Ray-Ban phishing scams occur a lot on Facebook

CS 88S

Phishing, Social Engineering, Various malwares

Week 3

Frank Chen | Spring 2017

Agenda

- *Review last week's material*
- *Phishing & Social Engineering*
- *Various Malwares*
- *Spam Classification: A Machine Learning Approach*
- *Resources + Best Practices*

Announcement

Agenda

- ***Review last week's material***
- *Phishing & Social Engineering*
- *Various Malwares*
- *Spam Classification: A Machine Learning Approach*
- *Resources + Best Practices*

Hack?

Def: Maliciously taking advantage of a system's **CIA paradigms**

Hack?

Def: A slang for innovatively **solving** a problem or making a product.

Hackathon?

Def: Programming competitions where students are encouraged to **build** anything they'd like. From websites to apps to hardware products etc.

Implicit Bias

Def: Bias in judgment and/or behavior that results from subtle **cognitive processes** (e.g., implicit attitudes and implicit stereotypes) that often operate at a level below conscious awareness and without intentional control.

MR. ROBOT

UCLA Vice Chancellor Jerry Kang's
TED talk video:
http://bit.ly/2oaM8Ek

SKYFALL
007

Agenda

- *Review last week's material*
- ***Phishing & Social Engineering***
- *Various Malwares*
- *Spam Classification: A Machine Learning Approach*
- *Resources + Best Practices*

Phishing

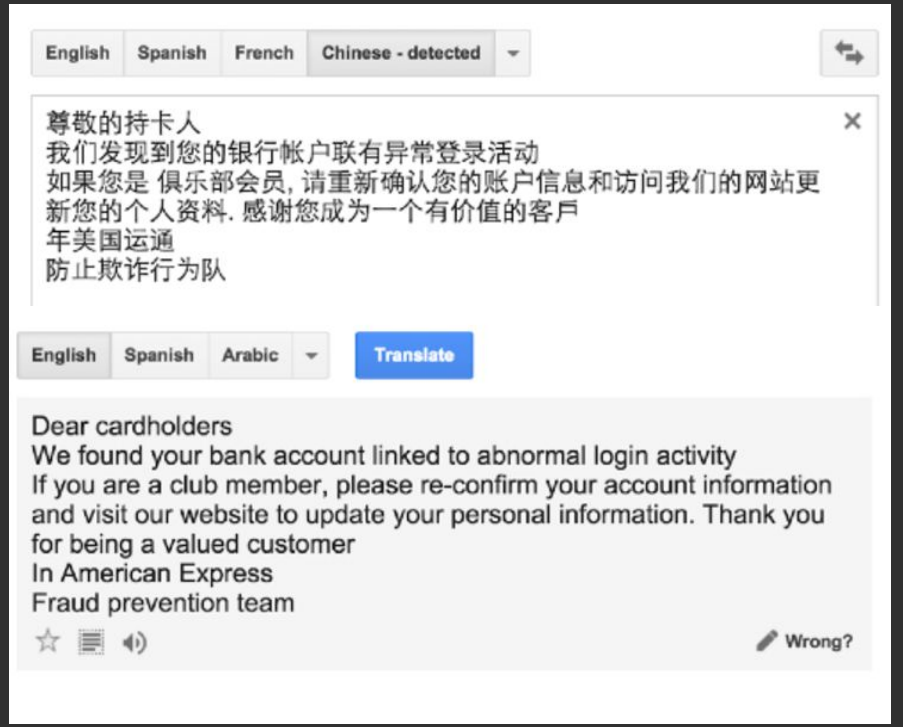
Def: The activity of **defrauding** an online account holder of financial information by posing as a **legitimate company**

An Overview

Source: http://bit.ly/24tI2V0

Spelling

Attackers may not speak English at all.



Source: http://bit.ly/2oCq1Jj

Suspicious Links

Never click on links before checking them properly. Most URL shortener websites give you the option to check a URL.

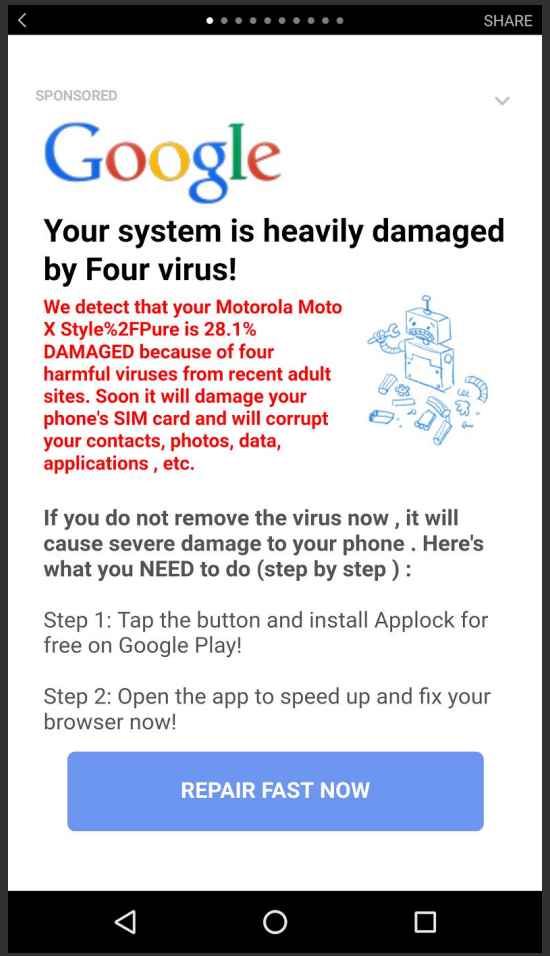
Source: https://techhelpkb.com/how-to-check-shortened-urls-for-safety/

