

CS 88S

Phishing, Social Engineering, Various malwares

Week 3

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*

A photograph of a man wearing a dark grey balaclava, sitting on the grass and looking at a laptop screen. The laptop screen displays a large black skull icon. In the background, a white hatchback car is parked on a grassy area with trees in the distance. A small American flag is visible in the top right corner.

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*

C

I

A

Phishing

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

An Overview

Hello!

As part of our security measures, we regularly screen activity in the Facebook system. We recently contacted you after noticing an issue on your account.

Spelling

Our system detected unusual Copyrights activity linked to your Facebook account, please follow the link below to fill the Copyright Law form:

http://www.facebook.com/application_form

Links in email

Note: If you dont fill the application your account will be permanently blocked.

Threats

Regards,

Facebook Copyrights Department.

Popular company

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

Frank Chen | Spring 2017

Spelling

Attackers may not speak English at all.



English Spanish French Chinese - detected

尊敬的持卡人
我们发现到您的银行帐户联有异常登录活动
如果您是 俱乐部会员, 请重新确认您的账户信息和访问我们的网站更新您的个人资料. 感谢您成为一个有价值的客户
年美国运通
防止欺诈行为队

English Spanish Arabic Translate

Dear cardholders
We found your bank account linked to abnormal login activity
If you are a club member, please re-confirm your account information and visit our website to update your personal information. Thank you for being a valued customer
In American Express
Fraud prevention team

☆ ⌂ ⓘ Wrong?

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

SPONSORED

Google

Your system is heavily damaged by Four virus!

We detect that your Motorola Moto X Style%2FPure is 28.1% DAMAGED because of four harmful viruses from recent adult sites. Soon it will damage your phone's SIM card and will corrupt your contacts, photos, data, applications , etc.



If you do not remove the virus now , it will cause severe damage to your phone . Here's what you NEED to do (step by step) :

Step 1: Tap the button and install Applock for free on Google Play!

Step 2: Open the app to speed up and fix your browser now!

