An Introduction to Cybersecurity

CS 1000 - Explorations in Computing

November 29, 2021

Bo Chen, PhD

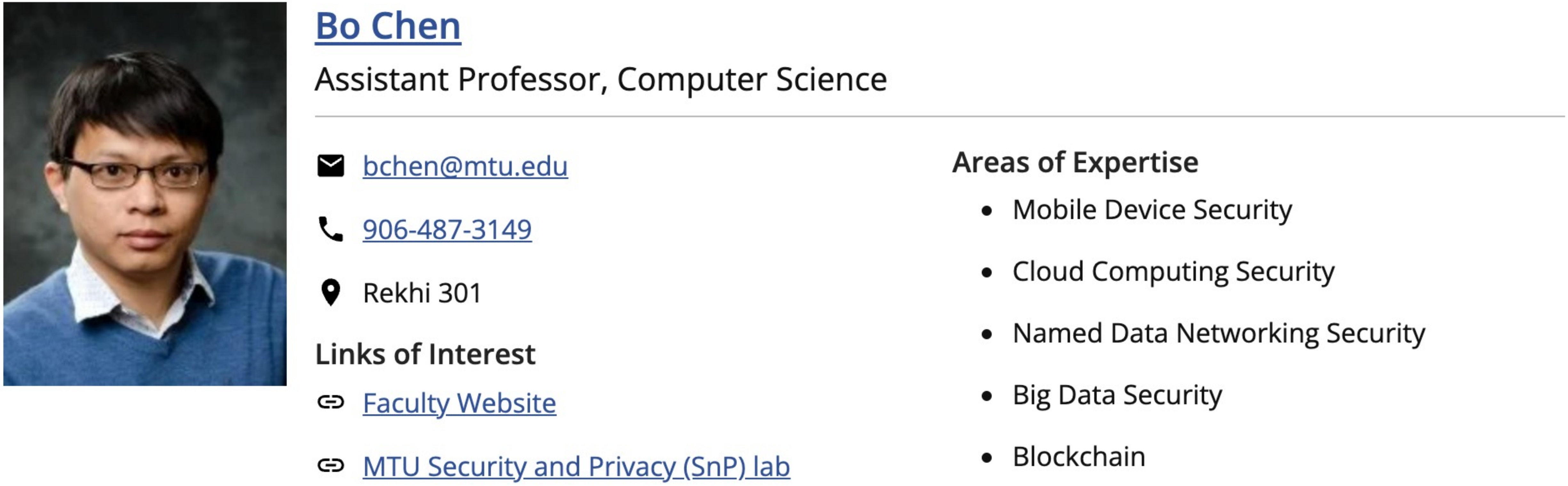
Department of Computer Science

bchen@mtu.edu

https://cs.mtu.edu/~bchen

https://snp.cs.mtu.edu

About Me



Bo Chen

Assistant Professor, Computer Science

✉ bchen@mtu.edu

☎ 906-487-3149

📍 Rekhi 301

Links of Interest

🔗 Faculty Website

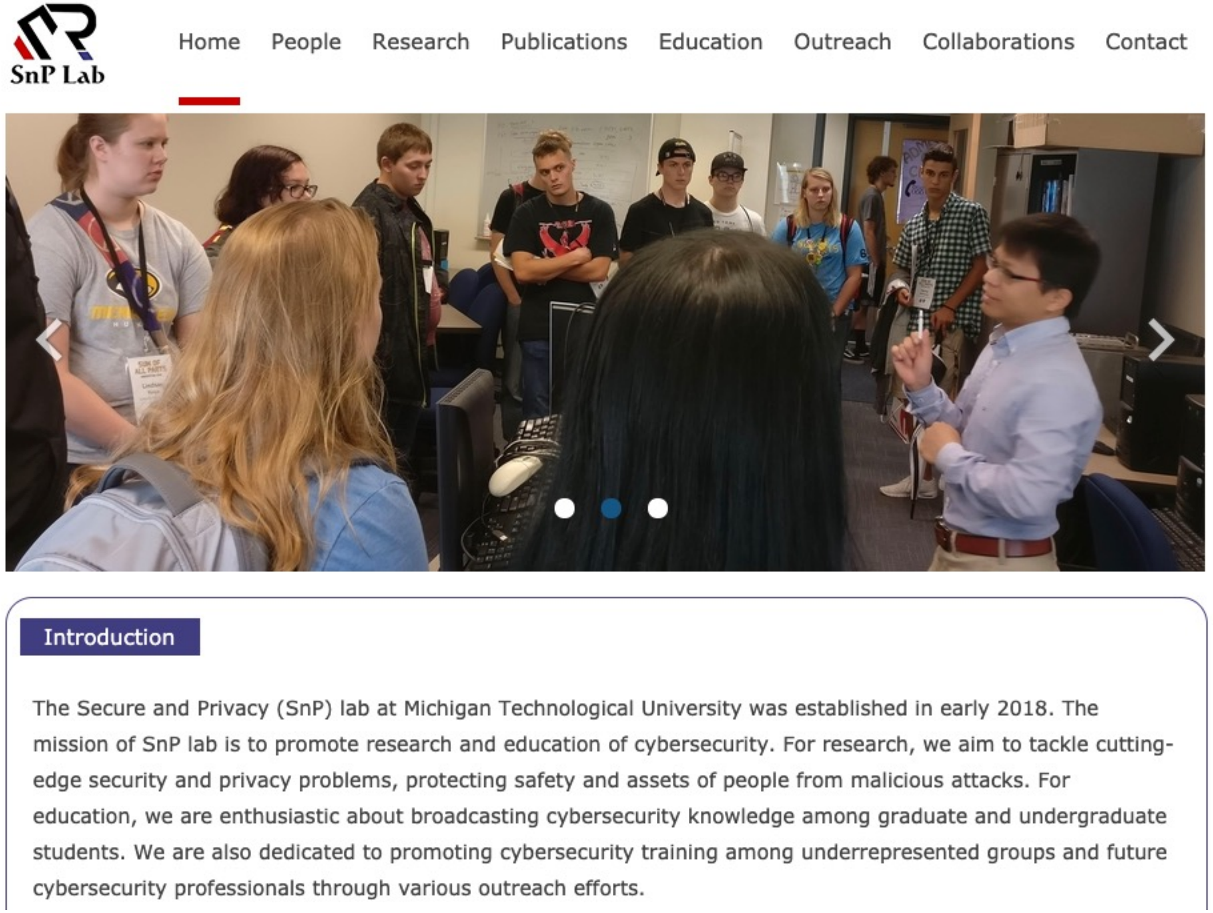
🔗 MTU Security and Privacy (SnP) lab

Areas of Expertise

- Mobile Device Security
- Cloud Computing Security
- Named Data Networking Security
- Big Data Security
- Blockchain

https://cs.mtu.edu/~bchen

About MTU Security and Privacy (SnP) Lab



The Secure and Privacy (SnP) lab at Michigan Technological University was established in early 2018. The mission of SnP lab is to promote research and education of cybersecurity. For research, we aim to tackle cutting-edge security and privacy problems, protecting safety and assets of people from malicious attacks. For education, we are enthusiastic about broadcasting cybersecurity knowledge among graduate and undergraduate students. We are also dedicated to promoting cybersecurity training among underrepresented groups and future cybersecurity professionals through various outreach efforts.

