

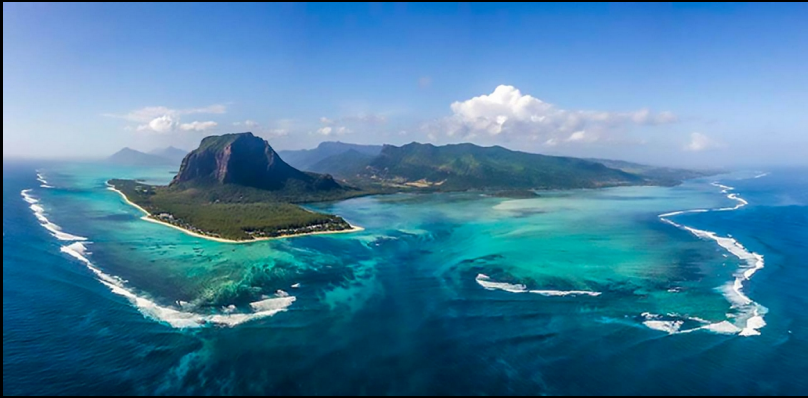
# Cybersecurity @Skokie Library

Eric Chan-Tin  
Loyola University Chicago



# About Me

- Teach cybersecurity and programming at Loyola University Chicago since 2018
- Research on cybersecurity and privacy
- Lead the Loyola Center for Cybersecurity and Privacy



# Ask Questions Anytime

- This session is for you

# THINK LIKE AN ADVERSARY







# Agenda

- **Authentication**
- Phishing
- Wireless Security
- Phone Security



# Types of Authentication

- “Something you know”
- “Something you have”
- “Something you are”
- “Someplace you are”

# Types of Authentication

- “Something you know”
  - Secret
  - E.g. password, PIN
- “Something you have”
  - E.g. ID card, smart card, token, authenticator apps
- “Something you are”
  - E.g. fingerprint, voice, face, iris
- “Someplace you are”
  - E.g.: Location + Time

# Most Common Passwords 2021 vs 2014

- 123456
- 123456789
- picture1
- password
- 12345678
- 111111
- 123123
- 12345
- 123456
- password
- 12345
- qwerty
- baseball
- dragon
- letmein
- 111111

# Password Selection

- Random
  - Best
  - Hard to remember
- Pronounceable phrase or sentence
  - H3110There
  - WY5iWY6
- Password phrases
  - CorrectHorseBatteryStaple
- User selection
  - Usually easy to guess



# TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

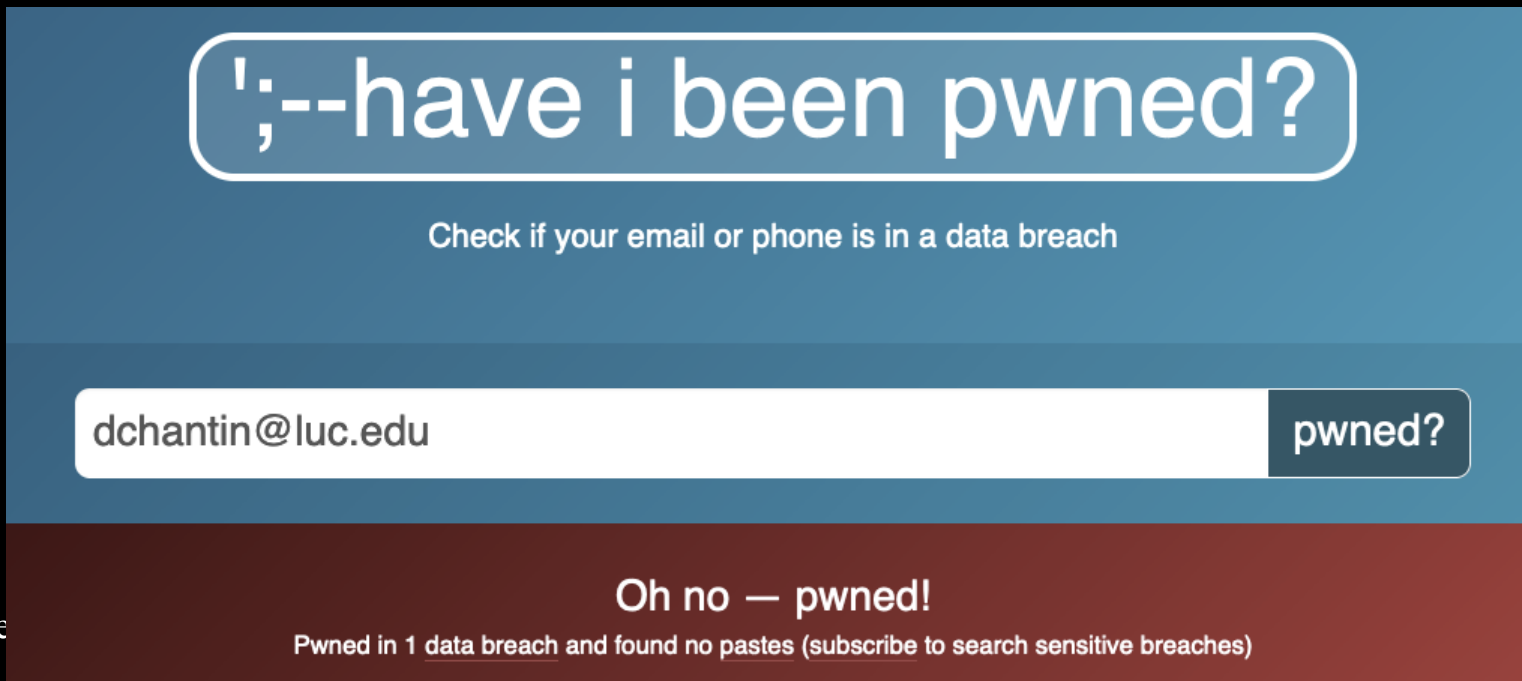
Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years



➤ Learn about our methodology at [hivesystems.io/password](https://hivesystems.io/password)

# Password Reuse

- One unique password per account!
- Password breach on one website → password spraying on other websites
- Check <https://haveibeenpwned.com/>



';--have i been pwned?

Check if your email or phone is in a data breach

dchantin@luc.edu pwned?

Oh no — pwned!

Pwned in 1 [data breach](#) and found no [pastes](#) ([subscribe](#) to search sensitive breaches)