Source: http://unfurlr.com/

Source: https://bitly.com/

Threats

Intended to take advantage of our fear of the unknown



Source: http://bit.ly/2kjyos0

Popular Company or Organization

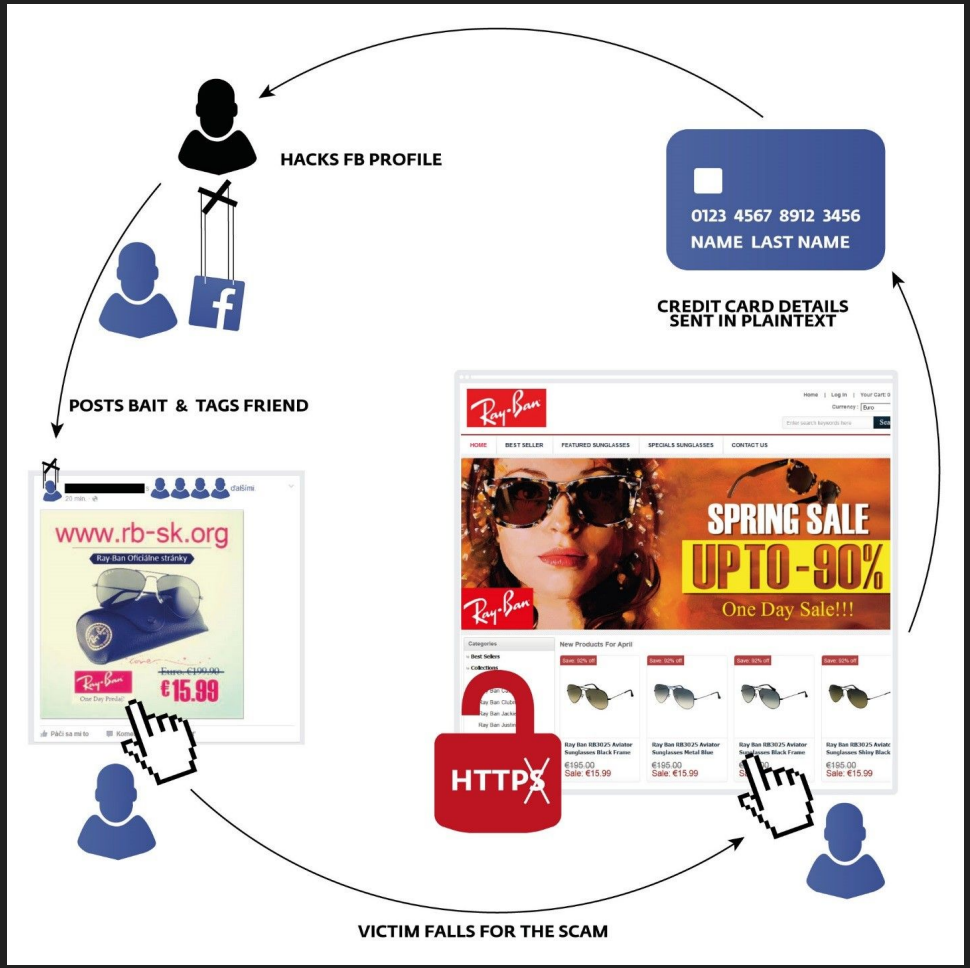
Intended to add credibility to the phish

Source: http://bit.ly/2oiuNbo

Scam websites

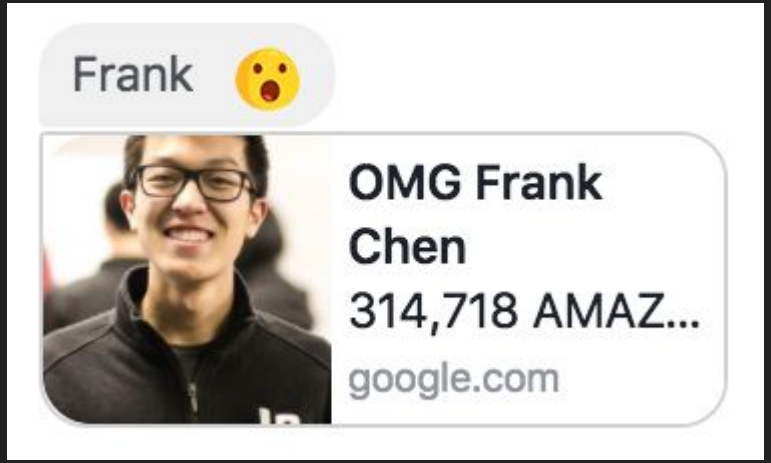
- sk-rb.com
- rb-sk.org
- rbbuy-sk.com
- rayban-sk.com
- rbs-sk.com
- cz-rb.com
- rb-rr.com
- rbstore-no.com
- rb-be.org
- rbeus.co
- rbius.co
- rb-nb.com
- rbsave-fr.com
- salesunglasses07.pw
- rb-ff.com
- rbcet.com
- ok-rb.top
- rbfr-rbs.com
- frrbsrbs.com
- rbese.com
- rb-as.com
- rbs-chile.com
- rayban-brand.com
- spain-rb.com
- rbshop-il.com
- ukrb-uk.com
- esnrb.com
- vt-rbs.com
- rbbuy-se.com
- rbstoreonline.org
- glasses-sale.com
- rb-cz.com
- rb-sk.com
- rbbuy-se.com
- rbnes.com
- 2015goodsunglasses.com