PhD Students

Niusen Chen

Wen Xie

Master Students

Tejaswi Chintapalli

Shashank Reddy Danda

Sankalp Shastry

Sai Venkateswaran

Undergraduate Students

Dominika Bobik

Ethan Brinks

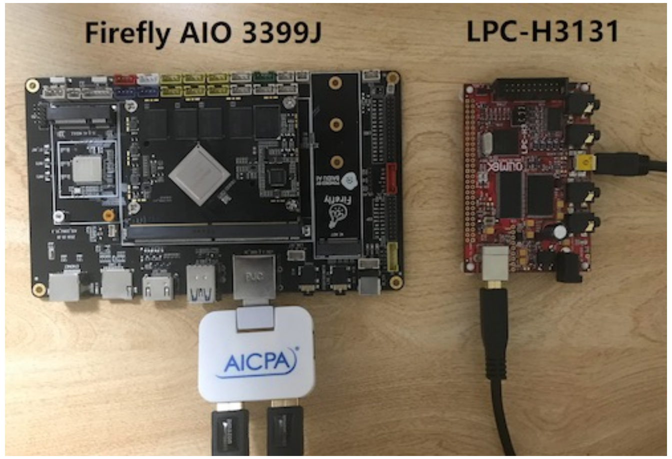
Thomas Grifka

Gary Watson

https://snp.cs.mtu.edu

About MTU Security and Privacy (SnP) Lab

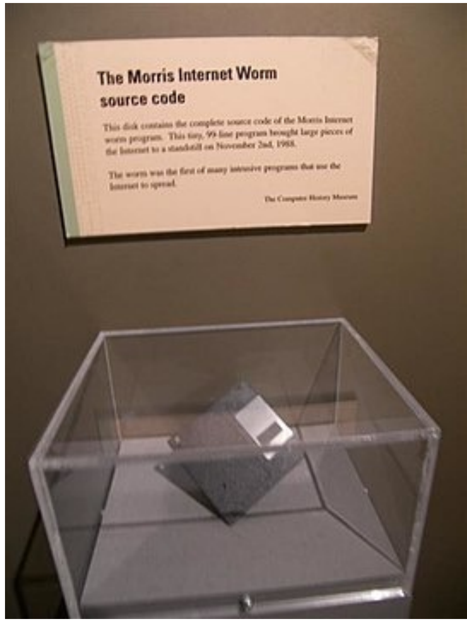
- Projects are currently funded by national science foundation, national security agency, etc.
  - Protecting sensitive data in mobile devices, IoT devices
  - Protecting critical data/ infrastructures outsourced to public clouds
  - Blockchain and information centric networking
  - Leveraging mobile devices for COVID-19 mitigation



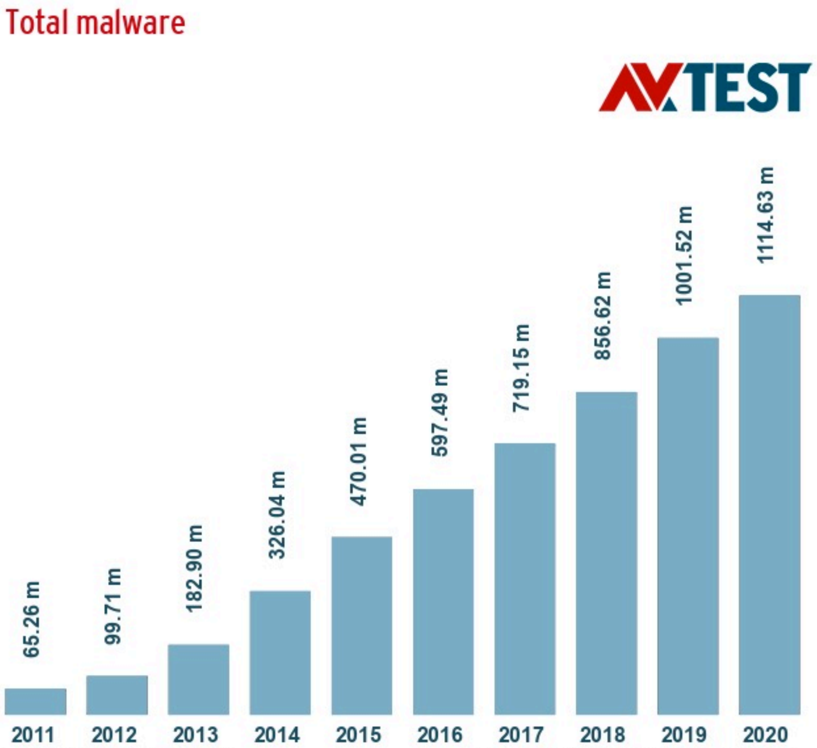
A Starting Video

- https://www.youtube.com/embed/ThBpRBpyxLI?start=0&end=50&version=3

All Starts from Malware and Hackers


The Morris Internet Worm
source code
This disk contains the complete source code of the Morris Internet worm program. This tiny, 99-line program brought large pieces of the Internet to a standstill on November 2nd, 1988.
The worm was the first of many intensive programs that use the Internet to spread.
The Computer History Museum

- On November 2, 1988, a graduate student at Cornell University, Robert Morris, unleashed what became known as the Morris worm
  - Morris worm disrupted a large number of computers then on the Internet, guessed at the time to be 10% of all those connected
- Malware and Hacks are here and there today



Last update: November 09, 2020 Copyright © AV-TEST GmbH, www.av-test.org

How to Combat Malware and Hackers?

- The answer is cybersecurity

- Ensure our systems and networks are well protected, such that any intruders can be detected, identified, and blocked
    - Make sure the software (code) we build is free of vulnerabilities
        - The attackers cannot exploit the vulnerabilities to intrude into our systems and networks

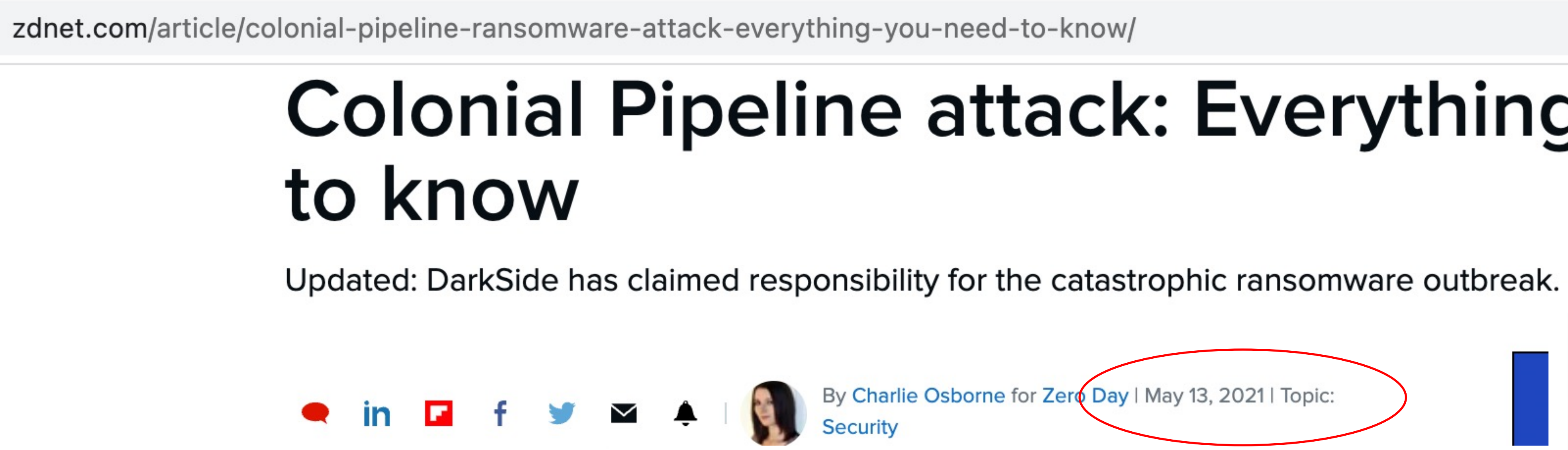
    - Make sure our data are protected
        - Not disclosed to unauthorized parties
        - Not modified by unauthorized parties
        - Always available for use
        - Always recoverable

Outline

- Recent cybersecurity instances
- What is cybersecurity (a few basic things you should know about cybersecurity) – cybersecurity 101
- Why learning cybersecurity
- How to learn cybersecurity in MTU

Recent Cybersecurity Instances

Hacking Instances Just Happen



zdnet.com/article/colonial-pipeline-ransomware-attack-everything-you-need-to-know/

Colonial Pipeline attack: Everything you need to know

Updated: DarkSide has claimed responsibility for the catastrophic ransomware outbreak.

