

CY2550 Foundations of Cybersecurity

Social Engineering

Alina Oprea

Associate Professor, Khoury College
Northeastern University

Announcements

- Welcome back from Spring break!
 - No pop-up quizzes for the rest of the semester
 - Can schedule online appointments
- Graded midterm and crypto homework
 - Grades and comments released in Gradescope
- Start reading the book: Countdown to Zero Days
 - Finish by March 30
- Next homework will be available today
 - Social engineering and ethics
 - Due on March 23
- Final exam moved to April 13
 - Last class
 - Time: 1 hour, 40 minutes

Focus on the Human

Cybersecurity is not just about computers

People play equally critical roles

- Authentication principals
- Holders of important information
- Operators and maintainers of security critical infrastructure
- Users of security sensitive apps

In many cases, humans are the easiest avenue to compromise



Outline

1. Cognitive vulnerabilities

How do humans function?

How can heuristics lead to cognitive biases?

2. Social engineering tactics

Weaponizing cognitive vulnerabilities

3. Social engineering attacks

Specific attacks with examples

Case studies

Cognitive Vulnerabilities

Psychological Heuristics

Cognitive Biases

Some Examples

Example 1: You are offered either \$100 now, or \$150 in a year.

Which one would you take?

Present bias: value present more

- People undersave for retirement
- Risk tolerance is low

Example 2: if a coin has landed heads up five times in a row, it's more likely to land tails up the sixth time. TRUE or FALSE?

FALSE: odds are equal (Gambler's fallacy)

Cognitive Biases

Subconscious decision making reduces cognitive burden

- Subconscious decisions may be made before you are consciously aware
- Many routine actions are completely automated

Psychological heuristics (shortcuts) can and do go wrong

- Cognitive biases
- We are typically unaware of subconscious biases

Knowledgeable attackers can exploit cognitive biases

Cognitive Biases

Behavioral Biases

Automation bias

Belief bias

Confirmation bias

Courtesy bias

Framing effect

Stereotyping

Social Biases

Authority bias

Halo effect

Ingroup bias

Memory Biases

Context effect

Suggestibility

Behavioral Biases

Belief bias

- Evaluation of an argument is based on the believability of the conclusion

Confirmation bias

- Tendency to search out and interpret information that confirms existing preconceptions

Courtesy bias

- Urge to avoid offending people

Framing effect

- Drawing different conclusions from the same info, based on how it was presented

Stereotyping

- Expecting members of groups to have certain characteristics

Social Biases

Authority bias

- Tendency to believe and be influenced by authority figures, regardless of content

Halo effect

- Tendency for positive personality traits from one area to “spill” into another

Ingroup bias

- Tendency to give preferential treatment to others from your own group

Memory Biases

Context effect

- Cognition and memory are dependent on context

Suggestibility

- Misattributing ideas from the questioner as one's own
- Fill gaps in memory with false information given by somebody else

Social Engineering Techniques

Research

Pretexting

Elicitation and Persuasion

From Vulnerabilities to Attacks

Social engineering

- Psychological manipulation of people into performing actions or divulging confidential information

Techniques are extremely old

- Confidence scams, con-men
- Magicians

Taken on new life in the information age

- Remote attacks let adversaries stay anonymous
- Connectivity makes reaching victims easier
- Networks massively increase the scale of attacks

Social Engineering Basics

Successful attacks rely on:

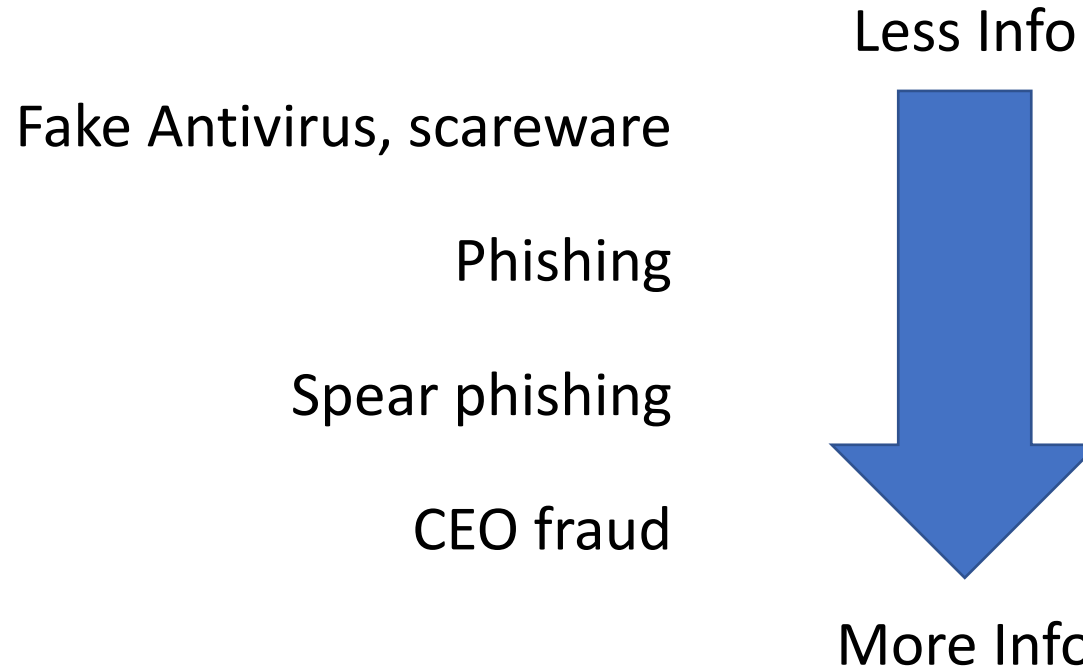
1. Information asymmetry
2. Context construction
3. Elicitation and persuasion

Cognitive biases are leveraged in all three steps



1. Information Asymmetry

Know more about the target than they know about you



Information Resources

Public records

- Mortgage, voter, criminal

Corporate websites

Social networks

- Facebook, LinkedIn, Twitter, Instagram

Background checks

- Spokeo “whitepages”
- Criminal background check
- Credit report



2. Context Construction

Design a frame that advances the attack

- Context effect – triggers social and memory cues in the victim
- Evokes advantageous cognitive vulnerabilities in the victim

Pretexting

- Attacker's "character" and background story
- Opens up cognitive bias attacks
 - Authority bias – "I'm from the internal cybersecurity department..."
 - Halo effect – "Listen to how nice I am. BTW, I need a favor..."
 - Ingroup bias – "You and I are alike, so trust me."
 - Stereotyping – "I'm an intern from marketing, and I forgot my password..."
- May create urgency and place pressure on the victim
 - Increases stress and cognitive load

Kevin On Pretexting

Ingroup bias and stereotyping

Context and framing

Authority bias

“When you use social engineering, or ‘pretexting’, you become an actor playing a role... When you know the lingo and terminology, it established credibility—you’re legit, a coworker slogging in the trenches just like your targets, and they almost never question your authority... People in offices ordinarily give others the benefit of the doubt when the request appears to be authentic. People, as I learned at a very young age, are just too trusting.”

Courtesy bias

Suggestability

Quote from “[Ghost in the Wires](#)” by Kevin Mitnick


Elicitation and Persuasion

Elicitation: The ability to draw people out and make them trust you

- Be polite (courtesy bias)
- Professionals want to appear well informed and intelligent
- People are compelled to reciprocate praise
- People respond kindly to concern
- Most people don't routinely lie

Persuasion: Make the victim take an action or reveal confidential information

- Appeals to ego
- Making deliberate false statements
- Volunteering information (credibility bias)
- Assuming knowledge
- Effective use of questions (suggestibility)
- Quid pro quo: give something to get something in return



More effective when
paired with cognitive biases

- Authority bias
- Belief bias
- Confirmation bias
- Ingroup bias

Follow-through

Suddenly dropping the victim arouses suspicion

- Cutting off contact abruptly
- “Ghosting”

Provide logical follow-through

- Conversations should end normally
- Emails should be answered cordially
- Give the victim normal closure

“Chatting is the kind of extra little friendly touch that leaves people with a good feeling and makes after-the-fact suspicions that much less likely.”

Quote from “[Ghost in the Wires](#)” by Kevin Mitnick

Social Engineering Attacks

Physical Attacks

(Spear) Phishing

Scareware

Attack 1: Baiting

Mr. Robot ;)

Very simple physical attack

1. Preload USB keys with malware
2. Drop the keys in public, near victims
3. Wait for victims to pick up and plug in
4. Victim executes malware
 - Either by accident due to curiosity
 - Or autorun by the OS (e.g. Windows)



Attack 2: Tailgating

Technique used by penetration testers

Goal: break in to a secure facility

- Security guards at the main entrance
- All doors have keycard access control

Idea:

1. Wait for an unsuspecting employee to open a door
2. Follow them inside
3. Leverages courtesy bias and ingroup bias



Attack 3: Phishing

Attempts to coerce sensitive info from targets

Spread via email, SMS, messaging apps

- Careful framing
 - Banks, social networks, webmail
- Leverages urgency
 - “You will lose access to your account!”