Phishing via Facebook



Source: http://bit.ly/2oiuNbo

Phishing via Google Translate

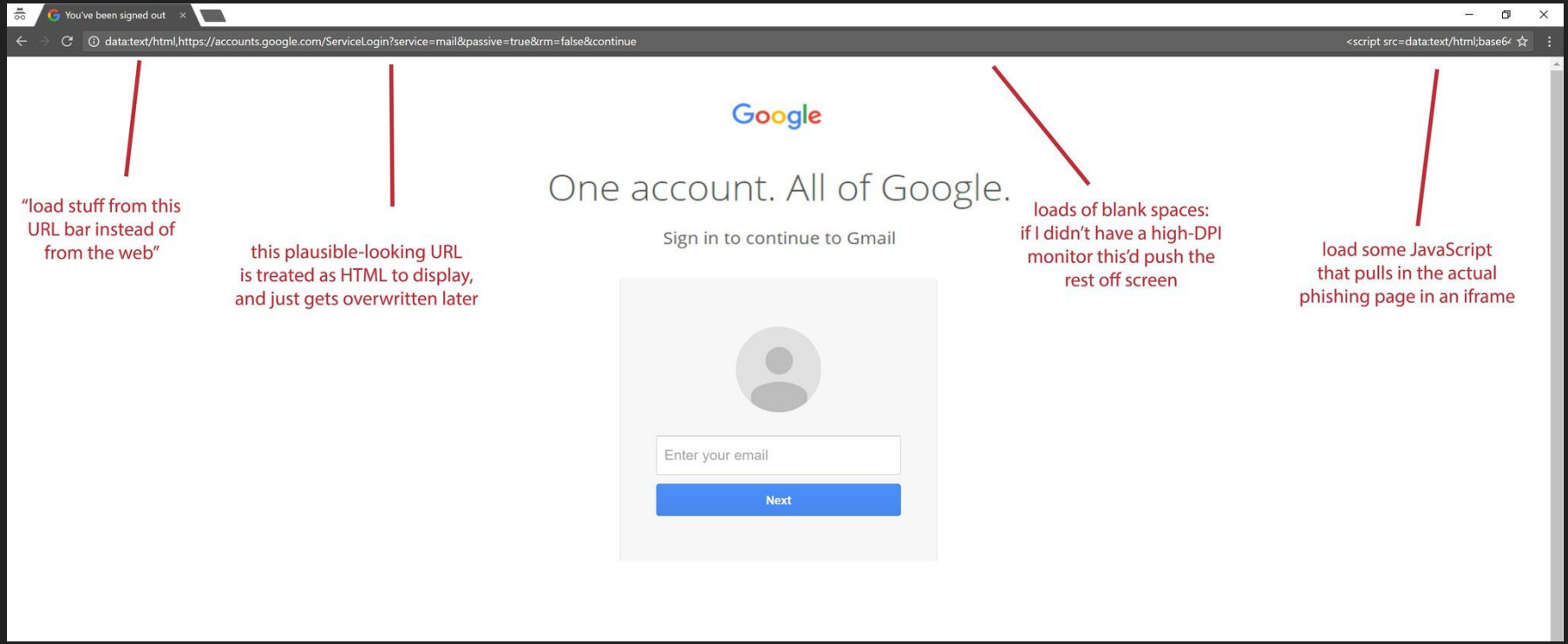


https://l.facebook.com/l.php?u=http%3A%2F%2Ftranslate.google.com%2Ftranslate%3Fsl%3Den%26tl%3Dde%26u%3Dhttp%253A%252F%252Fyjtdydjyc.es.tl%252F%253F0706155&h=ATP-krBIeekxAKsByfeNch_ZDF70pcQHGSWJdO3V40F_2ZZXQQTCwnH6YwGn8qHIwPq69ICvchuDq82FdPjgV2M7PiciBXVtpxmRiL9Lj52OhFuEh2rJsEc8ijG6LrJjHXJhVlWNphA&s=1