REPAIR FAST NOW

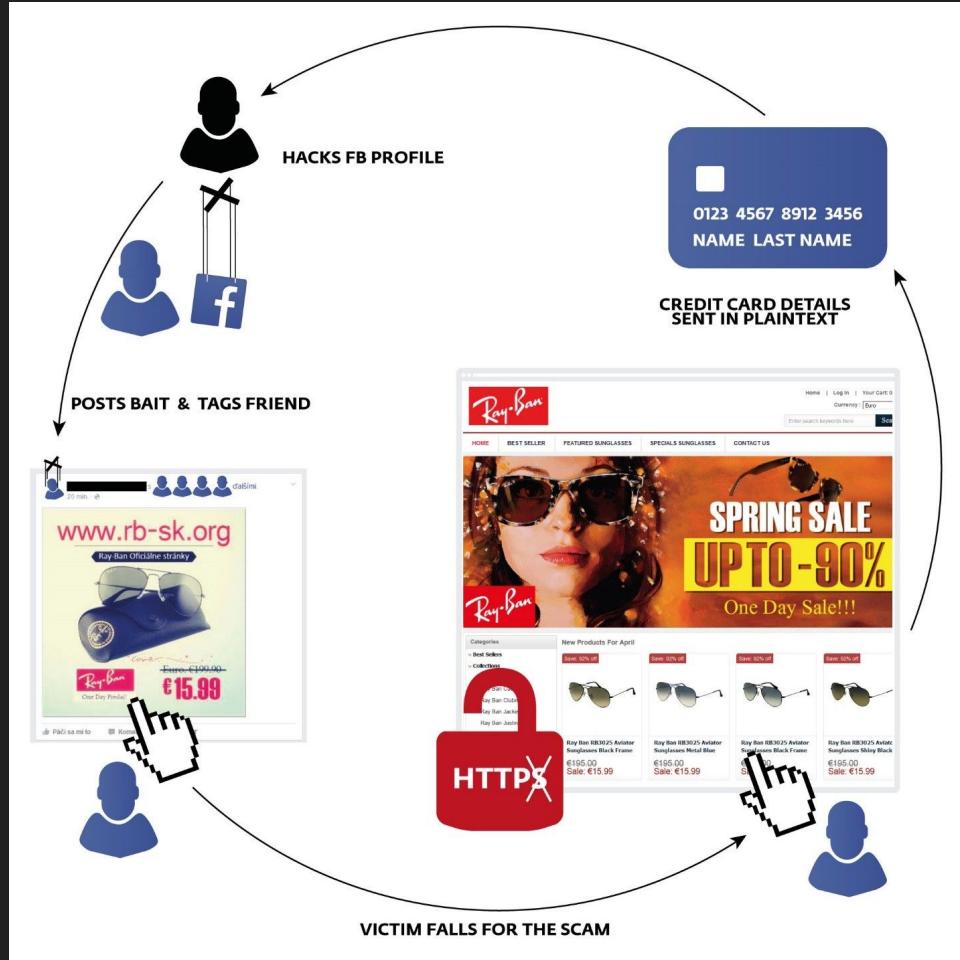
Popular Company or Organization

Intended to add credibility to the phish

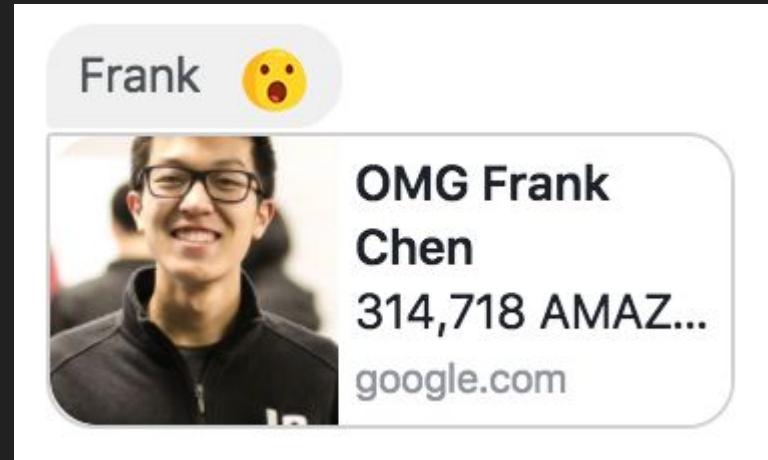
Scam websites

- 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



Phishing via Google Translate



https://l.facebook.com/l.php?u=http%3A%2F%2Ftranslate.google.com%2Ftranslate%3Fst%3Den%26tl%3Dde%26u%3Dhttp%253A%252F%252Fyjtdydjyc.es.tl%252F%253F0706155&h=ATP-krBIeekxAKsByfeNch_ZDF70pcQHGSWJdO3V40F_2ZZXQTCwnH6YwGn8qHIwPq69ICvchuDq82FdPjgV2M7PicibXVtpxmRiL9Lj520hFuEh2rJsEc8ijG6LrJjHXJhV1WNphA&s=1

Phishing via Gmail

This is the closest I've ever come to falling for a Gmail phishing attack. If it hadn't been for my high-DPI screen making the image fuzzy...

Back Archive Spam Delete Move to Labels More

plausible subject line Inbox x

to bcc: me email signature

PDF INVOICE-DEC287E.pdf
100 KB

not an attachment;
an embedded image
that links out to a fake
"sign in with Google" page

RETWEETS 6,787 LIKES 5,857

3:54 AM - 23 Dec 2016

A Closer Look

The screenshot shows a Google account sign-in page with several red annotations:

- A vertical line points to the URL bar: "load stuff from this URL bar instead of from the web"
- A vertical line points to the URL itself: "this plausible-looking URL is treated as HTML to display, and just gets overwritten later"
- A diagonal line points to the page content area: "loads of blank spaces: if I didn't have a high-DPI monitor this'd push the rest off screen"
- A vertical line points to the right edge of the page: "load some JavaScript that pulls in the actual phishing page in an iframe"

You've been signed out

data:text/html,https://accounts.google.com/ServiceLogin?service=mail&passive=true&rm=false&continue

<script src=data:text/html;base64

Google

One account. All of Google.

Sign in to continue to Gmail

Enter your email

Next

More Examples

你的夏天应该这样过 ❤ ----惊喜多多

Spam x

AUIA International Summer School info@auiaschool.com vi Mar 21 (6 days ago) to KANG

Why is this message in Spam? Learn more

Images are not displayed.