Trick the victim into visiting a carefully constructed landing page

- User inputs sensitive info
- Passwords, social security numbers, credit cards, bank accounts, etc.



John Podesta Phishing Email

- Sent by Russian intelligence to Clinton campaign staffers
- Podesta (campaign manager) asked IT if the mail was legit
- IT erroneously responded “this is a legitimate email”
- Account compromised, emails dumped to Wikileaks
- Massive political scandal

> *From:* Google <no-reply@accounts.googlemail.com>

> Date: March 19, 2016 at 4:34:30 AM EDT

> *To:* john.podesta@gmail.com

> *Subject:* *Someone has your password*

>

> Someone has your password

> Hi John

> Someone just used your password to try to sign in to your Google Account

> [REDACTED]@gmail.com.

>

> Details:

> Saturday, 19 March, 8:34:30 UTC

> IP Address: 134.249.139.239

> Location: Ukraine

>

> Google stopped this sign-in attempt. You should change your password

> immediately.

>

> CHANGE PASSWORD <<https://bit.ly/1PibSU0>>

>

> Best,

> The Gmail Team

> You received this mandatory email service announcement to update you about

> important changes to your Google product or account.

>

Attack 4: Spear Phishing

Advanced form of phishing

Highly targeted emails sent to high-value victims

- Includes many details about the target
- Does not trigger spam filters

Very challenging to detect by people and anomaly detectors

- May be sent from hacked, legit email accounts
- Or may use crafted domain names
 - E.g. googlemail.com

Attack 5: CEO Fraud

Specific type of spear phishing

Targets employees with access to corporate bank accounts

- Attacker impersonates the company CEO
- Asks that money be wired to the attacker's bank account

Exploits many cognitive biases

- Context and framing – Uses real names, jargon, and writing style
- Authority bias – orders from the CEO
- Creates a sense of urgency – “payment is late, send right away”

Attacker may follow-up with more emails or calls

- Further increases the sophistication of the attack

13 July 2016 at 9:38 AM

IJ

To: [REDACTED]

Reply-To: [REDACTED]

Payment

Hi Michael,

Please find enclosed vendor banking instructions for a payment that was suppose to go out in the previous week. I need you to process it immediately.

I am a bit busy now but will give you a call within the hour regarding the payment.

Regards,

[REDACTED]

Sent from my Mobile

Urgent



Carla E. Brodley <c.brodley1342@gmail.com>

to cbw ▾

Nov 11, 2018, 8:35 AM



Be careful with this message

Carla E. Brodley has never sent you messages using this email address. Avoid replying to this email unless you reach out to the sender by other means to ensure that this email address is legitimate.

[Report phishing](#)

Looks safe



Are you available?

Clara E. Brodley
Dean - College of Computer and Information Science.
440 Huntington Avenue
202C West Village H
Boston, MA 02115

Attack 6: Advance-fee Scams

Also known as Nigerian prince or 419 scams

- Known as the “Spanish prisoner” confidence trick in the 18th century

Attacker entices the victim with promise of huge financial reward

But, victim must pay a small fee up-front



REQUEST FOR ASSISTANCE-STRICTLY CONFIDENTIAL

I am Dr. Bakare Tunde, the cousin of Nigerian Astronaut, Air Force Major Abacha Tunde. He was the first African in space when he made a secret flight to the Salyut 6 space station in 1979. He was on a later Soviet spaceflight, Soyuz T-16Z to the secret Soviet military space station Salyut 8T in 1989. He was stranded there in 1990 when the Soviet Union was dissolved. His other Soviet crew members returned to earth on the Soyuz T-16Z, but his place was taken up by return cargo. There have been occasional Progrez supply flights to keep him going since that time. He is in good humor, but wants to come home.

In the 14-years since he has been on the station, he has accumulated flight pay and interest amounting to almost \$ 15,000,000 American Dollars. This is held in a trust at the Lagos National Savings and Trust Association. If we can obtain access to this money, we can place a down payment with the Russian Space Authorities for a Soyuz return flight to bring him back to Earth. I am told this will cost \$ 3,000,000 American Dollars. In order to access the his trust fund we need your assistance.

Consequently, my colleagues and I are willing to transfer the total amount to your account or subsequent disbursement, since we as civil servants are prohibited by the Code of Conduct Bureau (Civil Service Laws) from opening and/ or operating foreign accounts in our names.