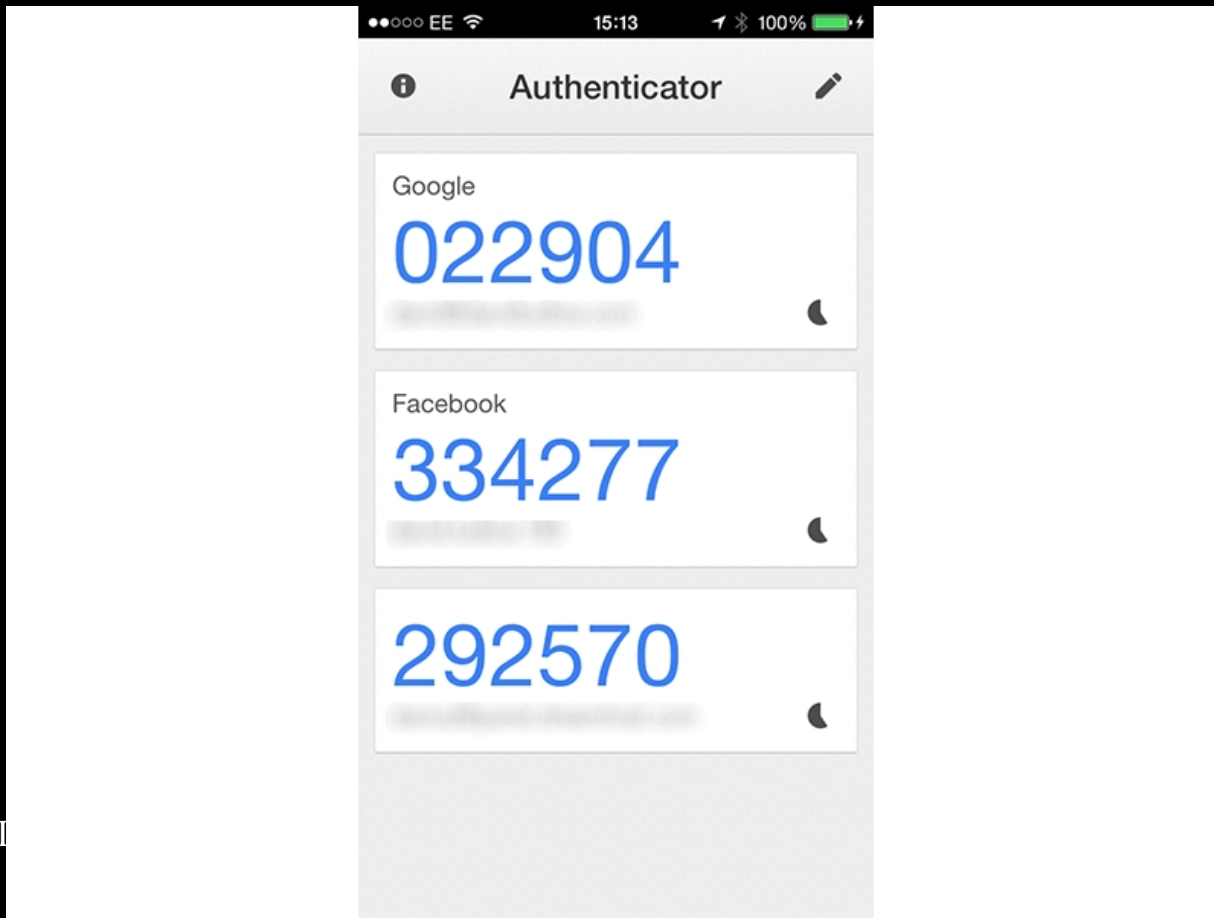
# Use Password Managers

- Automatic password generation
- One master password to remember all other passwords
- E.g. PasswordSafe, Dashlane, Keepass, etc...
- Demo on a password manager

**ONE PASSWORD MANAGER TO RULE THEM ALL**



# Hardware/Software Tokens





# Two-Factor Authentication

- Password and software token
- Multiple biometrics
- Password and biometric
- Biometric and token
- Etc...

*HURRY!*

IT KEEPS SAYING "WRONG PASSWORD!"  
I'VE TRIED EVERYTHING IT MIGHT BE!

*THE CLOCK IS TICKING!*

I REQUESTED A RESET BUT HAVEN'T  
GOTTEN IT! WHICH EMAIL DID I USE?!

*SIRENS ARE GOING OFF!!*

IT'S NOT IN MY PASSWORD MANAGER!  
IS IT IN A BROWSER? WHICH BROWSER?  
IS AUTOFILL SYNCED TO MY PHONE??

*OH MY GOD THE SCREAMING!!*



I FEEL BAD FOR EVERYONE IN HAWAII, BUT  
WHEN THE GOVERNOR COULDN'T GET INTO HIS  
TWITTER ACCOUNT, HE LIVED OUT ONE OF MY  
VERY SPECIFIC NIGHTMARES IN REAL LIFE.