Chinese English

Merle Butler 17 posts 111k followers 2 following Follow

Neil Trotter 15 posts 35k followers 9 following Follow

登陆AUIA官网

来听明

喜欢影子常常拉着我

Marcia A. Adams 1 posts 14k followers 2 following Follow

Bettina Still 1 posts 4391 followers 146 following Follow

Log in | Facebook www.facebook.cixx6.com/login/facebook/en/?i=250207_&fj=

Facebook Login

You must log in to see this page.

Email address:

Password:

Keep me logged in

Log In or Sign up for Facebook

Forgotten your password?

(US) Español Português (Brasil) Français (France) Deutsch Italiano हिन्दी 中文(简体)

Fake Facebook URL: www.facebook.cixx6.com

Frank Chen | Spring 2017

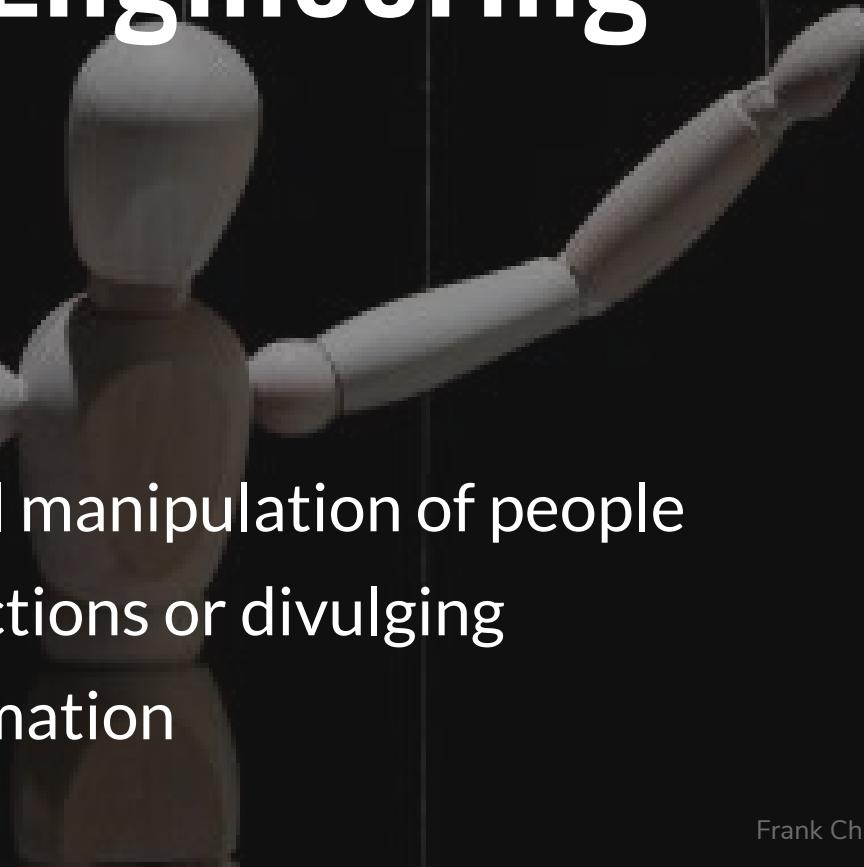
C

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>

Frank Chen | Spring 2017

Amazon Customer Service "Backdoor"

Your Amazon.com Inquiry

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

Hello,

Thank you for contacting us.

Best regards,
Maheshwaran

Message From Customer Service

Did I solve your problem?

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

Thank you.
Amazon.com

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

Frank Chen | Spring 2017

Amazon Customer Service "Backdoor"

The screenshot shows an email from Amazon Customer Service to the user. The subject is "Message From Customer Service". The email body contains a transcript of a chat between Eric Springer and Mahesh (CSA). A red box highlights the transcript text.

Your Amazon.com Order □ Inbox x

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

amazon Your Account | Amazon.com

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>

Frank Chen | Spring 2017

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](http://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>

Frank Chen | Spring 2017

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.

