

Hacking the Human Social Engineering (and why it can work on anyone)

Duke IT Security Office

April 2017

Social Engineering

The act of influencing an individual to take an action that may or may not be in their best interest

SE Isn't Always an Attack

- Child/Parent
- Customer Service
- Television
- Doctors

Attacking Humans, Not Computers

- Computers - vulnerabilities / exploits
 - Time & effort
- Humans – “Ask and ye shall receive”
 - Inherent desire to help
 - Emotional beings
 - Sorrow, celebrate, curious, opinionated, etc.

Don't Believe Me? Just Ask Jimmy Kimmel

<https://www.youtube.com/watch?v=opRMrEfAlil>

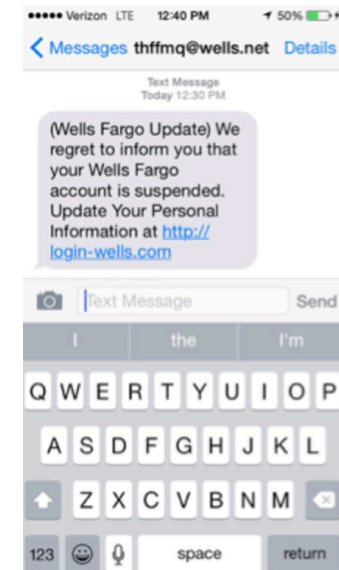
Something to Consider

Physical “Attacks”

- Shoulder surfing
- Tailgating
- Pin Codes
- Unlocked workstation

SE as an Attack

- Phishing – sending email to fraudulently obtain sensitive info
- Vishing – “phishing” via voice/phone calls
- Smshing – “phishing” via SMS/texting
- Pharming – method of fraudster installing malicious code onto a computer which redirects the user to fraudulent websites to harvest credentials



Types of Phishing

- Spearphishing – “phishing” a specific individual or group
- Whaling – “phishing” high level executives

Direct Deposit Fraud

From: DUKE Payroll Department <employeebenefits@duke.edu>
Reply-To: "hulacyun1@gmail.com" <hulacyun1@gmail.com>
Date: Thursday, March 13, 2014 at 12:01 PM
To: override <XXXXXXXXXXXX@duke.edu>
Subject: Your Salary Raise Details



Hello,

You are qualified for a salary raise on your next paycheck in March, follow the steps below to immediately confirm your details.

Allow few hours for your congratulatory letter to be delivered to your email "DU email"

Click here:

<http://support.duke.edu/employee-compensation>

Whaling – CEO Fraud

From: Kevin White <kwhite@duaa.duke.edu>
Date: August 10, 2016 at 11:41:03 AM EDT
To: <shelia.allen@duaa.duke.edu>
Subject: Re: Request
Reply-To: Kevin White <executiveceo2@aol.com>

Shelia,

I request you to kindly effect this W-transfer in on my behalf and consent as soon as you can and process the transfer required as same-day W-transfer instant payment to the vendors account.this request is urgent and must be treated confidential.

Bank Name: SharonView Federal Credit Union
Bank Address:501 N Main St, Salisbury, NC 28144, USA
Account Name: Toby meadows
Routing Number: 253075303
Account number: 713970

Amount: \$10,879

Basically this payment is for a project we are involved in as a sponsor.i will prepare the documents and make them ready before the end of today. And I will be expecting the hard cover of the invoice in order to know where to code this transaction, hopefully I should receive it later today or tomorrow,Reference it as donation, Please note there is an incoming transfer coming soon, I will let you know when the beneficiary company get in touch with me.Get back to me with a copy of the payment slip via email once you get the Wire transfer done.

Regards
Kevin White

Ransomware


From: **Arielle Vaisman** <vaisman.arielle8vr7@outlook.com>
Date: Sun, Dec 4, 2016 at 1:55 PM
Subject: Re: [REDACTED]
To: [REDACTED]

[REDACTED]

You will be charged USD ,181.94 on your Visa balance soon.
Check attachment for details.
Pwd for the file is 7778.

Respectfully yours
Rosie

From: USPS Priority Delivery [mailto:bruce.daniels@naitoh-denki.co.jp]
Sent: [REDACTED]
To: [REDACTED]
Subject: Parcel ID9967789 delivery problems, please review

Attached  Undelivered-Package-...
.zip File



Dear Customer,

Your parcel was successfully delivered January 20 to USPS Station, but our courier could not contact you.