By Charlie Osborne for Zero Day | May 13, 2021 | Topic: Security

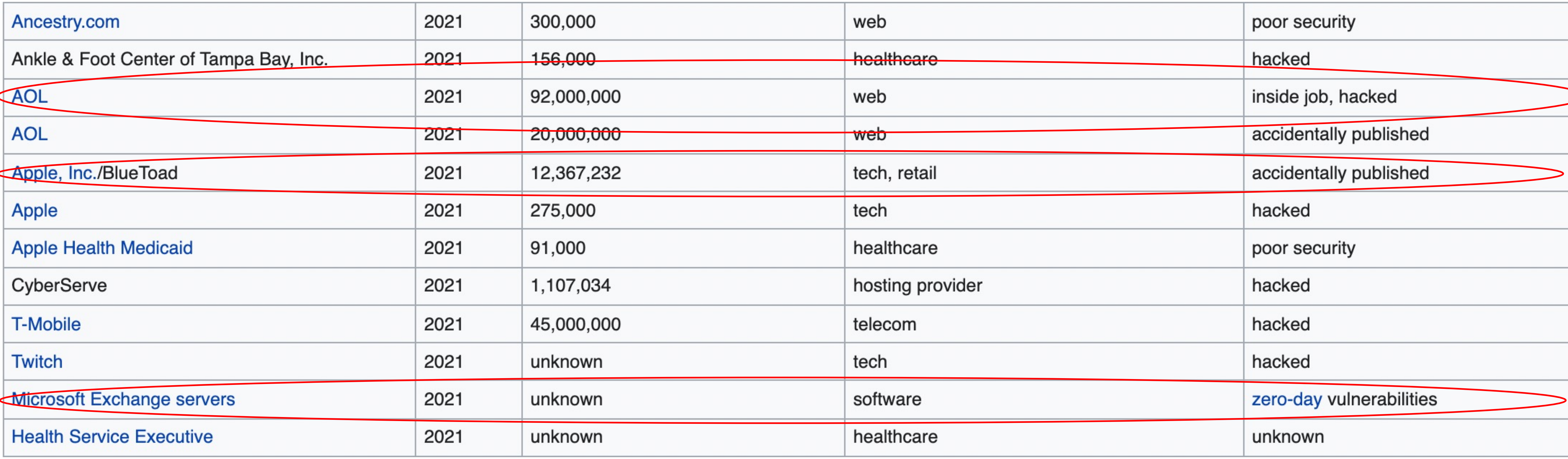
Panic buying caused widespread gasoline shortages

Colonial Pipeline paid the requested ransom (75 bitcoin or $4.4 million) within several hours after the attack

The hackers then sent Colonial Pipeline a software application to restore their network, but it operated very slowly

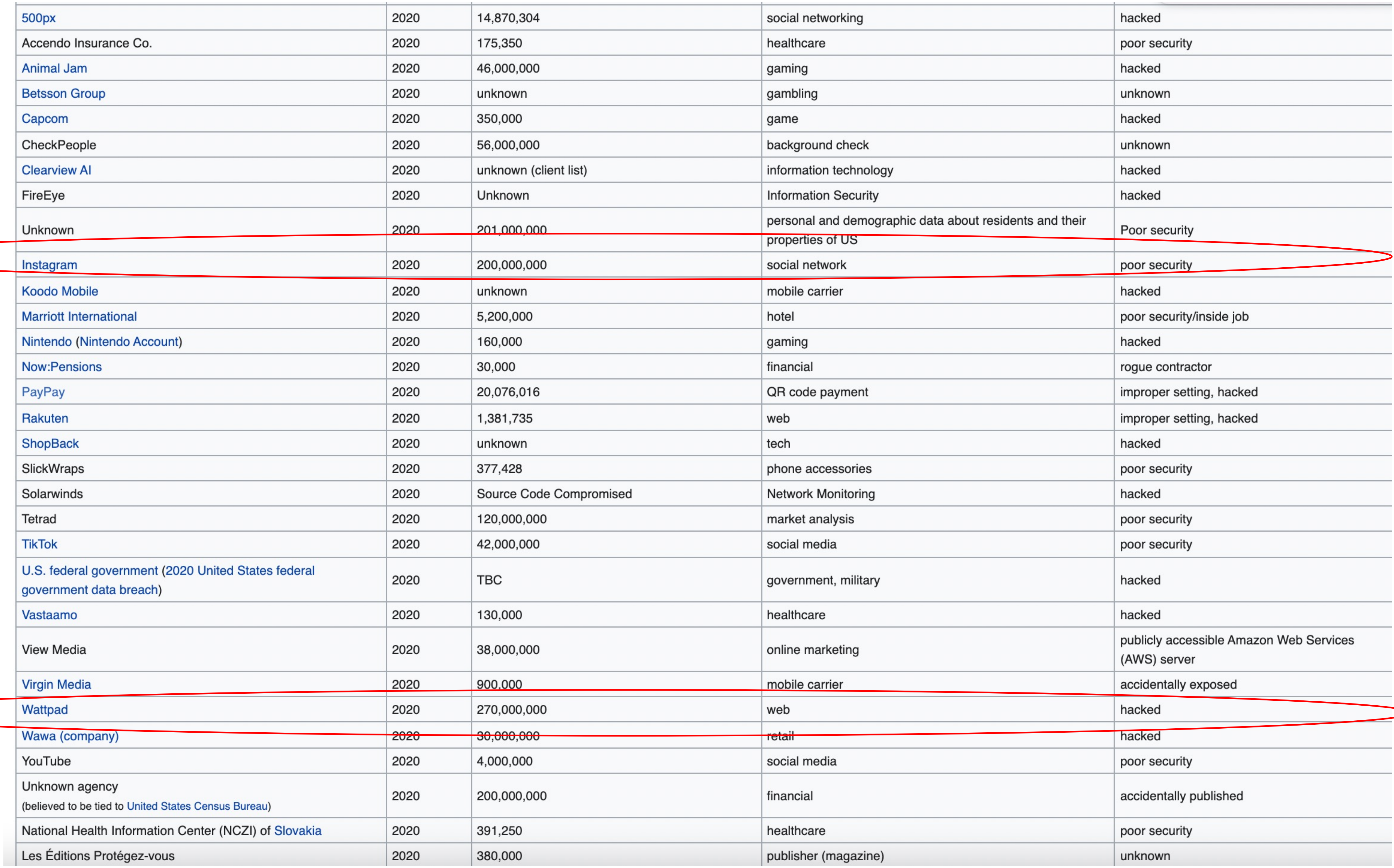
Some filling stations were without fuel for several days

Hacks 2021



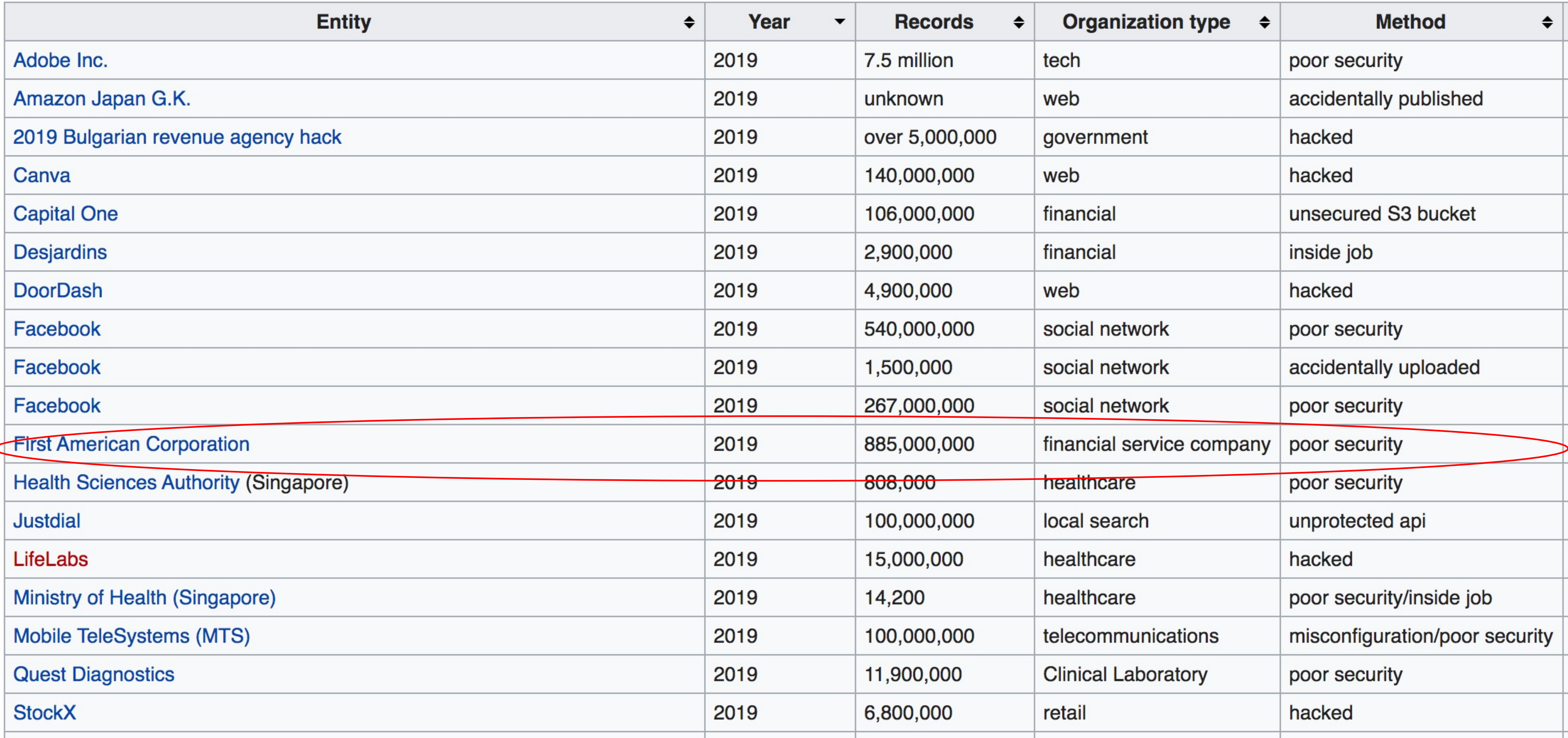
Ancestry.com	2021	300,000	web	poor security
Ankle & Foot Center of Tampa Bay, Inc.	2021	156,000	healthcare	hacked
AOL	2021	92,000,000	web	inside job, hacked
AOL	2021	20,000,000	web	accidentally published
Apple, Inc./BlueToad	2021	12,367,232	tech, retail	accidentally published
Apple	2021	275,000	tech	hacked
Apple Health Medicaid	2021	91,000	healthcare	poor security
CyberServe	2021	1,107,034	hosting provider	hacked
T-Mobile	2021	45,000,000	telecom	hacked
Twitch	2021	unknown	tech	hacked
Microsoft Exchange servers	2021	unknown	software	zero-day vulnerabilities
Health Service Executive	2021	unknown	healthcare	unknown

