Victor O. Schinnerer & Company, Inc.

YOU (and me) are the Weakest Link of a Social Engineering Hack

Jason Bucher, Senior Cyber Underwriter

A very recent personal experience

- My wife received call claiming to be from “Google Network Service” alerting her to “Unusual activity from our home network”
- The helpful caller offered to assist in setting up stronger virus protection but first needed our username/password
- We were saved from harm – as my wife could not remember our passwords…(they auto-populate from Dashlane)

“The first step toward change is awareness. The second step is acceptance” - Nathaniel Branden

- All of us have uttered the phrase – “It wouldn’t happen to me…”
  - Truth is…it can, and it will.

Outline for Today:

- Social Engineering – aka Human Hacking
- Common delivery methods/models of Social Engineering with specific loss events (awareness and acceptance)
  - Physical Social Engineering - Impersonation
  - Phone Social Engineering - Vishing
  - Email Social Engineering - Phishing
- Tips and Advice on how to prevent falling victim
- What to do if you fall victim

Social Engineering – Human Hacking

- **Social Engineering** is hacking of the end user. Technical/system vulnerabilities can be identified and corrected – but human error or decisions cannot
- Exploiting trust, emotions and personal interest – the target is manipulated into making a mistake or releasing targeted information

Social Engineering – Human Hacking

- 52% of successful email attacks get victims to click within an hour, 30% clicked within 10 minutes
  - The Human Factor 2018 Report by ProofPoint
- 43% of the 42,068 documented security breaches studied by Verizon involved a social engineering attack vector
  - 2017 Verizon DBIR
- Awareness training is the best defense – reducing risk by as much as 45 to 70%
  - Wombat Security Technologies and Aberdeen Group study
- Average cost of cyber crime has risen 62% since 2013
  - 2017 Cost of Cyber Crime Study by Poneman institute

Social Engineering Method - Impersonation

Why kick down the door when you can be invited?

- Armed with a $4 Cisco polo shirt from a thrift store and talking points from marketing material and support admin forums

Who ordered a sandwich?

- Armed with an empty sandwich bag, a red polo shirt, and name/title/contact info from LinkedIn

Interesting anecdote:

- Penetration test firm has 100% success rate with impersonation attempts

Social Engineering Method – On the Phone (Vishing)

A call from IT

- Armed with a spoofed phone number, individual details obtained from Facebook and LinkedIn

A different twist on a call from IT

- Armed with a spoofed phone number, individual details from Facebook, Network credentials from an IP ping, an official looking support e-mail with compromised link

Example of professional Vishing – and how quick it works:

- https://youtu.be/-Of7IaWzCVo

Social Engineering Method - Phishing

De-activation notice

- A simple email purporting to be from your bank or card issuer detailing false suspicious card activity requesting you to log in and review

Password reset/update notice

- An email purporting to be from IT service provider security department urging to update password or improve security procedures

Updated school event notice

- An email or notice purporting to be from your child's school with link to updated time or details for upcoming conference/dance

Social Engineering Method - Phishing

NSA/Edward Snowden

- Exploiting his position as a computer systems admin, he obtained between 20 and 25 credentials for fellow NSA workers in Hawaii.
- This detail to the NSA/Snowden saga proves just how successful a social engineering campaign can be

CIA Director John Brennan

- A 15 year old activist purported to be a Verizon employee to obtain user info for John Brennan. These details were used to reset the email password. With the changed password he was able to change security questions which then granted him access to the emails, contact list, iCloud storage and even his wife's iPad

How to Avoid Falling Victim

End User Awareness training
- Awareness of scam techniques – fake Tech Support calls, inspections, unexpected deliveries, urgent requests
- Account history or other seemingly innocuous data can form pieces of a bigger puzzle
- Skillbridge or similar service highly useful

Never provide personal information over the phone in response to a call
- Sounds like a no-brainer, but preparing individuals to resist is key to success

Password protection
- Use of Dashlane or similar service

Social Media education
- Choose wisely what info is shared
- Educate how social media information can be used to manipulate

What to Do if you Discover a Social Engineering attack

Move Quickly!

- Contact Fraud department of all banks involved
  - They have tools available
- Contact the FBI!
  - They have tools available
- Contact the Breach Coach
  - They have heard it all before – and can help
- Contact your Insurance Agent
  - They can assist in issuing notice to applicable insurance policies

Use Counsel to Establish Privilege

- Counsel directs forensics, notice drafting, and other vendors so that, in the event of litigation or regulatory investigation, all documents and communications are not discoverable
- Guard Attorney-Client Privilege: **do not** share forensic reports, legal analysis and drafts with clients or third parties if not absolutely necessary

What to Do if You Personally Fall Victim

- Contact your bank's fraud department
- Set up credit monitoring/credit freeze depending on nature of data released
- Contact law enforcement and file report
- Contact your homeowners insurance agent – might have coverage available for certain losses

Actions Upon Discovery – Additional Thoughts

- Have a plan in place **before** an event happens
  - Who internally should be contacted
  - Have banking contact information available – don't just call the front desk
  - Have FBI contact information available

- Additional reading on the topic:
  - http://www.maximumcyberliability.com/youve-been-breached/
  - http://www.maximumcyberliability.com/victim-of-wire-fraud-the-fbis-fkkc-program-can-help/

Tools and Actions to Minimize Cyber Risk

Dashlane

Every Schinnerer Cyber policyholder is provided access to Dashlane – a password analysis and protection tool.

Skillbridge

Every Schinnerer Cyber policy holder will be provided access to Skillbridge – a cyber education service provider who can help educate all employees on cyber risk avoidance. Coming Soon

---

PhishMe

- Awesome service that can provide phish tests of employees (lots of fun)
- Support service to report possible phishing emails for their safe analysis

https://cofense.com


Questions?

Your Schinnerer Cyber Team

Jason Bucher
Senior Cyber Underwriter
Phone: (913) 685-6166
jason.bucher@schinnerer.com

Jenn Pangborn
Cyber Underwriter
Phone: (301) 951-5418
Jennifer.Pangborn@schinnerer.com

Mark Schulz
Cyber Underwriter
Phone: (860) 723-5663
Mark.Schulz@schinnerer.com

Zach Atya
Cyber Assistant Account Executive
Phone: (301) 961-9893
Zacharia.Atya@schinnerer.com


VICTOR O.
SCHINNERER
& COMPANY, INC.