# Agenda

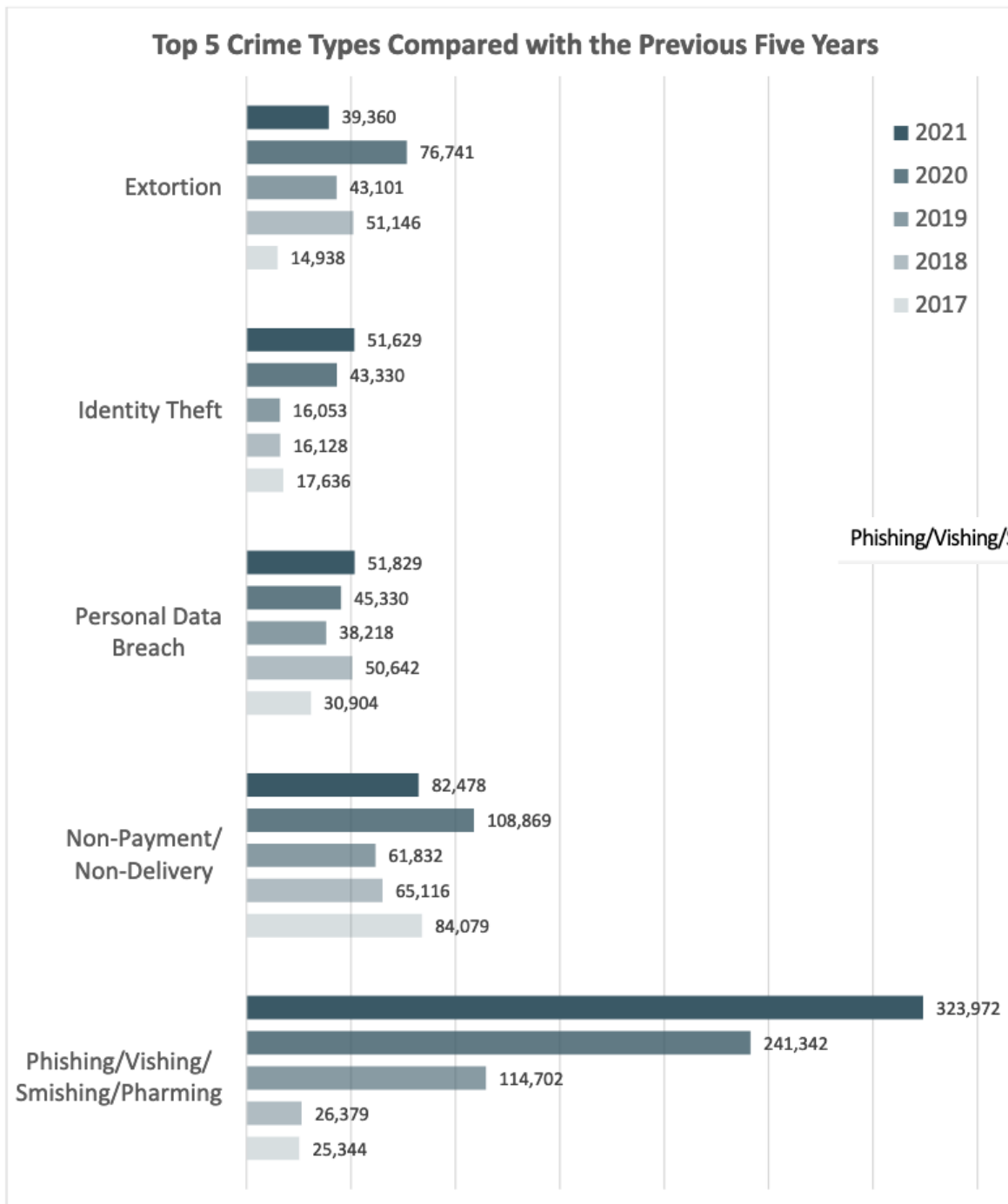
- Authentication
- **Phishing**
- Wireless Security
- Phone Security

# Phishing

- Via Email, Phone, Text message
- Someone posing as a legitimate individual/institution



TOP 5 CRIME TYPE COMPARISON<sup>4</sup>



# NETFLIX

⚠ Your account is on hold.

## Please update your payment details

Hi Dear,

We're having some trouble with your current billing information. We'll try again, but in the meantime you may want to update your payment details.

[UPDATE ACCOUNT NOW](#)

Need help? We're here if you need it. Visit the [Help Centre](#) or [contact us](#) now.

- Your friends at Netflix

Questions? Call [1800.096.3879](#)

**From:** ITS Helpdesk <[its@loyola-info.org](mailto:its@loyola-info.org)>

**Date:**

**To:** W

**Subject:** Account Recovery



# LOYOLA

## UNIVERSITY CHICAGO

*Preparing people to lead extraordinary lives*

Your account will be blocked unless you act right away for immediate service. Click [here](#) to provide ITS with your student ID and contact information to facilitate fast recovery.