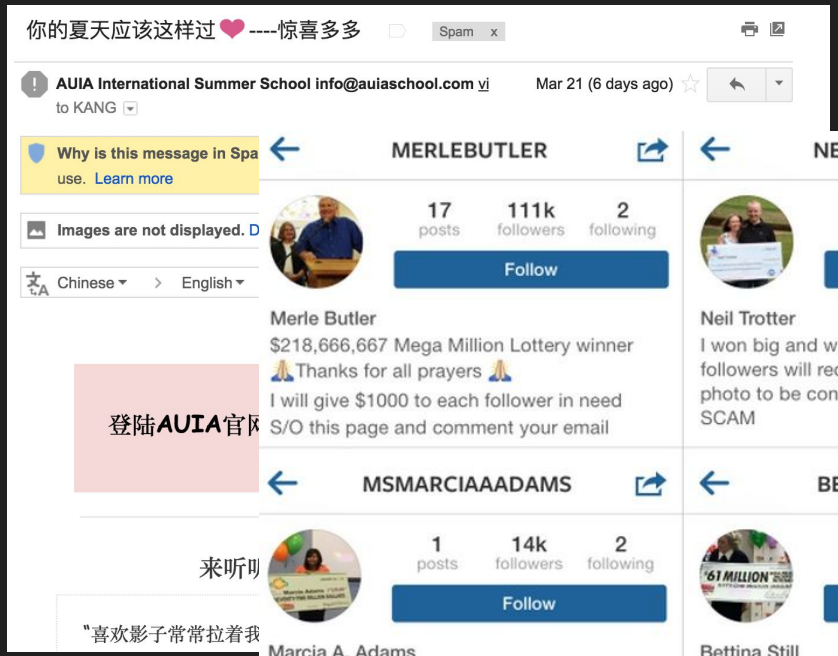
Source: http://bit.ly/2nYXZIp

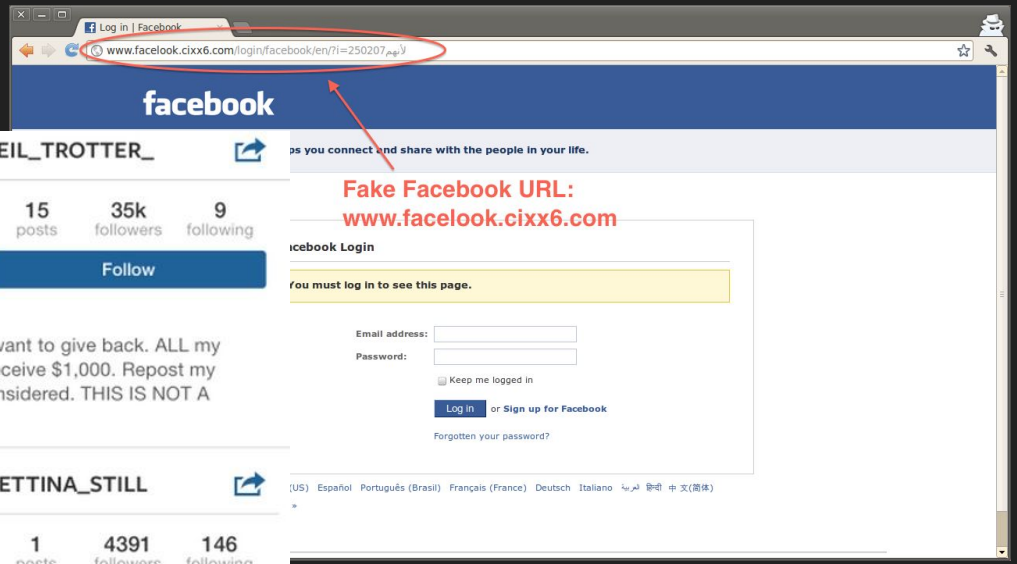
Phishing via Gmail

A CLoser Look



More Examples



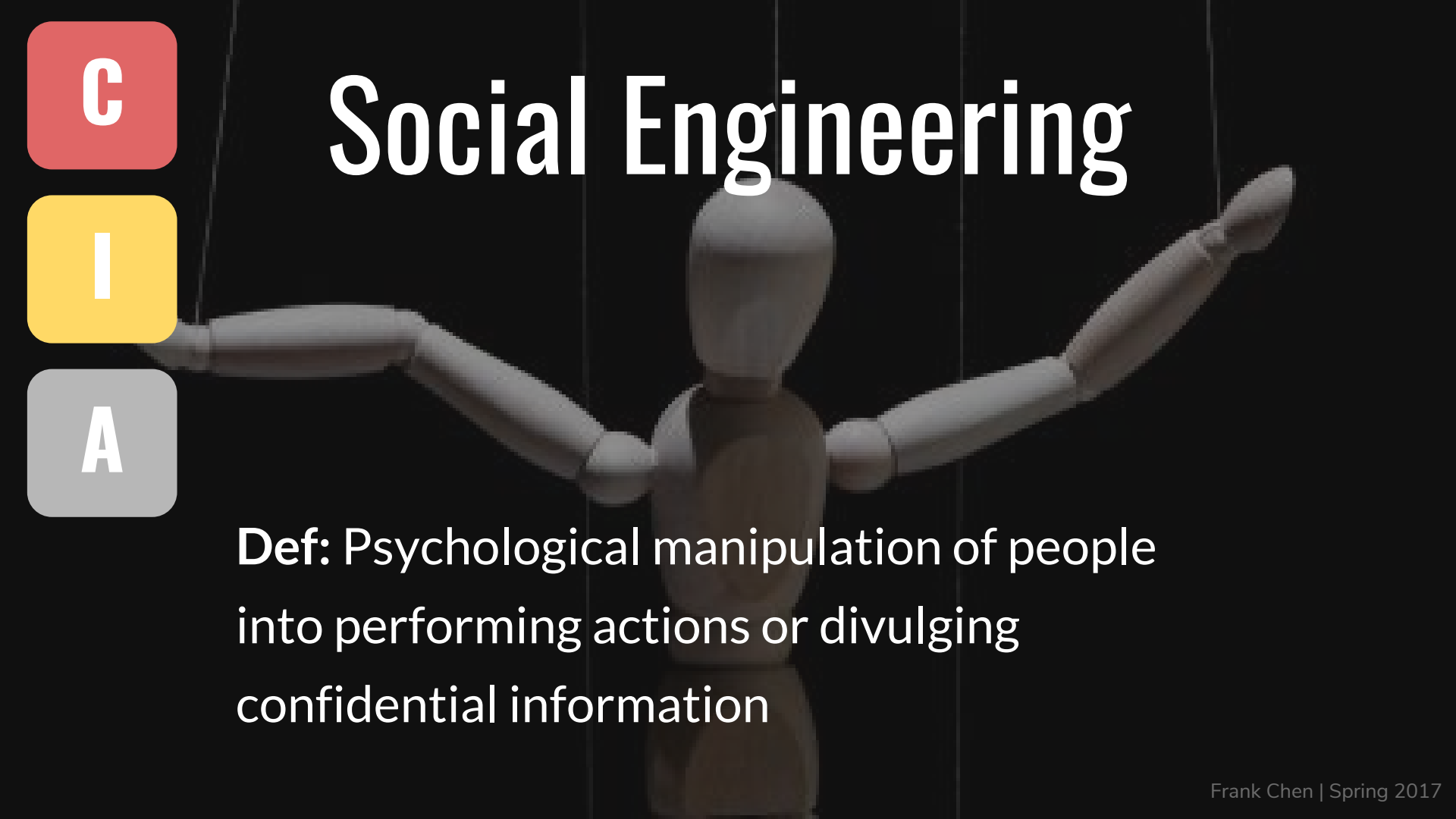


C

I

A

Social Engineering



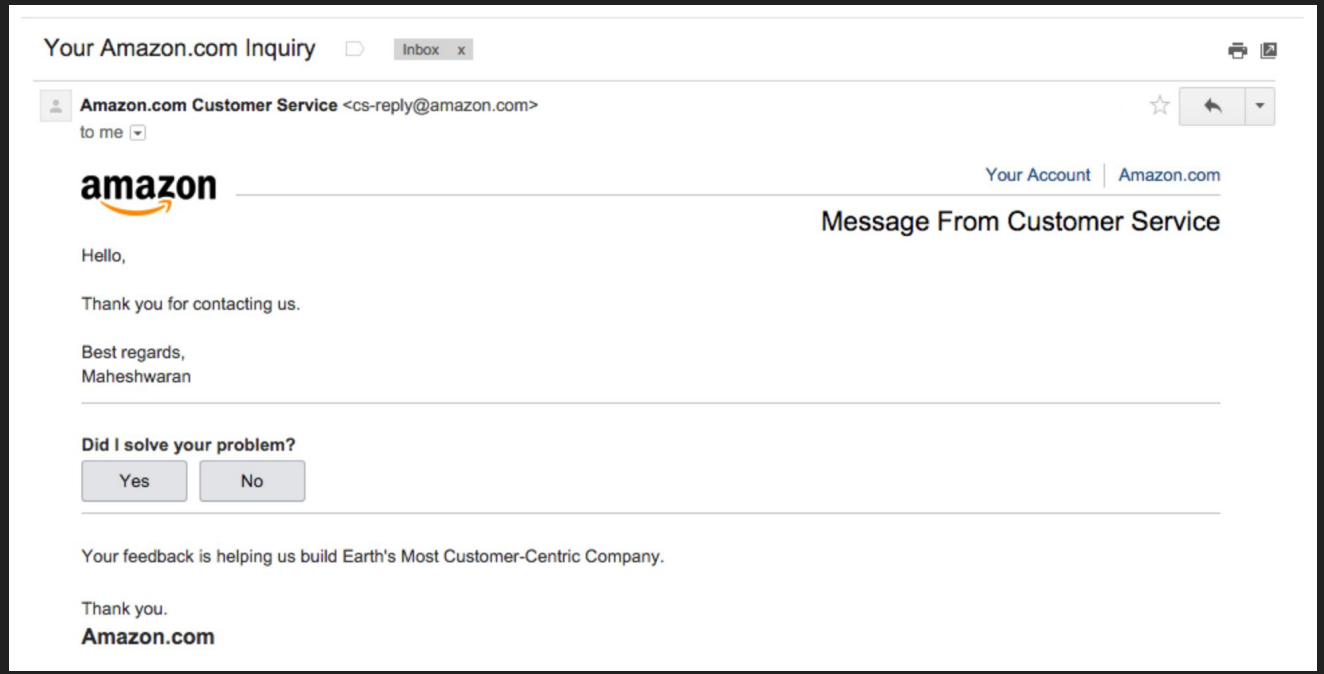
Def: Psychological manipulation of people into performing actions or divulging confidential information

Amazon Customer Service "Backdoor"

Def: A backdoor is a method, often secret, of bypassing normal authentication in a secure system.

Source: `http://bit.ly/2gHurHF`

Amazon Customer Service "Backdoor"



Your Amazon.com Inquiry Inbox x

Amazon.com Customer Service <cs-reply@amazon.com>
to me

amazon

Your Account | Amazon.com

Message From Customer Service

Hello,

Thank you for contacting us.

Best regards,
Maheshwaran

Did I solve your problem?

