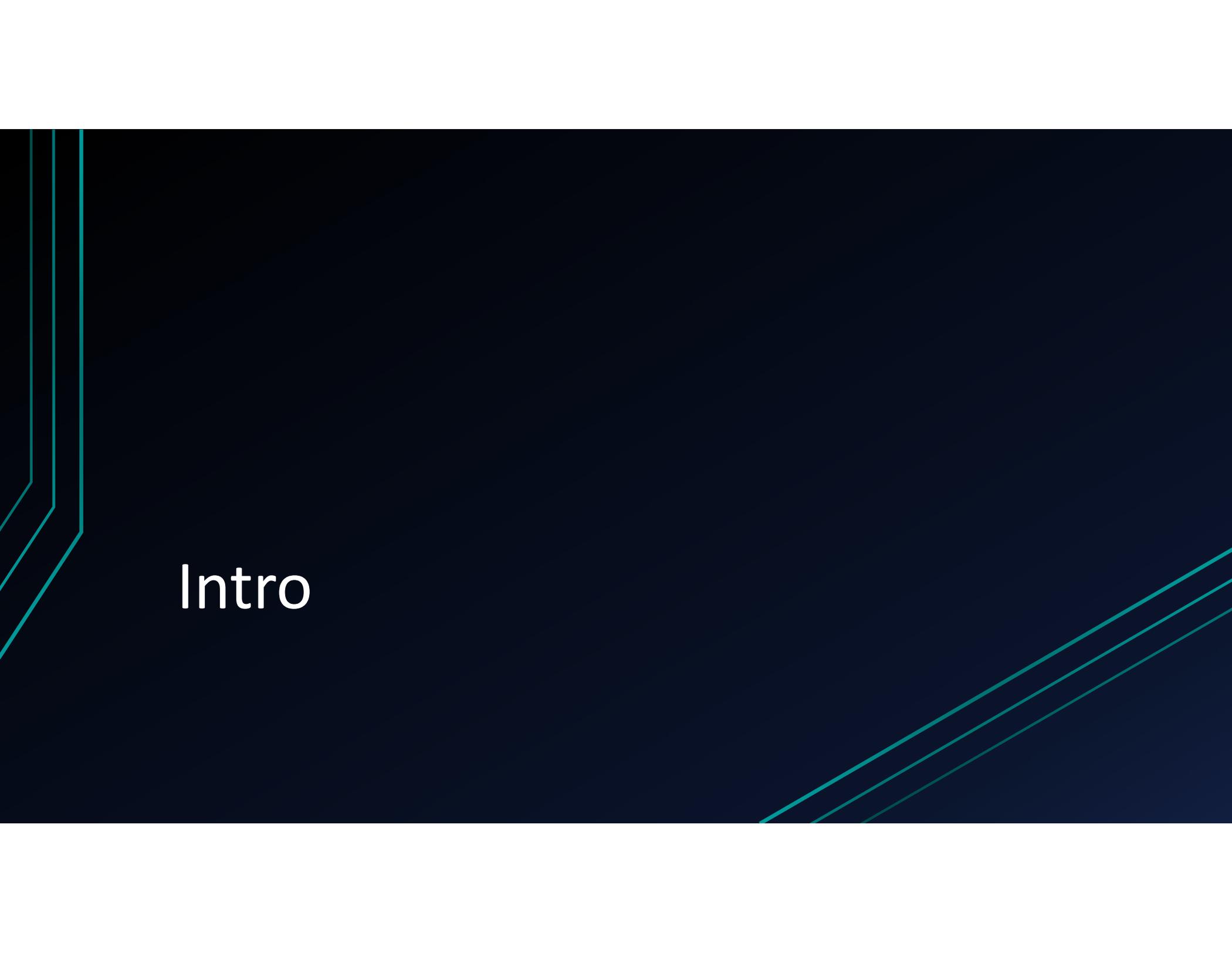
Traffic Light Protocol

- This presentation falls under WHITE
 - “Subject to standard copyright rules, WHITE information may be distributed freely, without restriction”

https://en.wikipedia.org/wiki/Traffic_Light_Protocol

What We Will Cover

- Intro
- Pick Your Battles
- Five Methods
- Takeaway



Intro



Who Am I

- Last name is pronounced BOO-zhair
- 13+ Years in IT
- Last 10 spent in various security roles
- Spent time in the Intelligence Community doing “fun” things that used many methods of social engineering
- Senior Security Consultant at Securicon, LLC doing the same “fun” things for commercial and government clients.
 - <http://securicon.com>

What exactly is social engineering?