-----  
Sincerely yours,

ITS Helpdesk

Hello, Linda Evans

## Here's your estimate

Billing Department of paypal sent you an estimate for \$600.00 USD.

[View Your Estimate](#)

### Seller note to customer

According to the information, your PayPal account may have been illegally accessed. \$600.00 has been deducted from your account to cover the cost of BEST BUY E-GIFT CARD. This transaction will appear on the Payment activity page in the amount that was automatically deducted after 24 hours. If you think you did not make this transaction, call us right away at +1 (844) 222-0466, or visit the PayPal Support Center for assistance.

### Don't know this seller?

You can safely ignore this estimate if you're not buying anything from this seller. PayPal won't ask you to call or send texts to phone numbers in an estimate. We don't ask for your credentials or auto-debit money from your account against any estimates. [Contact us](#) if you're still not sure.



[Help & Contact](#) | [Security](#) | [Apps](#)



NOTE: This estimate is between you and the seller or provider. PayPal is not a party to the estimate and is not responsible for the understanding you reach with the seller or provider.

PayPal is committed to preventing fraudulent emails. Emails from PayPal will always contain your full name. [Learn to identify phishing](#)

Please don't reply to this email. To get in touch with us, click [Help & Contact](#).

Not sure why you received this email? [Learn more](#)

Copyright © 1999-2022 PayPal, Inc. All rights reserved. PayPal is located at 2211 N. First St., San Jose, CA 95131.

PayPal RT000634:en\_US(en-US):1.2.0:f5609074fa996



# Smishing (SMS Phishing)



1410100027 >

Text Message  
Today 12:35 PM

FRM:WellsFargo-Call:[833.983.2265](tel:833.983.2265)  
SUBJ:\$240.00 @ ATM on  
04/12/2021 Approved.  
MSG:Ignore MSG if Valid. Contact  
Us if Suspicious.  
IDNo:[10452420082](tel:10452420082)

# Vishing (Voice Phishing)





# Why?

- Steal your identity, credit card number, health insurance
- Steal money from your bank account/credit card account

# Other Types of Phishing

- “Regular” phishing
- Business Email Compromise (whaling)
- Catphishing
- Romance scams
- Identity thefts

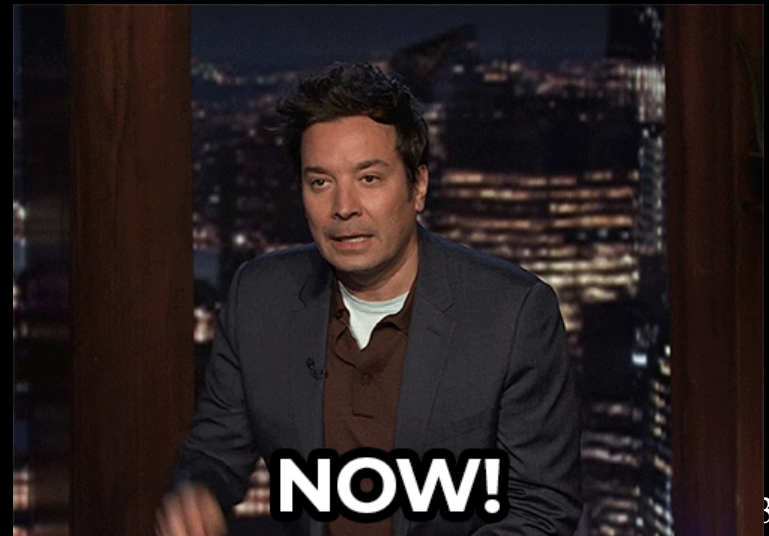


# Social Engineering

- <https://www.youtube.com/watch?v=lc7scxvKQOo>
- Be careful what you post and share online
- Check your social media privacy settings

# How to Protect Yourself?

- Wait, Pause
  - Phishers always make it “**urgent**”
- Call back using a known number
  - Do not use the number you received in the email/text/phone call
- Too good to be true