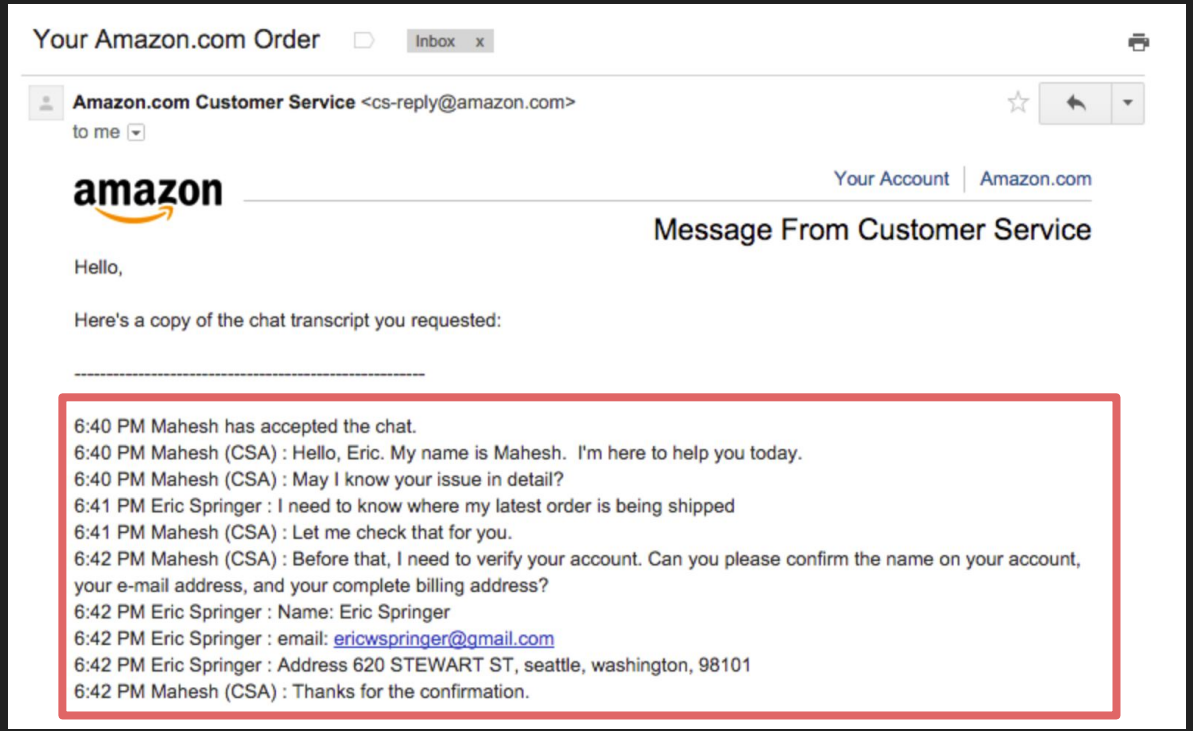
Yes No

Your feedback is helping us build Earth's Most Customer-Centric Company.

Thank you.
Amazon.com

Source: http://bit.ly/2gHurHF

Amazon Customer Service "Backdoor"



Your Amazon.com Order Inbox x

Amazon.com Customer Service <cs-reply@amazon.com>
to me

amazon

Your Account | Amazon.com

Message From Customer Service

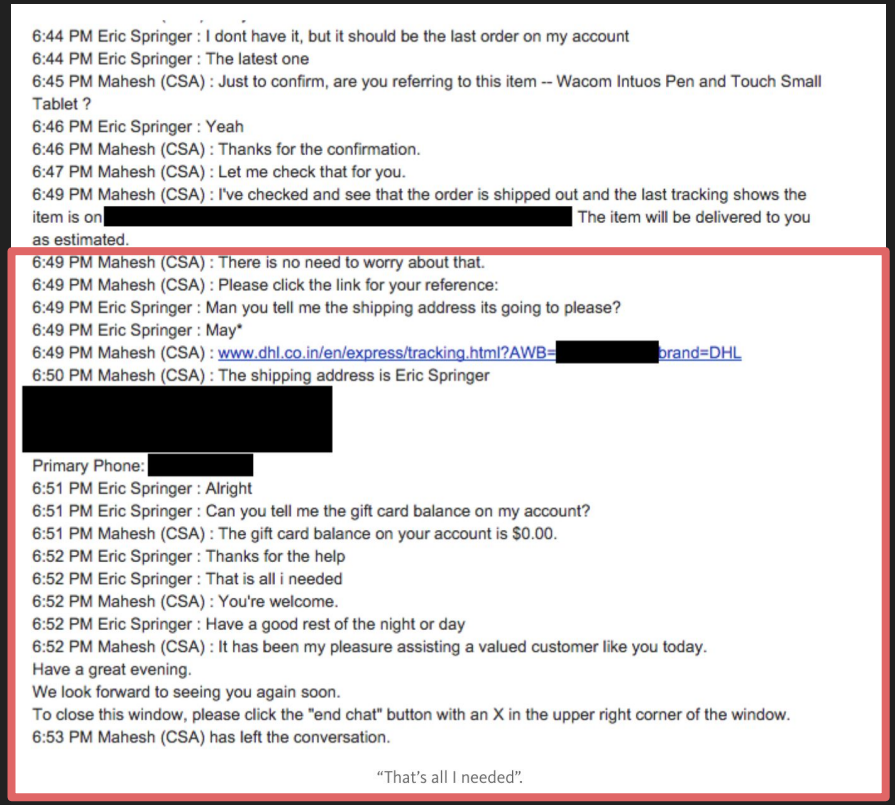
Hello,

Here's a copy of the chat transcript you requested:

6:40 PM Mahesh has accepted the chat.
6:40 PM Mahesh (CSA) : Hello, Eric. My name is Mahesh. I'm here to help you today.
6:40 PM Mahesh (CSA) : May I know your issue in detail?
6:41 PM Eric Springer : I need to know where my latest order is being shipped
6:41 PM Mahesh (CSA) : Let me check that for you.
6:42 PM Mahesh (CSA) : Before that, I need to verify your account. Can you please confirm the name on your account, your e-mail address, and your complete billing address?
6:42 PM Eric Springer : Name: Eric Springer
6:42 PM Eric Springer : email: ericwspringer@gmail.com
6:42 PM Eric Springer : Address 620 STEWART ST, seattle, washington, 98101
6:42 PM Mahesh (CSA) : Thanks for the confirmation.

Source: http://bit.ly/2gHurHF

Amazon Customer Service "Backdoor"



6:44 PM Eric Springer : I dont have it, but it should be the last order on my account
6:44 PM Eric Springer : The latest one
6:45 PM Mahesh (CSA) : Just to confirm, are you referring to this item -- Wacom Intuos Pen and Touch Small Tablet ?
6:46 PM Eric Springer : Yeah
6:46 PM Mahesh (CSA) : Thanks for the confirmation.
6:47 PM Mahesh (CSA) : Let me check that for you.
6:49 PM Mahesh (CSA) : I've checked and see that the order is shipped out and the last tracking shows the item is on [redacted] The item will be delivered to you as estimated.
6:49 PM Mahesh (CSA) : There is no need to worry about that.
6:49 PM Mahesh (CSA) : Please click the link for your reference:
6:49 PM Eric Springer : Man you tell me the shipping address its going to please?
6:49 PM Eric Springer : May*
6:49 PM Mahesh (CSA) : www.dhl.co.in/en/express/tracking.html?AWB=[redacted]brand=DHL
6:50 PM Mahesh (CSA) : The shipping address is Eric Springer
[redacted]
Primary Phone: [redacted]
6:51 PM Eric Springer : Alright
6:51 PM Eric Springer : Can you tell me the gift card balance on my account?
6:51 PM Mahesh (CSA) : The gift card balance on your account is $0.00.
6:52 PM Eric Springer : Thanks for the help
6:52 PM Eric Springer : That is all i needed
6:52 PM Mahesh (CSA) : You're welcome.
6:52 PM Eric Springer : Have a good rest of the night or day
6:52 PM Mahesh (CSA) : It has been my pleasure assisting a valued customer like you today.
Have a great evening.
We look forward to seeing you again soon.
To close this window, please click the "end chat" button with an X in the upper right corner of the window.
6:53 PM Mahesh (CSA) has left the conversation.