Hacks 2020



500px	2020	14,870,304	social networking	hacked
Accendo Insurance Co.	2020	175,350	healthcare	poor security
Animal Jam	2020	46,000,000	gaming	hacked
Betsson Group	2020	unknown	gambling	unknown
Capcom	2020	350,000	game	hacked
CheckPeople	2020	56,000,000	background check	unknown
Clearview AI	2020	unknown (client list)	information technology	hacked
FireEye	2020	Unknown	Information Security	hacked
Unknown	2020	201,000,000	personal and demographic data about residents and their properties of US	Poor security
Instagram	2020	200,000,000	social network	poor security
Koodo Mobile	2020	unknown	mobile carrier	hacked
Marriott International	2020	5,200,000	hotel	poor security/inside job
Nintendo (Nintendo Account)	2020	160,000	gaming	hacked
Now:Pensions	2020	30,000	financial	rogue contractor
PayPay	2020	20,076,016	QR code payment	improper setting, hacked
Rakuten	2020	1,381,735	web	improper setting, hacked
ShopBack	2020	unknown	tech	hacked
SlickWraps	2020	377,428	phone accessories	poor security
Solarwinds	2020	Source Code Compromised	Network Monitoring	hacked
Tetrad	2020	120,000,000	market analysis	poor security
TikTok	2020	42,000,000	social media	poor security
U.S. federal government (2020 United States federal government data breach)	2020	TBC	government, military	hacked
Vastaamo	2020	130,000	healthcare	hacked
View Media	2020	38,000,000	online marketing	publicly accessible Amazon Web Services (AWS) server
Virgin Media	2020	900,000	mobile carrier	accidentally exposed
Wattpad	2020	270,000,000	web	hacked
Wawa (company)	2020	30,000,000	retail	hacked
YouTube	2020	4,000,000	social media	poor security
Unknown agency (believed to be tied to United States Census Bureau)	2020	200,000,000	financial	accidentally published
National Health Information Center (NCZI) of Slovakia	2020	391,250	healthcare	poor security
Les Éditions Protégez-vous	2020	380,000	publisher (magazine)	unknown

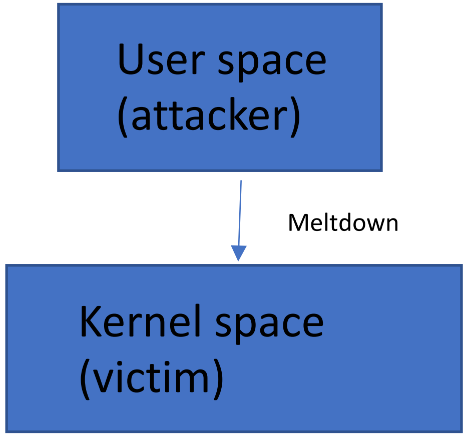
Hacks 2019



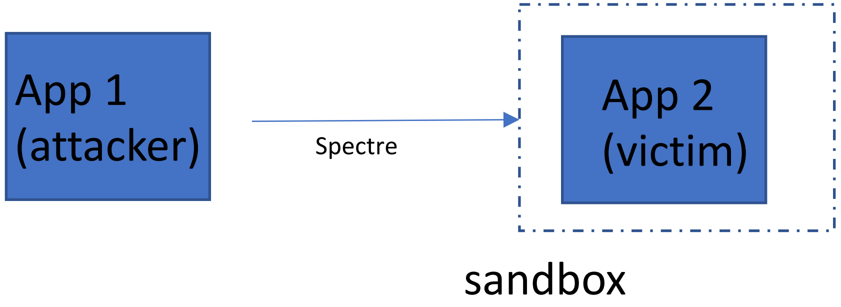
Entity	Year	Records	Organization type	Method
Adobe Inc.	2019	7.5 million	tech	poor security
Amazon Japan G.K.	2019	unknown	web	accidentally published
2019 Bulgarian revenue agency hack	2019	over 5,000,000	government	hacked
Canva	2019	140,000,000	web	hacked
Capital One	2019	106,000,000	financial	unsecured S3 bucket
Desjardins	2019	2,900,000	financial	inside job
DoorDash	2019	4,900,000	web	hacked
Facebook	2019	540,000,000	social network	poor security
Facebook	2019	1,500,000	social network	accidentally uploaded
Facebook	2019	267,000,000	social network	poor security
First American Corporation	2019	885,000,000	financial service company	poor security
Health Sciences Authority (Singapore)	2019	808,000	healthcare	poor security
Justdial	2019	100,000,000	local search	unprotected api
LifeLabs	2019	15,000,000	healthcare	hacked
Ministry of Health (Singapore)	2019	14,200	healthcare	poor security/inside job
Mobile TeleSystems (MTS)	2019	100,000,000	telecommunications	misconfiguration/poor security
Quest Diagnostics	2019	11,900,000	Clinical Laboratory	poor security
StockX	2019	6,800,000	retail	hacked