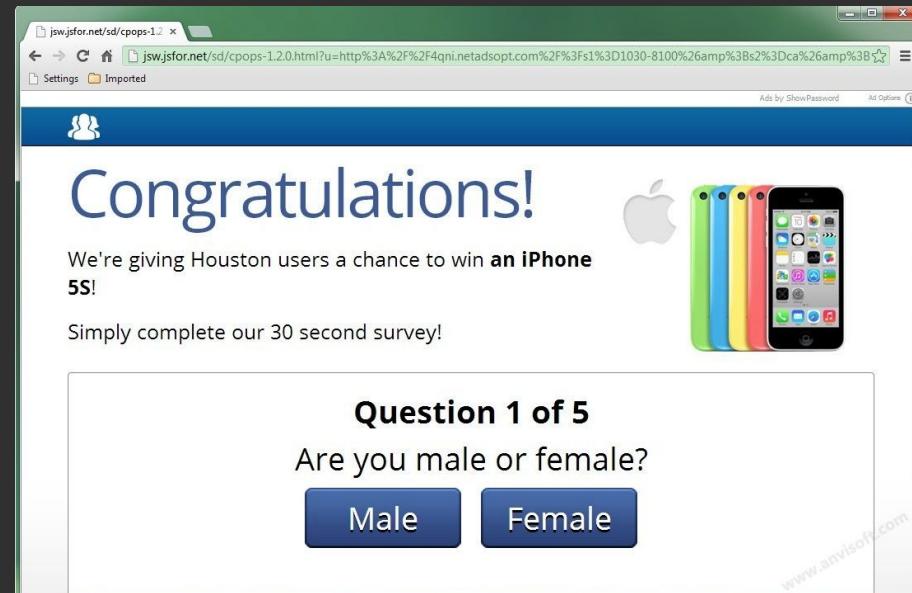
C

I

A

Adware

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



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

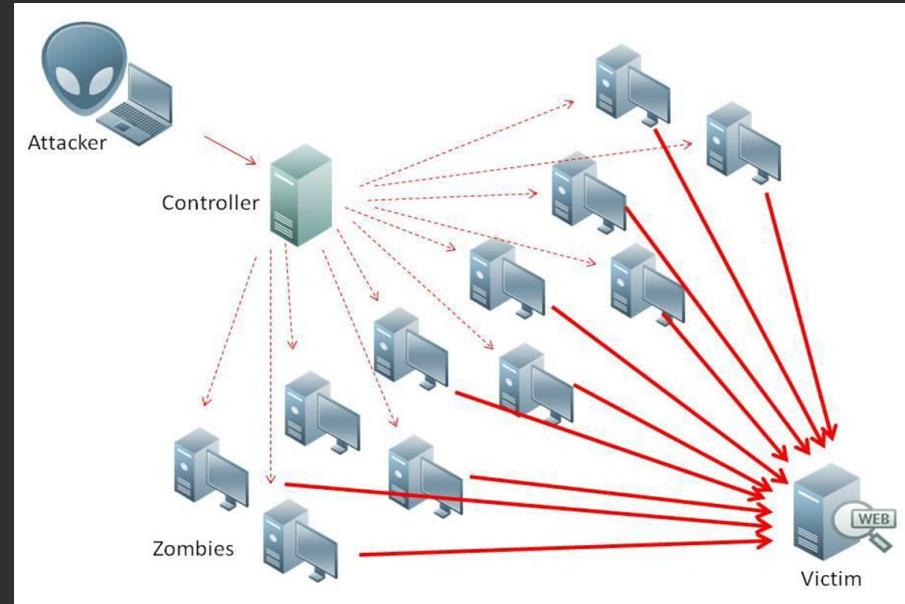
C

I

A

Bot

Bots are software programs created to automatically perform specific operations.



Source: <http://symc.ly/2pk0p3q>

C

I

A

Ransomware

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

YOUR COMPUTER HAS BEEN LOCKED!

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)

Following violations were detected:

Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.

This computer lock is aimed to stop your illegal activity.

To unlock the computer you are obliged to pay a fine of \$200.

You have 72 hours to pay the fine, otherwise you will be arrested.

You must pay the fine through [REDACTED]

To pay the fine, you should enter the [REDACTED] digits resulting code, which is located on the back of your [REDACTED] in the payment form and press OK (if you have several codes, enter them one after the other and press OK).