- Essentially, convincing someone to do something they otherwise would (or should) not.
- Relies on many ingrained psychological traits:
 - Rapport
 - Deference to authority
 - Reciprocation
 - Consistency of action/thought
 - Desire to help those in need
 - Desire to be considered a “good” or “helpful” person

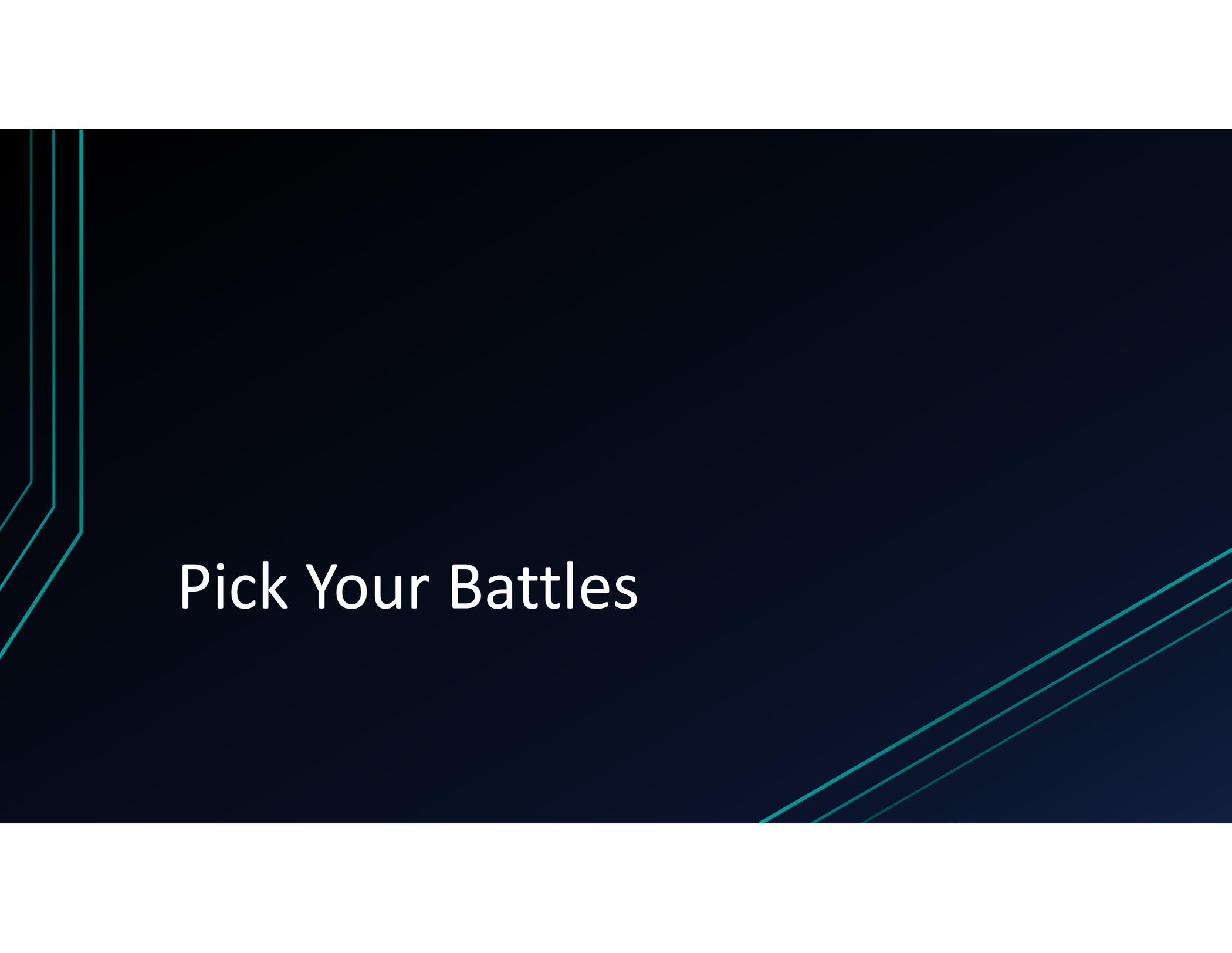
Why is it effective?

- Modern defense-in-depth strategies have made traditional methods of exploitation extremely difficult and time consuming.
- There is very little risk associated with performing these activities.
- Humans are, by far, the weakest link in any security chain.

“Every organization has that one person....”



©20th Century Fox



Pick Your Battles

Typical Social Engineering Threats

- Data Loss
 - Intellectual Property
 - Proprietary Information
- Ransomware
- Financial/Wire Transfer
- Internal/Customer Account Access

No, They Couldn't Have!