2018 – Intel Meltdown and Spectre

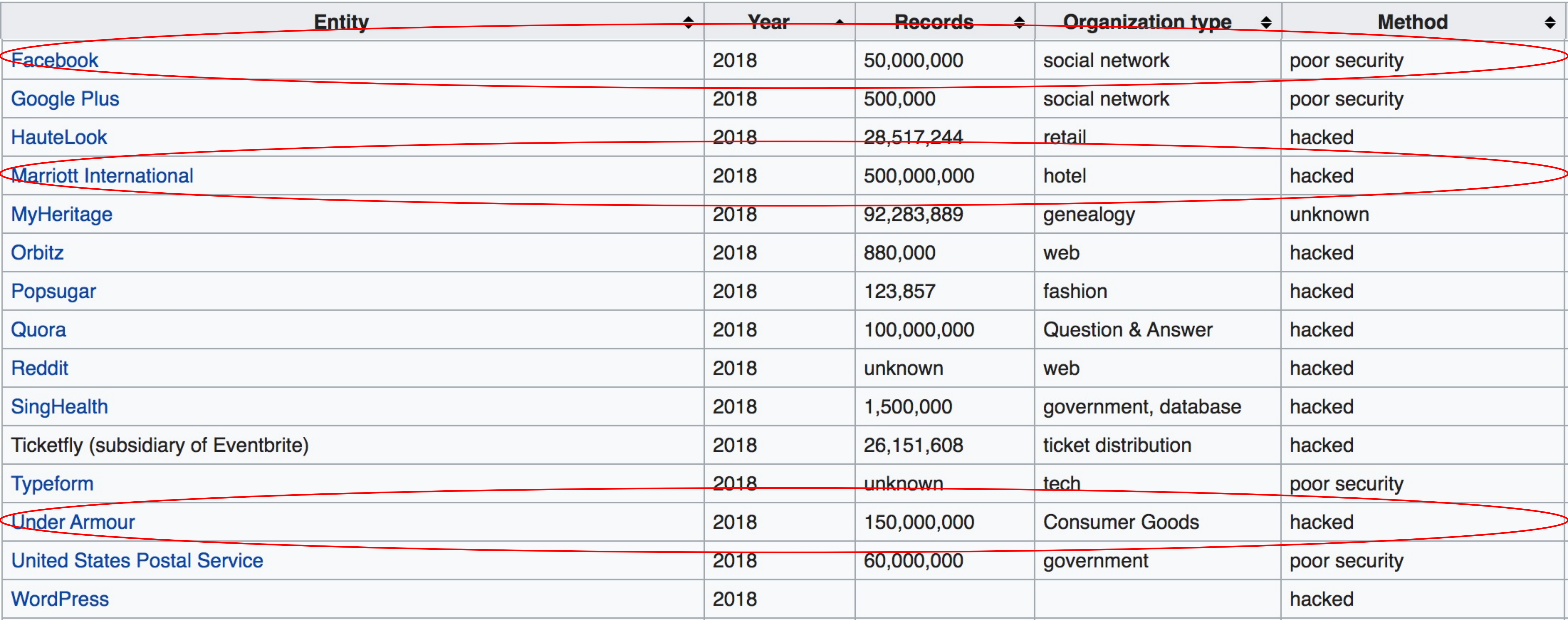
- Meltdown: affects Intel chips and lets hackers bypass the hardware barrier between applications run by users and the computer’s memory, potentially letting hackers read a computer’s memory and steal passwords.



- Spectre: affects chips from Intel, AMD and ARM and lets hackers potentially trick otherwise error-free applications into giving up secret information.



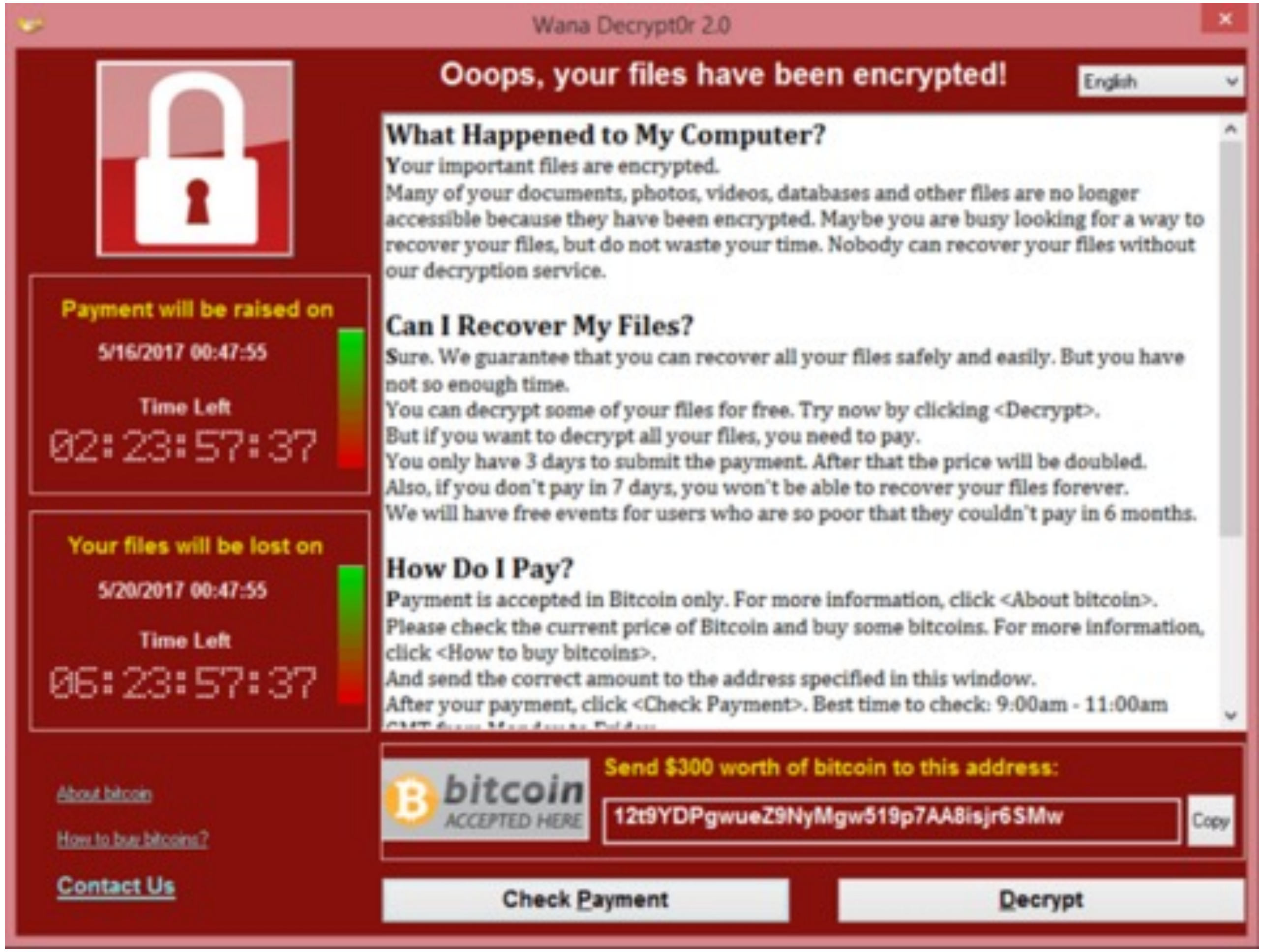
Hacks 2018



Entity	Year	Records	Organization type	Method
Facebook	2018	50,000,000	social network	poor security
Google Plus	2018	500,000	social network	poor security
HauteLook	2018	28,517,244	retail	hacked
Marriott International	2018	500,000,000	hotel	hacked
MyHeritage	2018	92,283,889	genealogy	unknown
Orbitz	2018	880,000	web	hacked
Popsugar	2018	123,857	fashion	hacked
Quora	2018	100,000,000	Question & Answer	hacked
Reddit	2018	unknown	web	hacked
SingHealth	2018	1,500,000	government, database	hacked
Ticketfly (subsidiary of Eventbrite)	2018	26,151,608	ticket distribution	hacked
Typeform	2018	unknown	tech	poor security
Under Armour	2018	150,000,000	Consumer Goods	hacked
United States Postal Service	2018	60,000,000	government	poor security
WordPress	2018			hacked

2017 - WannaCry

- WannaCry ransomware attack



Ooops, your files have been encrypted!

What Happened to My Computer?

Your important files are encrypted.
Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.
You can decrypt some of your files for free. Try now by clicking <Decrypt>.
But if you want to decrypt all your files, you need to pay.
You only have 3 days to submit the payment. After that the price will be doubled.
Also, if you don't pay in 7 days, you won't be able to recover your files forever.
We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