"That's all I needed".

Source: http://bit.ly/2gHurHF

A semi-realistic example

Agenda

- *Review last week's material*
- *Phishing & Social Engineering*
- ***Various Malwares***
- *Spam Classification: A Machine Learning Approach*
- *Resources + Best Practices*

Malware

Def: Malware is short for **malicious software**, meaning software that can be used to compromise CIA principles of a system.

Malware is a broad term that refers to a variety of malicious programs.

****Note:** Advanced understanding of how these malware works is out of the scope for this class, but the relevant readings are provided as resources.

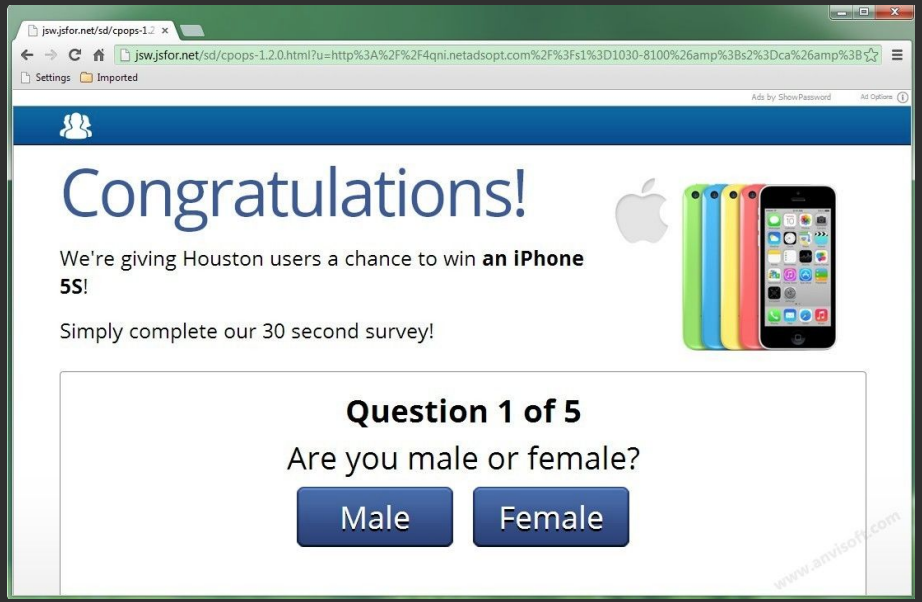
C

I

A

Adware

Adware (short for advertising-supported software) is a type of malware that automatically delivers advertisements.



Source: http://symc.ly/2pkTubZ

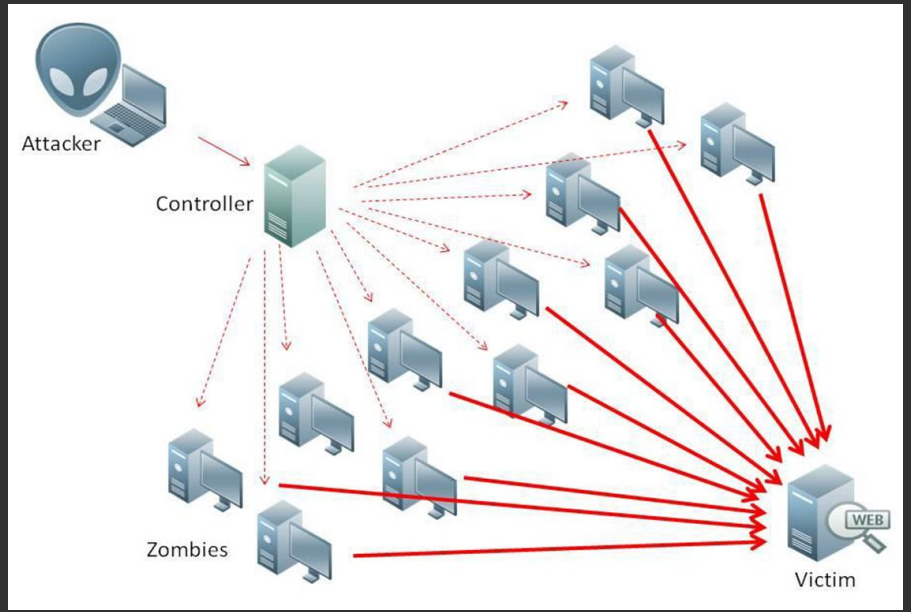
C

I

A

Bot

Bots are software programs created to automatically perform specific operations.



Source: http://symc.ly/2pkOp3q

C

I

A

Ransomware

Ransomware is a form of malware that essentially holds a computer system captive while demanding a ransom.

Source: http://symc.ly/2oMbU4t

C

I

A

Rootkit

A rootkit is a type of malicious software designed to remotely access or control a computer without being detected by users or security programs.

Source: https://www.avast.com/c-rootkit

C

I

A

Spyware

Spyware is a type of malware that functions by spying on user activity without their knowledge. These spying capabilities can include activity monitoring, collecting keystrokes, data harvesting

Source: http://bit.ly/2mZDefB

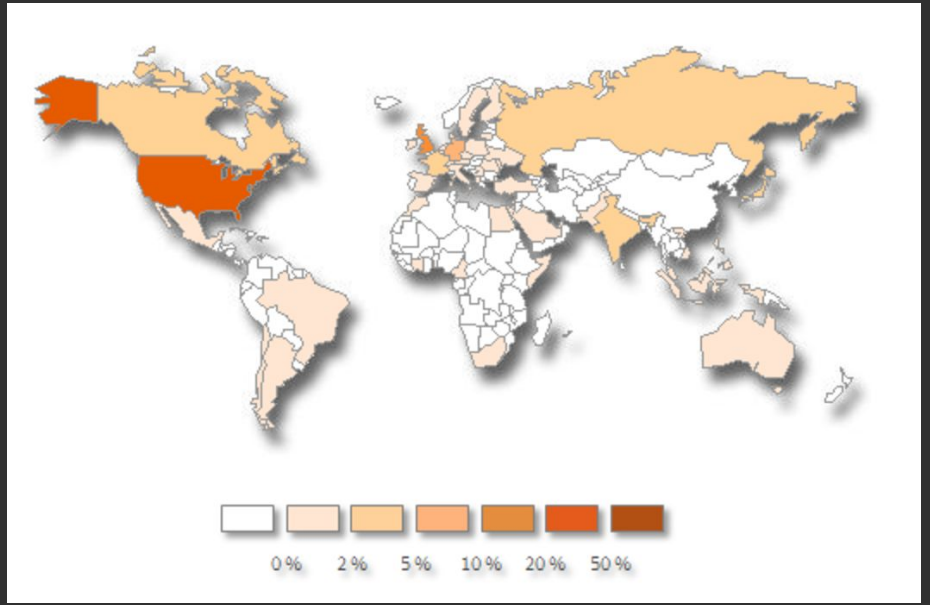
C

I

A

Trojan Horse

A Trojan horse, commonly known as a “Trojan,” is a type of malware that disguises itself as a normal file or program to trick users into downloading and installing malware.
(Right: Impact of Zeus Trojan Horse worldwide)