Postal label is enclosed to this e-mail. Please check the attachment!

Thanks and best regards,
Bruce Daniels,
USPS Station Manager.

Re: Documents Re [REDACTED]

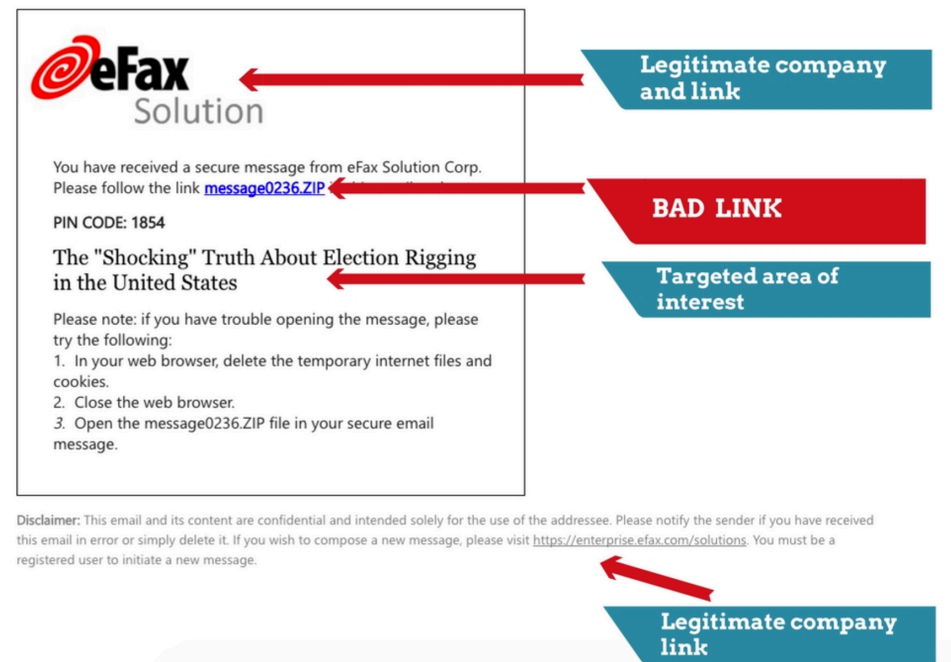
 **Fernando**
Friday, August 12, 2016 at 6:28 AM
To: [REDACTED]
📎 :  Untitled(18).zip (9.2 KB) [Preview All](#)

Dear [REDACTED],

Please find attached documents as requested.

Best Regards,
Fernando

APT



It Can Happen to You & Me

- It's just a matter of the right..
 - Time
 - Scenario
 - Mood
 - Info
 - Background

Scenarios

- Amazon order cancelled due to issues with Credit Card -- (*fear*)
- HR is giving away Men's BB tickets for survey completion -- (*entice*)
- Manager forwards required training at the last minute -- (*urgency*)

SE Isn't Just for Phishing

- Hacking
 - Penetration Testers (“The good hackers”)
 - Spies/Espionage
 - Identity Theft
 - Disgruntled Employees
 - Scam Artists
-
- Recruiting
 - Sales

And When We Want to Help

<https://www.youtube.com/watch?v=e-ZcomTYc64>

Reconnaissance

Know the individual / organization

- Background
- Relationships
- Skills
- Social Media

What Do They Want with Me?

- Username / Passwords
- Access
- Contacts
- Relationships
- Identity

Open Source Intelligence (OSINT)

Intelligence collected from publicly available sources. In the intelligence community (IC), the term "open" refers to overt, publicly available sources (as opposed to covert or clandestine sources); it is not related to open-source software or public intelligence.