OK

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

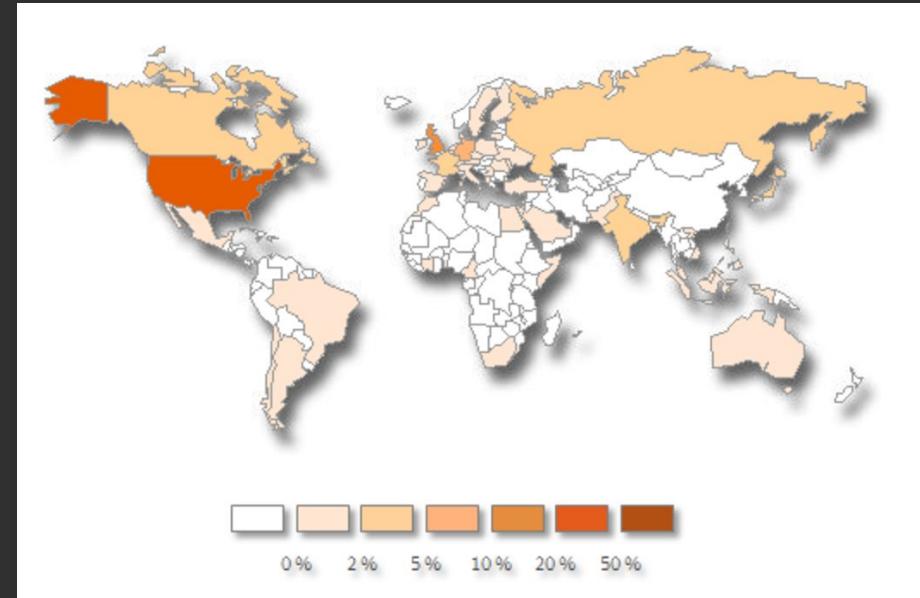
I

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

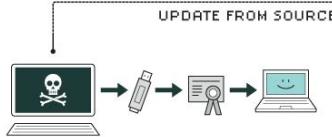
I

A

Virus

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

HOW STUXNET WORKED



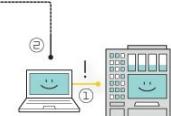
1. infection

Stuxnet enters a system via a USB stick and proceeds to infect all machines running Microsoft Windows. By brandishing a digital certificate that seems to show that it comes from a reliable company, the worm is able to evade automated-detection systems.



2. search

Stuxnet then checks whether a given machine is part of the targeted industrial control system made by Siemens. Such systems are deployed in Iran to run high-speed centrifuges that help to enrich nuclear fuel.



3. update

If the system isn't a target, Stuxnet does nothing; if it is, the worm attempts to access the Internet and download a more recent version of itself.



4. compromise

The worm then compromises the target system's logic controllers, exploiting "zero day" vulnerabilities—software weaknesses that haven't been identified by security experts.



5. control

In the beginning, Stuxnet spies on the operations of the targeted system. Then it uses the information it has gathered to take control of the centrifuges, making them spin themselves to failure.



Source: <http://symc.ly/2pk0p3q>

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... □

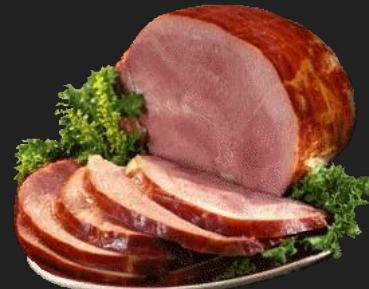
<link to strange website URL:
<http://difirtyuio.ga/neyJjljogNzM1NjAsICJmljogMCwgIm0iOiA2Mzk3MCwgImwiOiA2NCwgInMiOiAwLCAidSI6IDIzNTYzMtQwMywgInQiOiAxLCAiC2QiOiAyMH0=>>



Dear Frank,

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

Thanks,
Bob

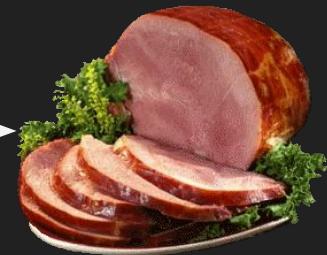


Strategy: Count the Words

| | | |
|---------|-----|-----|
| free | ... | 100 |
| money | ... | 10 |
| . | ... | . |
| . | ... | . |
| . | ... | . |
| account | ... | 2 |



| | | |
|---------|-----|---|
| free | ... | 1 |
| money | ... | 1 |
| . | ... | . |
| . | ... | . |
| . | ... | . |
| account | ... | 2 |