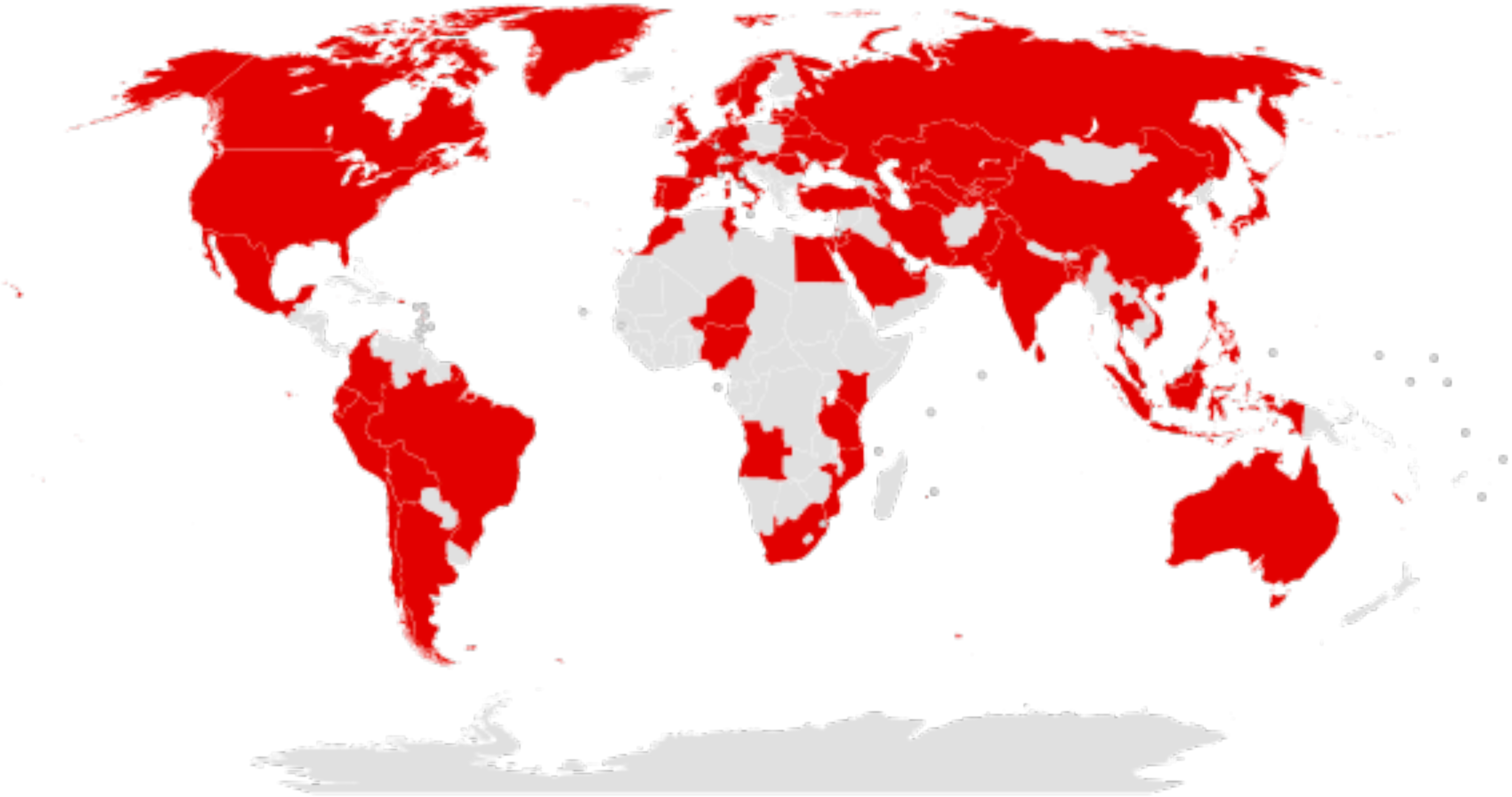
Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.
Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.
And send the correct amount to the address specified in this window.
After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Payment will be raised on
5/16/2017 00:47:55
Time Left
02:23:57:37

Your files will be lost on
5/20/2017 00:47:55
Time Left
06:23:57:37

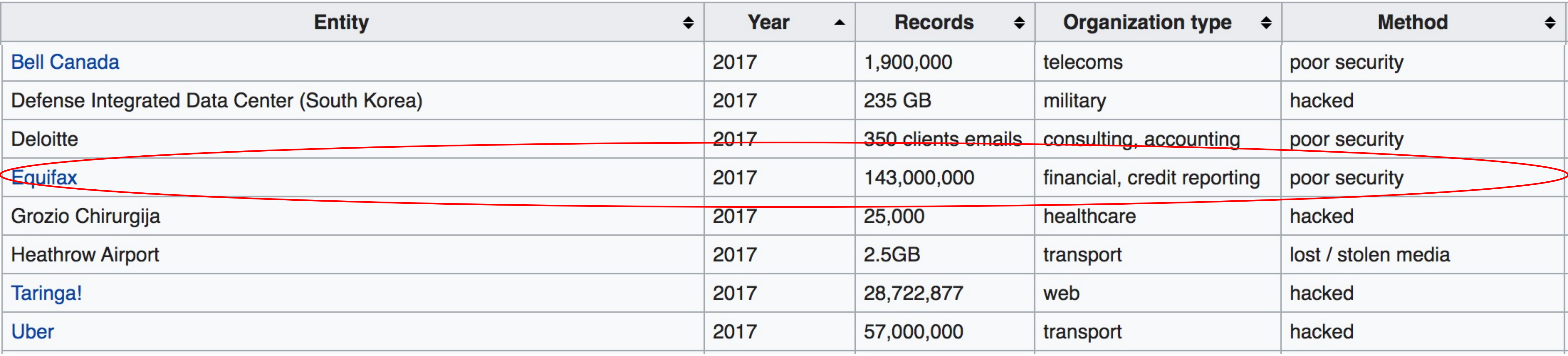
Send $300 worth of bitcoin to this address:
12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

Impact of WannaCry



Map of the countries initially affected

Hacks 2017



Entity	Year	Records	Organization type	Method
Bell Canada	2017	1,900,000	telecoms	poor security
Defense Integrated Data Center (South Korea)	2017	235 GB	military	hacked
Deloitte	2017	350 clients emails	consulting, accounting	poor security
Equifax	2017	143,000,000	financial, credit reporting	poor security
Grozio Chirurgija	2017	25,000	healthcare	hacked
Heathrow Airport	2017	2.5GB	transport	lost / stolen media
Taringa!	2017	28,722,877	web	hacked
Uber	2017	57,000,000	transport	hacked

What is Cybersecurity?

Cybersecurity 101

The Definition of Security

- Security: freedom from, or resilience against, potential harm (or other unwanted coercive change) from external forces (*wikipedia*) – **in physical space**

- Cybersecurity: the protection of computer systems from theft or damage to their hardware, software or electronic data, as well as from disruption or misdirection of the services they provide – **in cyber space**

Cybersecurity Objectives (Defender)

- Confidentiality
- Integrity
- Availability
- Authentication
- Access control
- …

Confidentiality

- *The concealment of information or resources*
  - Information is not made available or disclosed to unauthorized individuals, entities, or processes
  - E.g., your bank accounts, private photos, etc

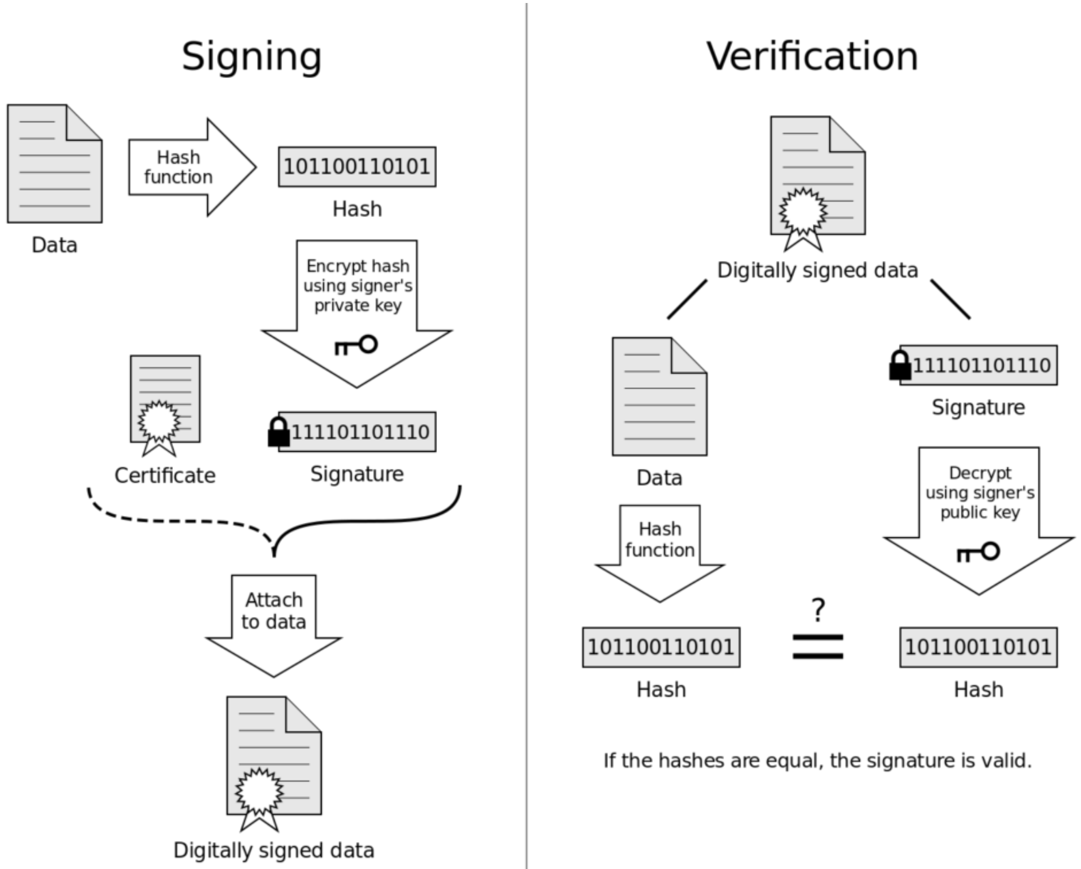
- How to achieve confidentiality? Encrypt the data using a secret key, and only the authorized entities can obtain the secret key to decrypt the data
  - Symmetric encryption: AES, DES, 3DES
  - Asymmetric encryption: RSA