AKA

- Recon
- Scoping
- Footprinting
- Cyberstalking

Recon Tools

- Metasploit
- Recon-ng
- Maltego
- Various scrapers

Search Engines (Other than Google)

- Alhea
- Aol Search
- Ask
- Baidu
- Bing
- Cluuz
- Contenko
- Deeperweb
- Dogpile
- DuckDuckGo
- EntireWeb
- Exalead
- Gigablast
- Info
- Infospace
- Ixquick
- Mozbot
- MyWebSearch
- Oscobo
- Peeplo
- Qwant
- Soovle
- Sputtr
- StartPage
- Teoma
- Yahoo
- Yandex
- Yippy
- WebCrawler
- Wow

People Searching

- Black Book Online
- Intellius
- Peekyou
- Pipl
- Rootsweb
- Snitch.name
- Spokeo
- UserSearch
- Webmii
- Zaba Search
- ZoomInfo

Social Media/Networking

- Classmates
- Facebook
- Flickr
- Google+
- Hi5
- Instagram
- Kik
- LinkedIn
- Meetup
- Periscope
- Pinterest
- Reddit
- SnapChat
- Swarm
- Tumblr
- Twitter
- Vine
- YikYak
- YouNow
- YouTube

More Online Profiles

- Online Dating
 - eHarmony, Match.com, Zoosk, Tinder, etc.
- Online Gaming
 - Miiverse, Playstation Network, Xbox Live, Twitch

The List Goes On

- Online communities
 - Google groups, Yahoo groups, many forums
- Specific interest communities
 - Reverbnation, Sportstats, DeviantArt, Nextdoor
- Blogs
 - Blogger, Wordpress, etc.