Train a Classifier Model



Email labeled as 'ham'



Email labeled as 'spam'

Our
"Magical"
Classifier
Model

How to train the Classifier Model

Given: Training Data \mathcal{D}

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

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>

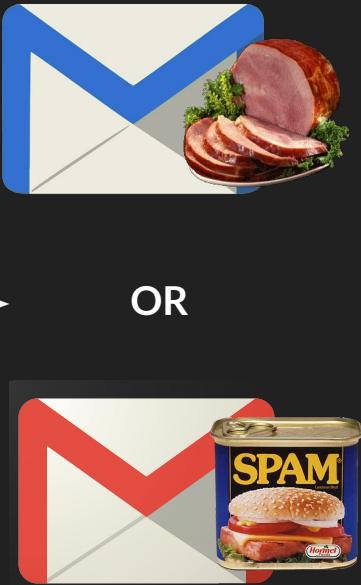
Use model to make prediction



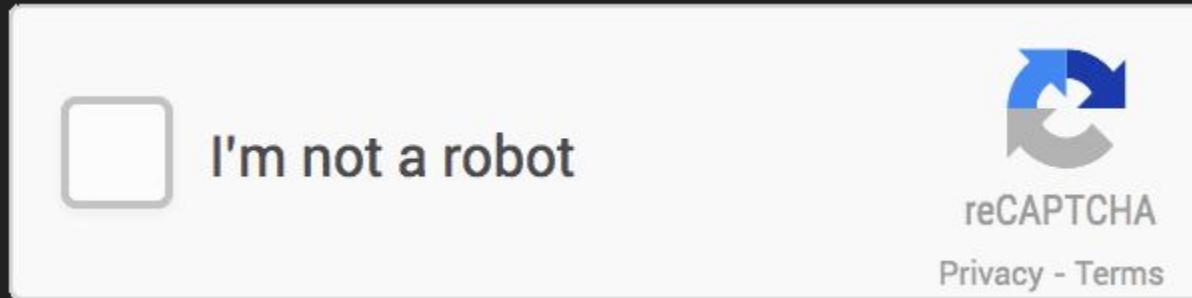
New, unlabeled email



OR



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.