Integrity

- Maintaining and assuring the accuracy and completeness of data over its entire lifecycle
  - Data cannot be modified in an unauthorized or undetected manner
  - E.g., your emails, your electronic homework

How to Ensure Integrity?

- Generate digest and perform integrity checking
  - Cryptographic hash function (SHA1, SHA2, MD5) – no key
  - Message Authentication Code (MAC) – key hash
  - Digital signature – sign the hash using the private key



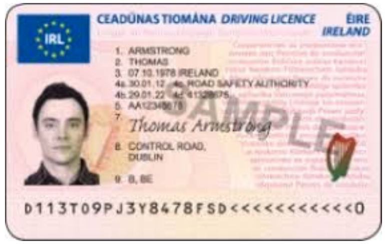
Availability

- For any information system to serve its purpose, the service/ information must be available when it is needed
  - This means the computing systems used to store and process the information, the security controls used to protect it, and the communication channels used to access it must be functioning correctly

- High availability systems aim to remain available at all times
  - Preventing service disruptions due to power outages, hardware failures, and system upgrades
  - Preventing denial-of-service attacks, such as a flood of incoming messages to the target system, essentially forcing it to shut down

Authentication

- Authentication in physical world: are you really who you claim?

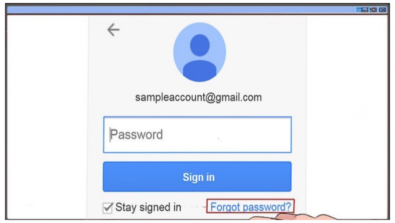

CEADÚNAS TIOMÁNA DRIVING LICENCE
ÉIRE IRELAND
IRL
1. ARMSTRONG
2. THOMAS
3. 07.10.1978 IRELAND
4a. 30.01.12 4c. ROAD SAFETY AUTHORITY
4b. 29.01.22 4d. 4132867S
5. AA1234567B
Thomas Armstrong
SAMPLE
8. CONTROL ROAD, DUBLIN
9. B, BE
D113T09PJ3Y8478FSD<<<<<<<<<<<0

Your School Name
1234 Pencil Drive, Branch TY 01234
Elizabeth Benjamin
Teacher Name: Eleanor Christoper
School Year: 09-01-20XX/06-30-20XX
Grade: 3
Parent Name: Anastasia Benjamin
Parent Phone Number: 123-456-7890
Student ID
12345

- Authentication in computers: the user who accesses to the resources is some one desired, rather than an unknown intruder/hacker. But how?

How to Do Authentication?

- Four general means for authenticating user's identity
  - Something the individual knows
    - Passwords



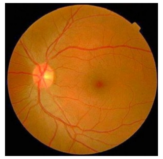
sampleaccount@gmail.com

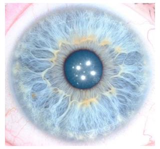
  - Something the individual possesses, a *token*
    - Memory card, smart card

CAV2/CID/CVC2/CVV2
(all other payment brands)

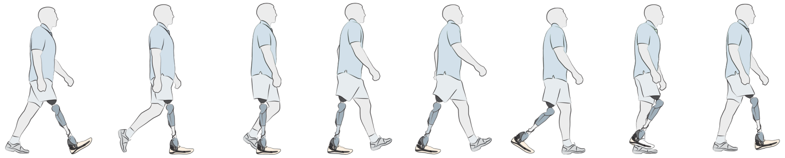
Magnetic stripe
(data on tracks 1 & 2)

  - Something the individual is
    - Fingerprint, iris, retina, face





  - Something the individual does (behavior pattern)
    - Typing rhythm, gait, and voice



How to Do Authentication (cont.)?

- Multi-factor authentication (MFA)

Access Control

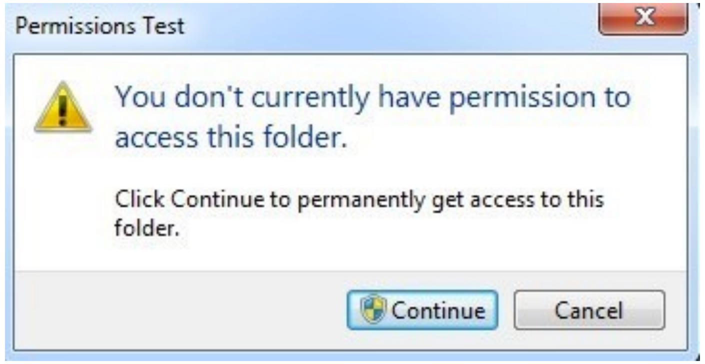
- Access control in physical world: the selective restriction of access to a place.

- Access control in computers: the selective restriction of access to computing resources
  - What files the user can read or write in the computer
  - What apps/processes the user can run
  - What data the user can have access to

How to Do Access Control?

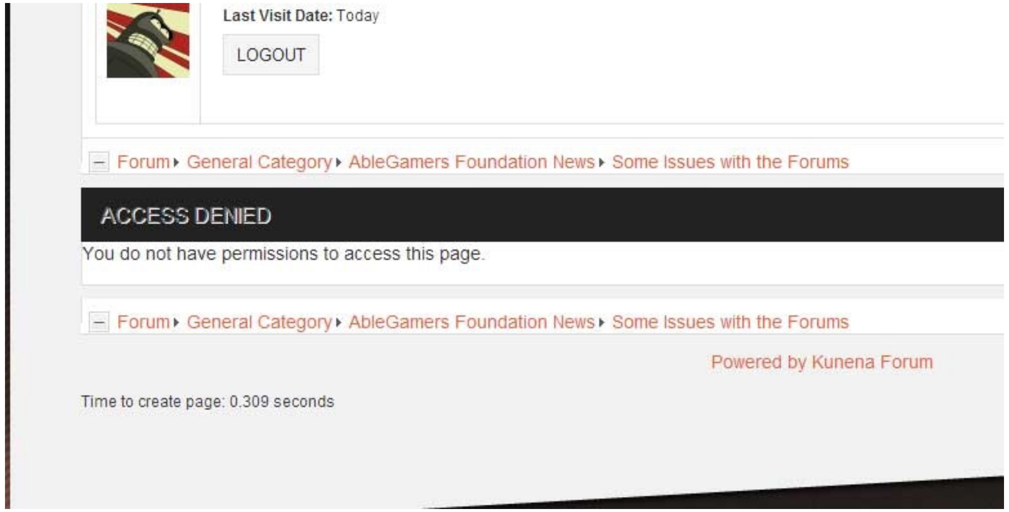
- Encrypting the protected computing resources using secret keys, and only disclose keys to those who are authorized

- The access control is enforced by systems (operating systems, database management systems, etc.) following permissions



You don't currently have permission to access this folder.

Click Continue to permanently get access to this folder.