Source: http://symc.ly/2joUzZG

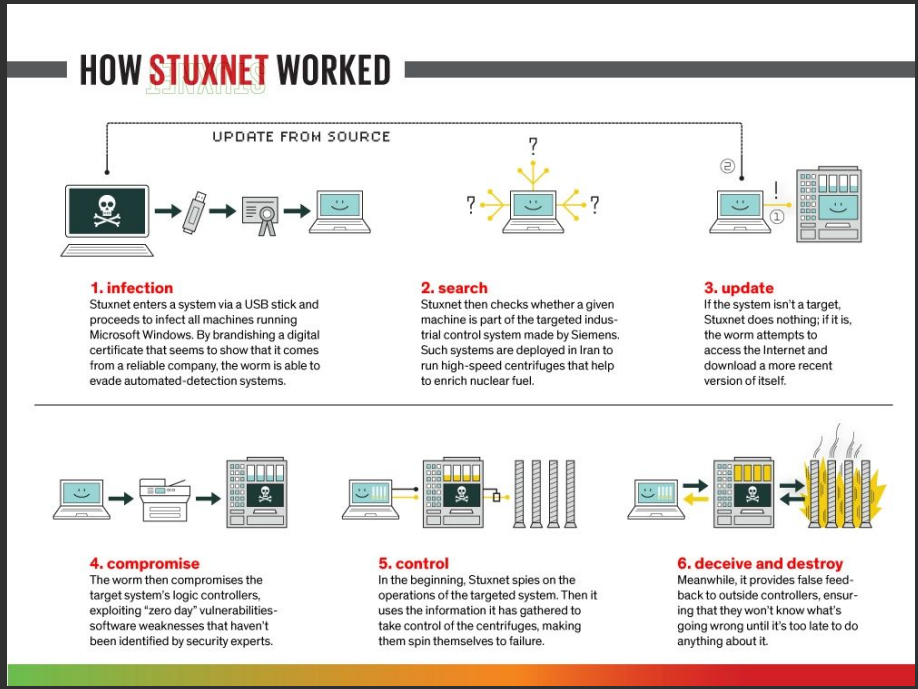
C

I

A

Virus

A virus is a form of malware that is capable of copying itself and spreading to other computers.



Source: http://symc.ly/2pkOp3q

C

I

A

Worm

They spread over computer networks by exploiting operating system vulnerabilities.Worms typically cause harm to their host networks by consuming bandwidth and overloading web servers.

Source: http://bit.ly/2p6Mz6h

Agenda

- *Review last week's material*
- *Phishing & Social Engineering*
- *Various Malwares*
- ***Spam Classification: A Machine Learning Approach***
- *Resources + Best Practices*

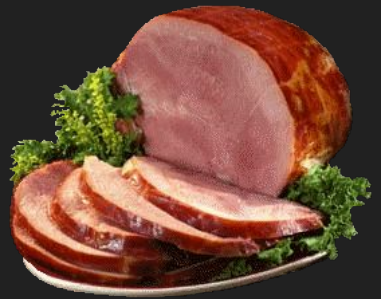
Spam/Ham

 143 Million Americans...they didn't expect this at all...
<link to strange website URL:
http://difirtyuio.ga/neyJjIjogNzM1NjAsICJmIjogMCwgIm0iOiA2Mzk3MCwgImwiOiA2NCwgInMiOiAwLCAidSI6IDIzNTYzMTQwMywgInQiOiAxLCAic2QiOiAyMH0=>

Dear Frank,

Do you have 10 minutes to meet tomorrow about
my roommate conflict situation?

Thanks,
Bob

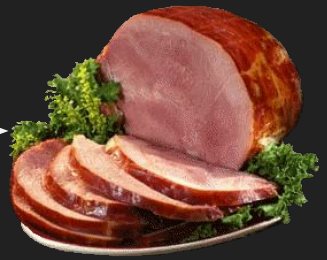


*Slide content credit to Prof. Ameet Talwalkar

Strategy: Count the Words

free	...	100
money	...	10
.		.
.		.
.		.
account	...	2

free	...	1
money	...	1
.		.
.		.
.		.
account	...	2



*Slide content credit to Prof. Ameet Talwalkar

Train a Classifier Model

Email labeled as 'ham'

Email labeled as 'spam'

Our "Magical" Classifier Model

*Slide content credit to Prof. Ameet Talwalkar

How to train the Classifier Model

Given: Training Data Ɗ

Goal: Learn some parameters π, θ under some constraints.

*Slide content credit to Prof. Ameet Talwalkar

Solve: Constrained Optimization

Out of scope for this class!

For more information on the math formulations behind Bayes Optimal Classifier and Constrained Optimization using Lagrange Multipliers, check out Prof. Talwalkar's slides on Logistic Regression.

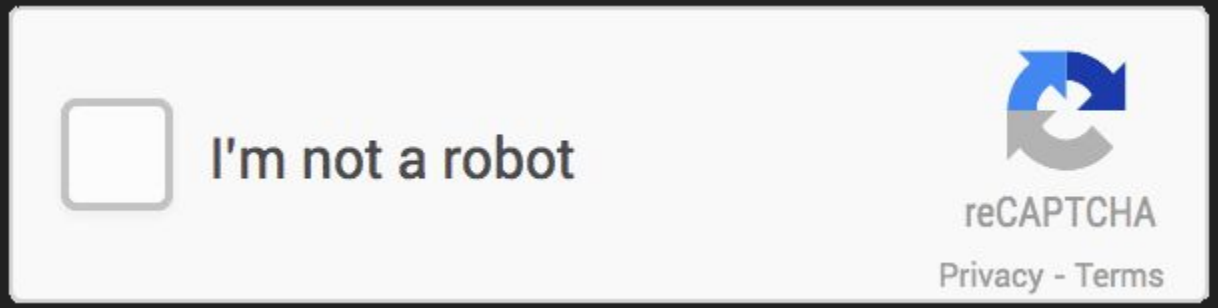
`http://web.cs.ucla.edu/~ameet/teaching/winter17/cs260/lectures/lec05.pdf`