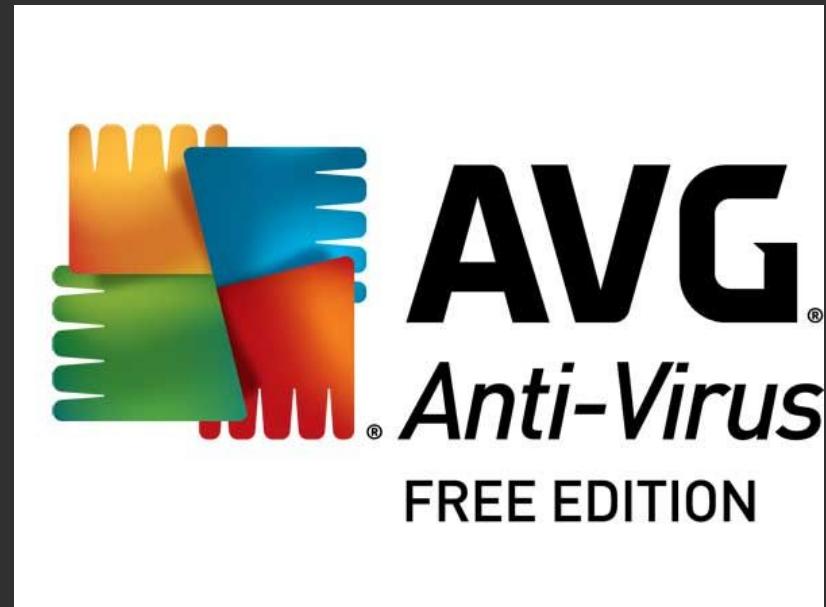
Avast

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





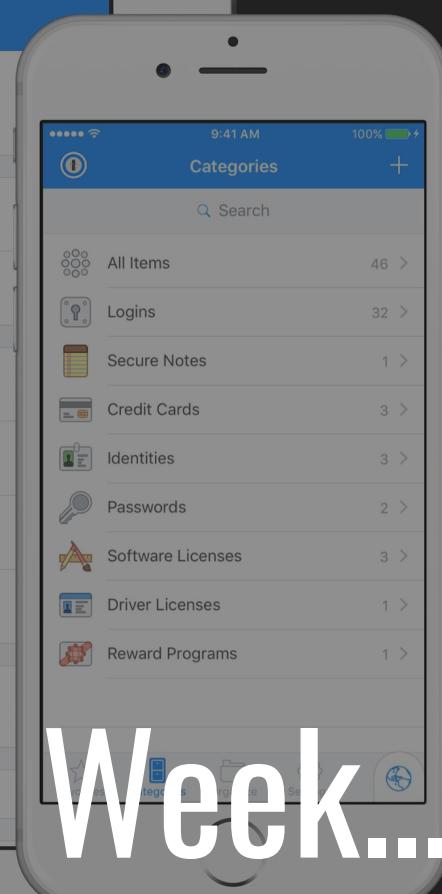
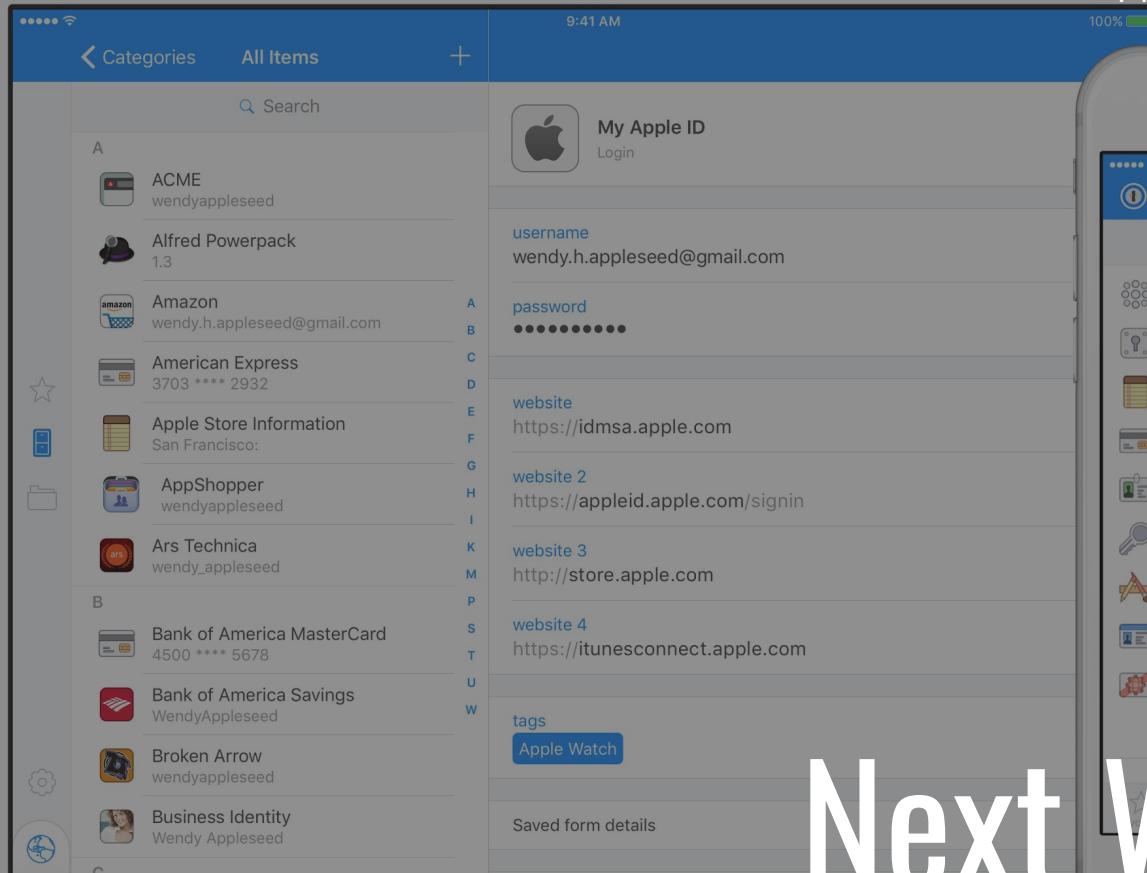
Safety in the Cloud Tip

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...