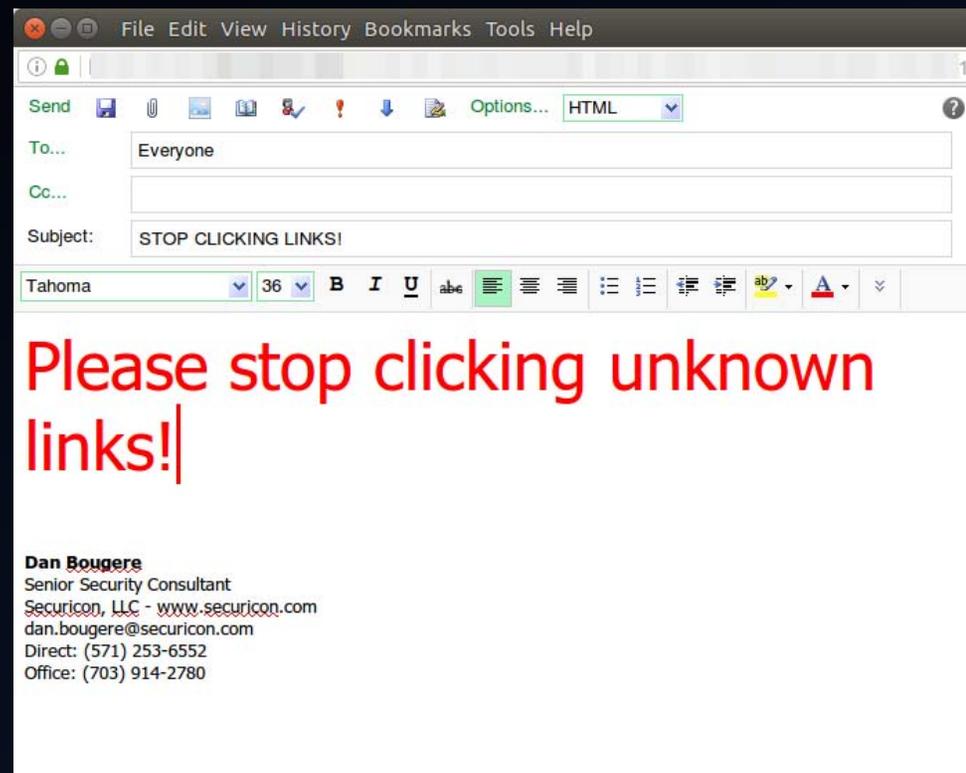
KrebsonSecurity
In-depth security news and investigation

07 FBI: \$2.3 Billion Lost to CEO Email Scams

APR 16

The **U.S. Federal Bureau of Investigation** (FBI) this week warned about a “dramatic” increase in so-called “CEO fraud,” e-mail scams in which the attacker spoofs a message from the boss and tricks someone at the organization into wiring funds to the fraudsters. The FBI estimates these scams have cost organizations more than \$2.3 billion in losses over the past three years.

Why Keep Fighting?



Seriously, Why Keep Fighting?



**WATCH THIS HACKER
BREAK INTO
MY CELL PHONE ACCOUNT
IN 2 MINUTES**

Mindful Acceptance

- Your people are going to do this.
- You are expecting them to change ingrained social behaviors from our earliest ancestors.
- Everyone knows what the “definition of insanity” is, right?



Five Methods

1

Use Your Existing Technology

1 – Use Your Existing Technology

- Turn **OFF** HTML email.
 - Email is used for business communication, yes? Do you really need backgrounds, icons, or cat pictures?
 - Multiple methods to hide malicious links are quickly exposed in text-only emails.
 - Web bugs are popular and can provide drips of information that are useful in later stages. These are not viable in non-HTML email.
 - There are many how-to guides available for almost all email servers:
 - Gmail - <https://support.google.com/a/answer/2786758?hl=en>
 - Exchange 2013 - [https://technet.microsoft.com/en-us/library/bb310794\(v=exchg.150\).aspx](https://technet.microsoft.com/en-us/library/bb310794(v=exchg.150).aspx)

1 – Use Your Existing Technology (2)

- Blacklists

- While not perfect, there are many blacklists maintained on the internet that you can subscribe and implement on your server(s).
 - Return Path Reputation Network Blacklist (RNBL)
 - SpamHaus
 - SpamCop
 - Many more: <https://blog.returnpath.com/blacklist-basics-the-top-email-blacklists-you-need-to-know-v2/>

1 – Use Your Existing Technology (3)

- Antivirus and Gateway Scanners
 - Everyone is running an antivirus scanner on their email server, right?
 - It is much easier to stop infections and shenanigans at the source.
 - Most popular malware and ransomware comes in archives (zip, tar, msi, etc) or in malicious Office or PDF documents.
 - Or in BOTH!
 - ClamAV is a popular solution that is cross platform.
 - <http://www.clamav.net/>

1 – Use Your Existing Technology (4)

- Filtering

- Everyone has a firewall, even if it is Windows Firewall or iptables.
- Most are familiar with blocking unwanted traffic coming **IN** to the network.
- What if I told you that you can also do the same thing for traffic going **OUT** of your network?