# Agenda

- Authentication
- Phishing
- **Wireless Security**
- Phone Security



# Wireless Security

- Connect to SECURE wifi (lock icon)
- Open wifi, e.g. at airports, hotels
  - Your phone broadcasts everything!
  - No privacy
  - Risk of interception/modifications of messages
- Use https 
- Use your phone hotspot



- If possible, will show a demo of the Pineapple wireless sniffer

# Agenda

- Authentication
- Phishing
- Wireless Security
- **Phone Security**

# Mobile Applications

- Only download from official App store
- Be careful what you download and install

# Mobile Applications

- Can access
  - Your phone number
  - Other phone information
  - Location

# Phone Metadata is very Useful!

- E.g.  
<https://www.abc.net.au/news/2015-08-24/metadata-a-what-you-found-will-ockenden/6703626>
- ~\$12 billion market (in 2021)
- If you really “had nothing to hide”, why would your data be so expensive!

Find the right taxonomy by searching across all industries, taxonomies, and dataset values.

Explore BDEX Taxonomies

By default, search results are by Unique Users. Use this dropdown to filter your search results to only include taxonomy info associated with the selected target identities

Mobile (AAID), Mobile (IDFA) ▼

- Email (MD5)
- Mobile (AAID)
- Mobile (IDFA)
- Browser Cookie ID
- US Postal Address ID

**Selected Taxonomy**

Industry Name: **Computers\Internet**

CPM Distribution: Min: **\$1.00** Avg: **\$2.40** Max: **\$5.00**

Taxonomy Name: **Audience Class**

Taxonomy Description: **Type in an audience classification if Dataset Class = Audience**

Dataset Value: **VISIT WEATHER.COM IN THE LAST 30 DAYS**

Dataset Class: -

436 Available Industries

Industry Name	Count
Computers\Ethics	11
Computers\Faqs, Help, And Tuto...	92,966
Computers\Graphics	769
Computers\Hacking	47
Computers\Hardware	132,993
Computers\History	22
Computers\Home Automation	462
Computers\Human-Computer In...	420
<b>Computers\Internet</b>	<b>3,828,031,607</b>
Computers\Mailing Lists	23,729
Computers\Mobile Computing	9,592
Computers\Multimedia	13,336
Computers\News And Media	187,779,250

2 Taxonomies

Taxonomy Name	Count
<b>Audience Class</b>	<b>3,824,997,239</b>
Dataset Class	3,828,031,607

70 Values

Permitted Values

Value	Count
VISIT TICKETMASTER.COM IN ...	53,635,629
VISIT TMZ.COM IN THE LAST ...	35,984,393
VISIT TWITTER.COM IN THE L...	57,936,857
VISIT VERIZON.COM IN THE L...	66,365,869
<b>VISIT WEATHER.COM IN THE ...</b>	<b>91,930,791</b>
<b>Dataset Class</b>	<b>Count</b>
Audience	91,930,791
<b>Target Identity</b>	<b>Count</b>
Mobile (AAID)	44,157,837
Mobile (IDFA)	47,772,954
VISIT WEATHERBUG.COM IN T...	48,143,520
VISIT WEBMD.COM IN THE LA...	68,178,867
VISIT WHITEPAGES.COM IN T...	49,626,032

# Other Phone Security

- Lock your phone
- Create a PIN (or better a password)
- Use fingerprinting/FaceID
- Erase phone after 10 failed logins
- Enable “find my phone”



# Final Words

- Use a password manager with strong passwords
  - Use MFA
- Use HTTPS
- Anybody can be anybody on the Internet
- Be careful online
- Patch/Update
- Be aware of what you install



# Questions?

- Happy to talk about anything else
- Contact: [dchantin@luc.edu](mailto:dchantin@luc.edu)



# If there is time, some cool videos

- “side channel” attacks:  
<http://cheezburger.com/64009217>
- Dolphin attack: <https://www.youtube.com/watch?v=21HjF4A3WE4>
- Potato chip video: <https://www.youtube.com/watch?v=FKXOucXB4a8>
- Laser video: <https://www.youtube.com/watch?v=nlTrnEoCOjs>