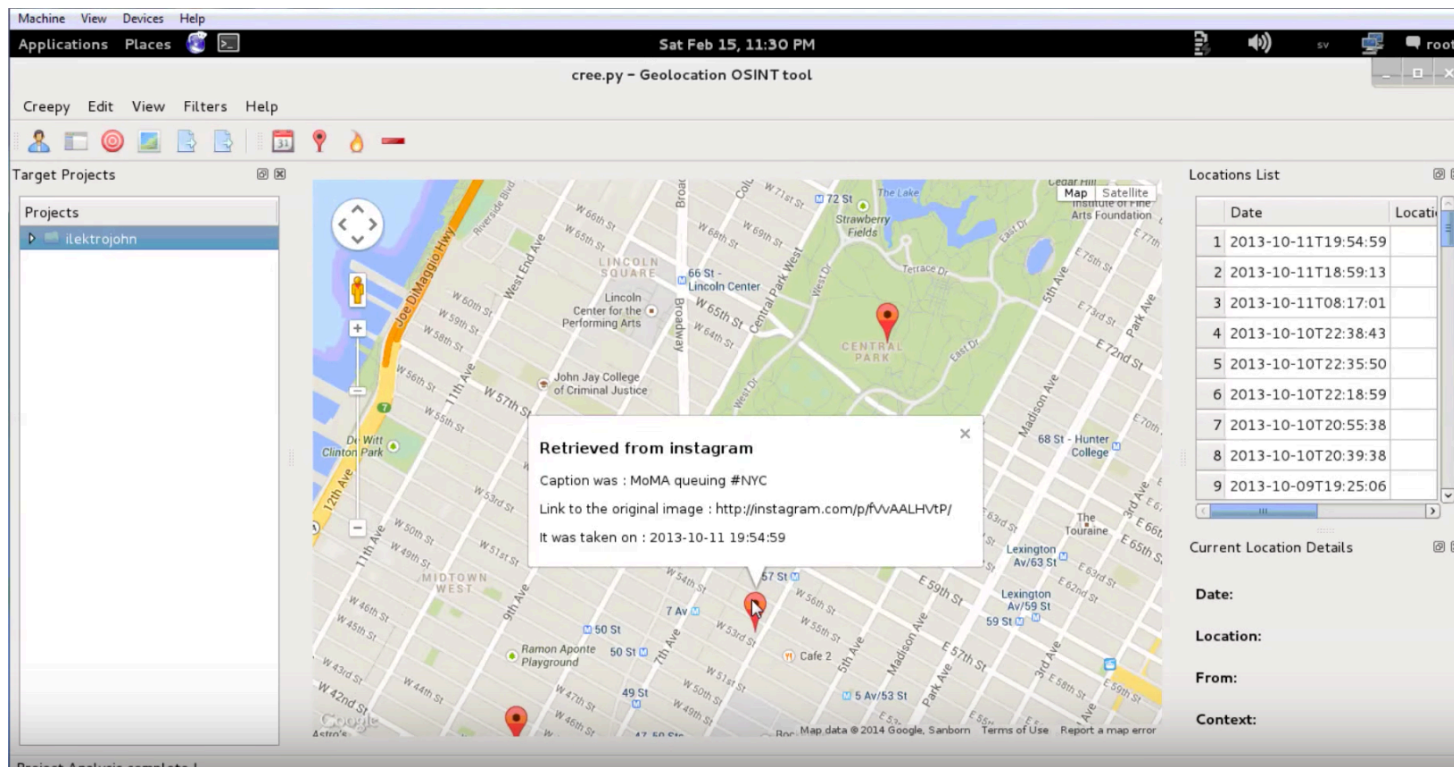
Online Classified

- Amazon
- Craigslist
- Ebay
- Geebo
- Oodle
- So many more

GeoLocation Searching

- Creepy
- Echosec
- Google Maps APRS
 - (Auto-Position Reporting System)
- Pushpin
- Social Bearing

Cree.py



Facebook Recon

- FindMyFBid.com
 - Used to acquire Facebook "ID"
- IntelTechniques.com/OSINT/facebook.html
 - Using the acquired ID search for info on FB

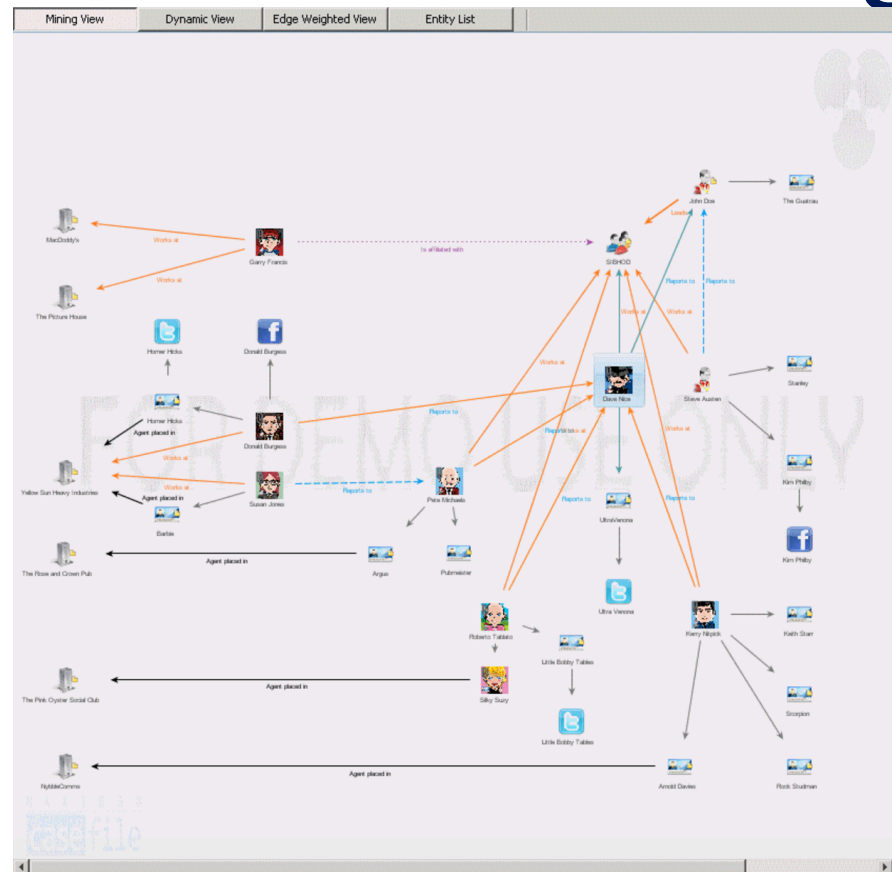
Linkedin Recon

- Linkedin-gatherer
 - [Github.com/DikS0nn3cT](https://github.com/DikS0nn3cT)
- Linkedin Scraper
 - [Github.com/yatish27](https://github.com/yatish27)
- Linkedin tool to gather profile data
- Import into OSINT relationship analysis tools such as Recon-ng or Maltego

Recon-ng / Maltego

- Relational database of information used to link “pieces of info” together
- Handles / automates correlation of large datasets
- Ex. – linking relationships of things such as websites, email addresses, IP info to gain context or insight into a target

A Visual of Maltego



The Moral of this Story

Thoughts, Questions,
or Concerns?

Thank You!