- Do client desktops need to send email via SMTP?
- Do your file servers (or any servers) need to communicate to servers in Asia or Eastern Europe?
- Do your credit card systems need to communicate with ANYONE else besides your processor? Hint: This answer should probably be no.

2

Social Media/Internet Awareness

2 – Social Media/Internet Awareness

- You would be amazed at the amount of information that is available on social media.
 - It's not just Millennials!
 - It takes one friend/contact who isn't careful to open up your entire profile.
 - Metadata is also important
 - Friends of friends
 - Interest groups
 - Alumni networks

2 – Social Media/Internet Awareness (2)

- You would be appalled at the amount of information that is available on BUSINESSES via social media.
 - Photographs with tags of employees/positions
 - Philanthropic outreach
 - Advertising
 - Contract Awards
 - Open Positions

2 – Social Media/Internet Awareness (3)

- You would be terrified at the amount of information that is available via Google and other search engines.
 - Google...Google Hacking: https://www.blackhat.com/presentations/bh-europe-05/BH_EU_05-Long.pdf
 - Documents
 - Directories
 - Firewall/Router Configurations
 - Waivers on Old Technology

2 – Social Media/Internet Awareness (4)

- Recognize that this information is out there, and will be used by bad people.
- Recognize that a blanket ban is unrealistic and ineffective.
- Find a middle ground!
 - Mitigate the amount of information exposed on social media and the internet
 - Restrict profiles to Friends/Contacts only
 - Stress to everyone that this information can be used against not only them, but everyone ELSE that knows them.

3

Procedures and People

3 – Procedures and People

- What happens when someone gets a call or an email from “IT” requesting their password be reset?
- What happens when someone receives an “urgent request” from your CEO to transfer money to an account quickly?
- What happens when your front desk person is asked to plug in a thumb drive when a client’s laptop mysteriously no longer works?
- What happens when someone forgets or loses their badge?

3 – Procedures and People (2)

- Remember those psychological traits we discussed earlier?
- If an individual has no guidance, they will do what they feel is best. That is what social engineers depend on!
 - “IT you said? Sure, I’ll go change my password right now on the new site.”
 - “I’ll transfer the money right now. The reference ID is....”
 - “Sure! Here, I’ll print those up for you really quick. Technology huh?”
 - “I’ll badge you in this time, but next time you’ll need to get a temp one.”

3 – Procedures and People (3)

- Give them the tools to be successful!
 - Procedures
 - Accounts and passwords
 - Financial transactions
 - Change management
 - Access controls
 - Other critical areas
 - Points of Contact
 - Who do I call when I get a request outside of procedure?
 - Who do I call second when the first person is sick, on vacation, or just not answering?



4

Training

4 – Training

- Individuals have a variety of technology levels, cultural touchstones, trusting behavior, and willingness to help.
- Social engineers will keep trying until they find “that one user.”
- How do we get everyone on the same page?

4 – Training (2)

- Send phishing emails
 - Many companies will provide this service with differing degrees of fine tuning.
 - May also provide off-the-shelf solutions and ongoing training
- Make vishing calls
 - Again, many companies will provide this service and ongoing training.
- **NO ONE IS IMMUNE**, so no one should be excluded.

4 – Training (3)

- Take this seriously. Bad guys do!
 - “Annual Training” is basically useless. No one pays attention and wants to get through it as quickly as possible.
 - All negative reinforcement all the time is ineffective as well. You will terrify people into refusing to do anything for anyone.
- Games and Positive Reinforcement
 - Competition is good!
 - Small rewards and prizes for “catching the phisherman” keeps it relevant, and if you ever ARE targeted...
 - Positive atmosphere of communication. When in doubt, ASK!



5

Vigilance

5 – Vigilance

- It is vitally important that the same emphasis is placed on securing the human as well as the organization.
- Remember that we are all susceptible, and that our attack surface is constantly changing as we live our lives.
- Instill a healthy skepticism in all new hires, and make sure they are aware of policies and procedures. New hires are always a target!
- Make sure to stress that anyone may question a request and have it verified at any time with NO repercussions.



Takeaway

What Did We Learn?

- Your people are going to do this. Accept that!
- Give them the tools and awareness to fight back.
- It's better you do it rather than "Peggy" from Posnan, right?



©Discover



Dan.Bougere@Securicon.com



@Rouxgaru



<https://www.linkedin.com/in/danbougere>



Slides: <https://github.com/Rouxgaru/slides>