*Slide content credit to Prof. Ameet Talwalkar

Use model to make prediction

*Slide content credit to Prof. Ameet Talwalkar

Google ReCaptcha



- *Cursor Movement in the x and y-axis*
- *Prior Behavior*
- *Click Location History*

For more information, visit Google's Security Blog: `http://bit.ly/2fUMY2G`

Agenda

- *Review last week's material*
- *Phishing, Social Engineering, Identity Theft*
- *Extended Examples*
- *Spam Classification: A Machine Learning Approach*
- ***Resources + Best Practices***

Anti-Virus Software

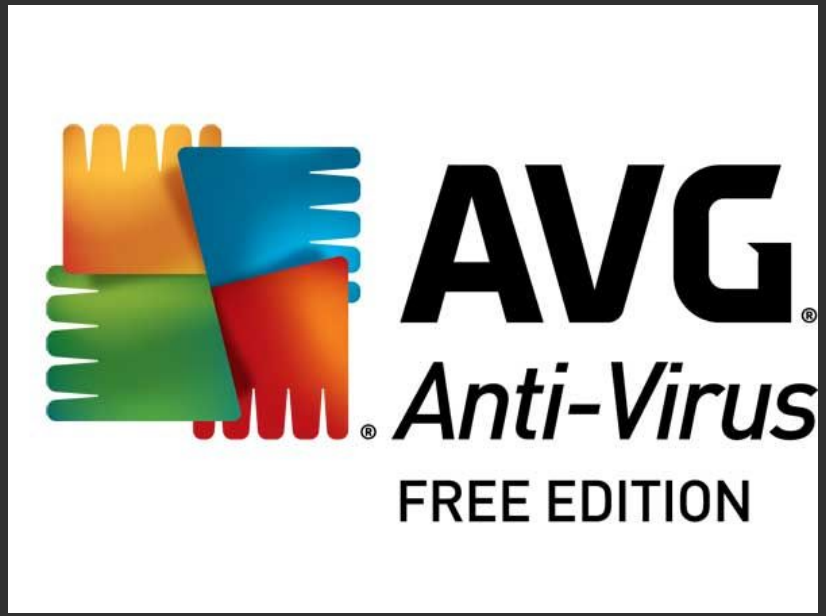
Def: computer software used to **prevent, detect** and **remove** malicious software.

Avast

As of 2015, Avast is the most popular antivirus on the market, and it had the largest share of the market for antivirus applications. Avast has both desktop and mobile applications.

AVG

A family of antivirus and Internet security software developed by AVG Technologies, a subsidiary of Avast Software.



MalwareBytes

Primarily a scanner that scans and removes malicious software, including rogue security software, adware, and spyware

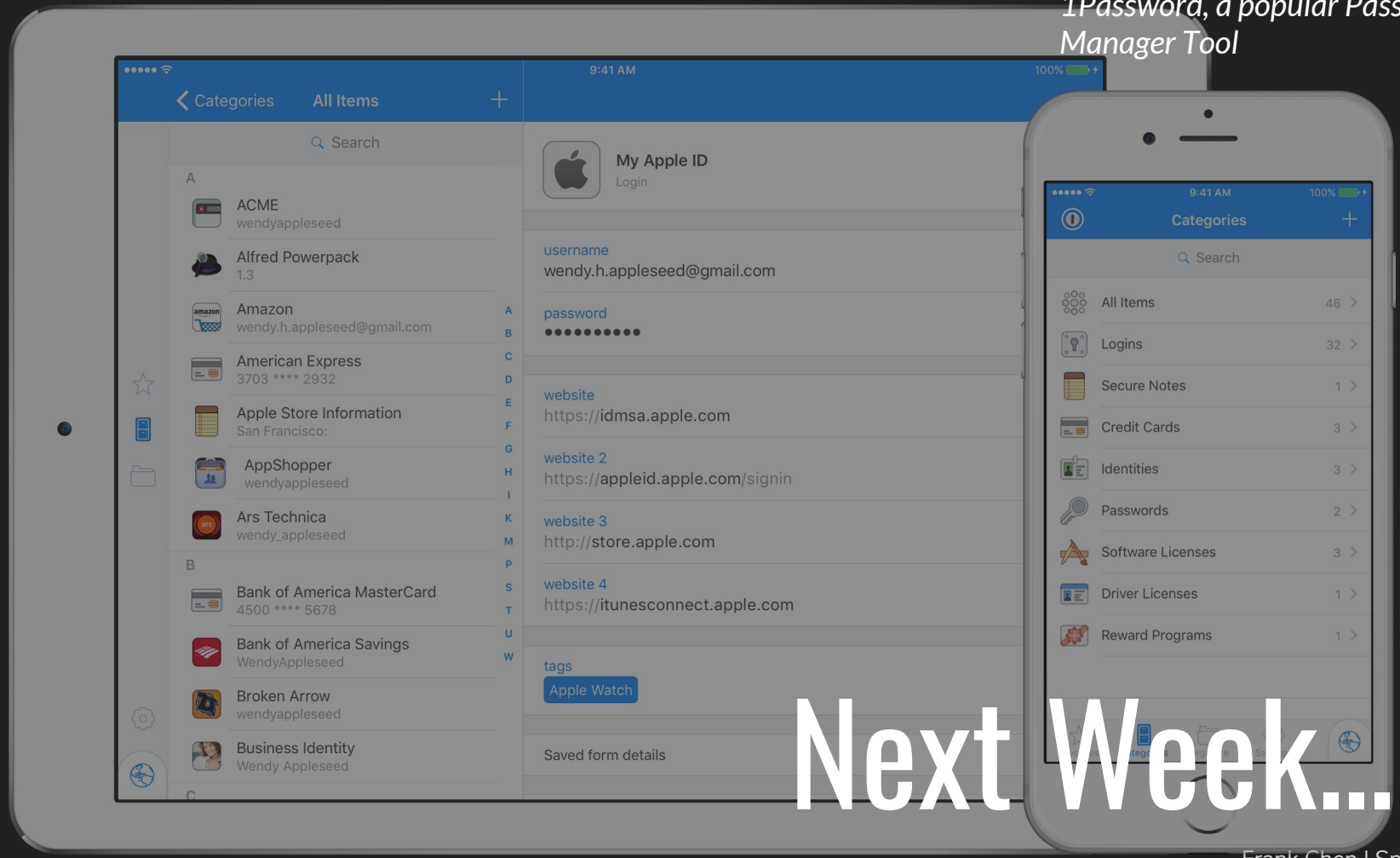
Safety in the Cloud Tip

Have an Anti-Virus Software **Installed**!

Homework! (not really)

- *Install Anti-Virus Software on your:*
  - *Laptop*
  - *Smartphone*
  - *Any other devices*
- *Be part of PhishTank! Sign up @: `https://www.phishtank.com/`*

1Password, a popular Password Manager Tool



Next Week...