Needless to say, the trust reposed on you at this juncture is enormous. In return, we have agreed to offer you 20 percent of the transferred sum...

Attack 7: Scareware

Attempts to convince the victim to install malware on their system

Paradoxically, leverages people's fears of security problems

- Virus and malware infections
- Data breaches

Distributed via online ads and compromised websites

Whole fake antivirus industry around these scams

- Scareware companies have real customer support hotlines
- Sometimes the products actually remove malware
 - But only from competing crime gangs ;)





Context and framing:
real security logos
and product names

Urgency: you
are infected!

Familiarity: real-
looking security
dialogs

The screenshot shows a web browser window with the address bar displaying "247tech.help/crt/uk_seg1003/micr_ess". The page features the Microsoft Security Essentials logo on the left, which includes a blue castle icon. The main heading is "WINDOWS VIRUS WARNING!" in large, bold, black letters. Below this, the text reads "Identity Theft and Hacking Possibilities. Contact emergency virus support now." followed by the large orange phone number "0-800-051-3723".

Below the main text, a section titled "The system have found (4) viruses that" is partially visible. It contains a table with two columns: "Threat" and "Alert".

Threat	Alert
	Trojan.FakeAV-Download
	Spyware.BANKER.ID
	Trojan.FakeAV-Download
	Trojan.FakeAV-Download

Below the table, there is a warning icon and the text: "Your personal and financial information is compromised call 0-800-051-3723 to be secured." At the bottom right, the Microsoft logo is visible.

Overlaid on the page is a "Message from webpage" dialog box. It contains a yellow warning icon and the text: "Microsoft Detected Security Error, Due to Suspicious Activity Found On Your Computer. Contact Microsoft Certified Live Technicians 0-800-051-3723 (Toll Free)". An "OK" button is at the bottom right of the dialog box.

Case Study: Phishing

Evaluating emails

Evaluating websites

Does training work?

John Podesta Phishing Email

```
> *From:* Google <no-reply@accounts.googlemail.com>
> *Date:* March 19, 2016 at 4:34:30 AM EDT
> *To:* john.podesta@gmail.com
> *Subject:* *Someone has your password*
>
> Someone has your password
> Hi John
>
> Someone just used your password to try to sign in to your Google Account
> [REDACTED]@gmail.com.
>
> Details:
> Saturday, 19 March, 8:34:30 UTC
> IP Address: 134.249.139.239
> Location: Ukraine
>
> Google stopped this sign-in attempt. You should change your password
> immediately.
>
> CHANGE PASSWORD <https://bit.ly/1PibSU0>
>
> Best,
> The Gmail Team
> You received this mandatory email service announcement to update you about
> important changes to your Google product or account.
>
```

Test Your Skills!

<https://www.phishingbox.com/phishing-test>



Why Do People Fall Prey to Phishing?

Evaluating the veracity of emails is challenging

- Non-spoofed header?
- Security indicators like DKIM and SPF?
- Personalization, e.g. your name?
- Quality of the text?

Evaluating the veracity of a website is challenging

- Realistic domain name?
- SSL/TLS lock icon?
- “Professional” layout and images?
- Quality and quantity of links?

Back

Forward

Reload

Stop

Home


http://www.bankofthewest.com/BOW/home/index.html

Go

Friday, July 29, 2005

中文 Chinese | Locations | En | Contact Us | Search:

BANK OF THE WEST



PERSONAL

SMALL BUSINESS

COMMERCIAL

ABOUT US

Online Banking


[Learn More](#) | [Enroll Online](#)

eTimeBanker® Sign In:

User Name:

Password:

[Forgot Password?](#)



Other Online Services:

Select...

Locations

State:

ZIP code:

CONSUMER ALERT!


Tips on protecting yourself and how to report suspicious activities


[READ MORE »](#)

News Bulletin

June 14, 2005 | BancWest

HOME EQUITY

Get in on the Great Rate Lock-in! [Click here for the key](#) 



Personal Banking

Welcome to your community bank.

First job. Last job. New home. College tuition. We're here to help guide your finances through the challenges of every life stage. Stop by a branch to experience our hallmark service for yourself.

Checking

Savings & CDs

Debit & Credit Cards

Online Banking

Wealth & Trust


Consumer Loans

Private Banking

More ...

Tennis. Beach Games. Rodeo.

Join us for summer fun this week only!



Small Business Banking

Taking care of business. Across town. Around the globe.

As you navigate your business through all its cycles, you're not on your own. We assign a dedicated relationship manager to help you make the right financial choices. Give us a call. We pick up the phone!

Business Checking

Cash Management

Merchant Services

Loans & Lines

SBA Lending

More...

Commercial Banking

Your cornerstone of stability and growth.

Middle-market to multi-national, our corporate

“vv” instead of “w”

38



https://system.confirm.fbsettings-recovery.com/confirmation-sysytem.html



facebook

Not under
facebook.com

login to continue.

Facebook Security

Log In

[Forgot Password?](#) · [Help Center](#)

“Decision Strategies and Susceptibility to Phishing”

- Julie Downs, Mandy Holbrook, and Lorrie Faith Cranor
- 2006
- Interviewed 20 normal people about their strategies for identifying phishing emails

Quilt and dress containing the most frequently used (i.e. terrible) passwords



Methodology

Participants were asked to role play as another person

- Given this fake person's wallet, containing ID, a credit card, a social security card, and a note containing login credentials for Amazon and Paypal
- Told to read this person's mail and respond to them normally

Inbox contents: Eight total messages

- Three phishing
 - Urgent request from "Citibank", link www.citicard.com, actual URL www.citibank-accountonline.com
 - Reset password from "Paypal", link "Click here to activate", actual URL www.payaccount.me.uk
- One 419 scam

Participants

20 total

- 15 females
- Age 18 – 65 (mean 27)
- 50% white, 25% African American, 15% Asian
- 95% used e-commerce sites
- 70% used online banking
- 25% reported being victims of fraud in the past

Email Decision Strategies

Email	Legit?	% Suspicious
Meeting	Real	0%
"Cool Pic"	Real	15%
Amazon	Real	25%
Citibank	Phishing	74%
"Great Article"	Malware	85%
Paypal	Phishing	70%
Amazon	Phishing	47%
"Katrina"	419 Scam	95%

Three identified strategies

1. Is the email personalized and grammatically correct?
 - Somewhat good at identifying malicious email
2. Do I have an account with this business?
 - Not a good strategy
3. Reputable companies send email
 - Extremely naïve

Sensitivity to Phishing Cues

Cue	% Sensitive	Takeaway
Spoofed “from” address	95%	Good – strange email sources are suspicious
Broken image links on the website	80%	Not good – decent phishing pages will look correct
Strange URL	55%	Good – odd spelling or TLDs are indicative of phishing sites
Awareness of HTTPS	35%	Not good – any website, including phishing sites, can use TLS

Interpretation of Security Warnings

Message	Seen?	Proceed	Stop	Depends
Leaving secure site	71%	58%	0%	42%
Insecure form submission	65%	45%	35%	20%
Self-signed certificate	42%	32%	26%	42%
Entering secure site	38%	82%	0%	18%

Overall, people tend to ignore warnings

Participants were often inured

- “I get these warnings on my school website, so I just ignore them”

“Entering secure site” sometimes made people more suspicious!

- The paradox of security

“Why Phishing Works”

- Rachna Dhamija, J. D. Tygar, Marti Hearst
- In ACM CHI 2006
- Similar study: showed 20 websites to 22 participants, asked them to identify phishing sites and explain why they thought so

Methodology

- 20 websites, first 19 in random order
 - 7 legit
 - 9 representative, real phishing sites
 - 3 phishing sites crafted by the researchers
 - Final site: self-signed SSL certificate
- All websites were fully functional

Participants and Overall Results

- 22 participants
 - 45.5% female
 - Age 18—56 (mean 30)
 - 73% had a bachelors degree
 - 50% used Internet Explorer (remember, its 2006)
- Results:
 - The best phishing site fooled 90% of participants
 - Indicators that are designed to signal trustworthiness were not understood (or even noticed) by many participants
 - The indicators of trust presented by the browser are trivial to spoof
- Designing usable security is still a challenge

Sources

- Kevin Mitnick, “Ghost in the Wires: My Adventures as the World’s Most Wanted Hacker”
- Christopher Hadnagy, “Social Engineering: The Art of Human Hacking”
- Cormac Herley, “Why do Nigerian Scammers Say They are from Nigeria?”, WEIS 2012.
- Julie Downs, Mandy Holbrook, and Lorrie Faith Cranor, “Decision Strategies and Susceptibility to Phishing”, CHI 2006.
- Tom Jagatic, Nathaniel Johnson, Markus Jakobsson, and Filippo Menczer, “Social Phishing”, Communications of the ACM 2005.
- Rachna Dhamija, J. D. Tygar, Marti Hearst, “Why Phishing Works”, CHI 2006