Last Visit Date: Today

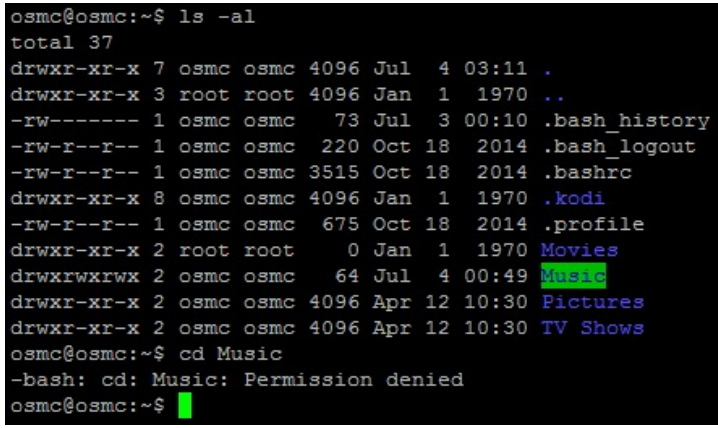
LOGOUT
Forum ▸ General Category ▸ AbleGamers Foundation News ▸ Some Issues with the Forums

ACCESS DENIED

You do not have permissions to access this page.

Forum ▸ General Category ▸ AbleGamers Foundation News ▸ Some Issues with the Forums
Powered by Kunena Forum

Time to create page: 0.309 seconds



```
osmc@osmc:~$ ls -al
total 37
drwxr-xr-x 7 osmc osmc 4096 Jul  4 03:11 .
drwxr-xr-x 3 root root 4096 Jan  1  1970 ..
-rw------- 1 osmc osmc   73 Jul  3 00:10 .bash_history
-rw-r--r-- 1 osmc osmc  220 Oct 18  2014 .bash_logout
-rw-r--r-- 1 osmc osmc 3515 Oct 18  2014 .bashrc
drwxr-xr-x 8 osmc osmc 4096 Jan  1  1970 .kodi
-rw-r--r-- 1 osmc osmc  675 Oct 18  2014 .profile
drwxr-xr-x 2 root root    0 Jan  1  1970 Movies
drwxrwxrwx 2 osmc osmc   64 Jul  4 00:49 Music
drwxr-xr-x 2 osmc osmc 4096 Apr 12 10:30 Pictures
drwxr-xr-x 2 osmc osmc 4096 Apr 12 10:30 TV Shows
osmc@osmc:~$ cd Music
-bash: cd: Music: Permission denied
osmc@osmc:~$ 
```

Non-repudiation, Privacy, and Anonymity

- Non-repudiation: users cannot deny actions
- Privacy: privacy vs. confidentiality
- Anonymity: no people know who you are when you are browsing the Internet

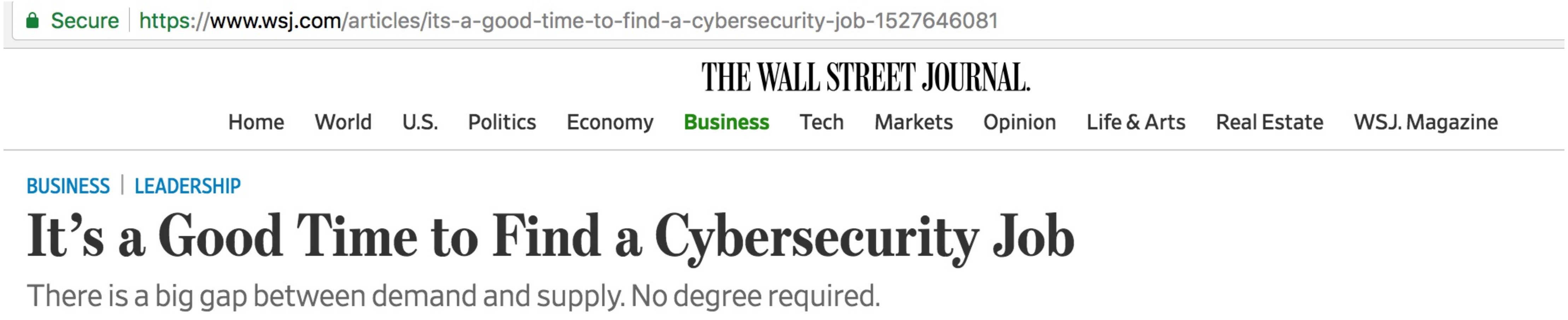
Malware (Attacker)

- Computer virus
- Computer worm
- Trojan horse
- Backdoor
- Keyloggers
- Ransomware
- Phishing
- …

Why Learning Cybersecurity?

Great Job Market

- There will be 3.5 million unfilled cybersecurity positions by 2021
  - According to Cybersecurity Jobs Report, sponsored by Herjavec Group
- The rate of growth for jobs in information security is projected at 37% from 2012 to 2022
  - According to the Bureau of Labor Statistics
  - Much faster than the average for all other occupations



THE WALL STREET JOURNAL.

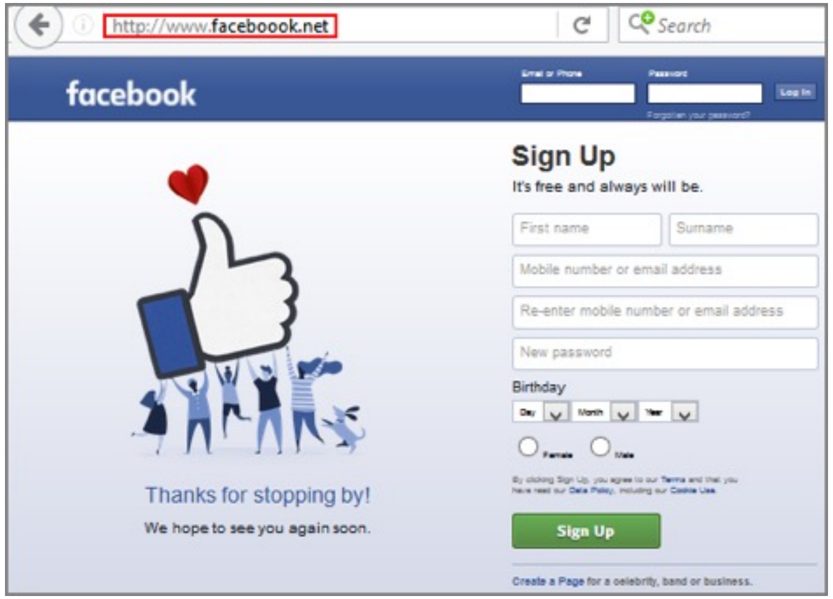
BUSINESS | LEADERSHIP

It’s a Good Time to Find a Cybersecurity Job

There is a big gap between demand and supply. No degree required.

Protect Your Own Asset

- Reduce the possibility of exposure to potential hacks
  - Malicious code is here and there (malicious java scripts, applets, etc.)
  - Make sure you trust the web sites before you go there (a lot of phishing website)
    - www.google.com is fine, but www.go0gle.com may not
    - Do you want to click the link www.facebook.net, or www.b-of-America.co.cc



http://www.faceboook.net

Sign Up

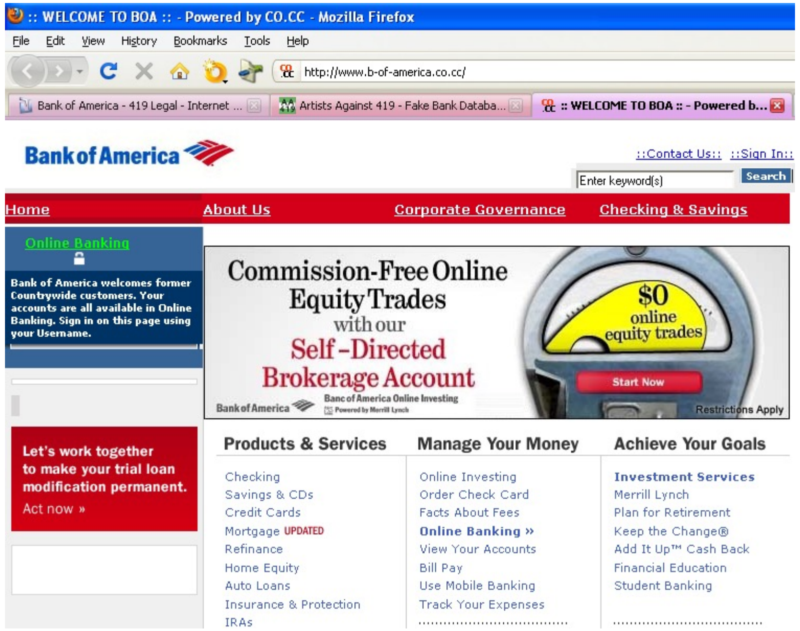
It's free and always will be.

Thanks for stopping by!

We hope to see you again soon.

By clicking Sign Up, you agree to our Terms and that you have read our Data Policy, including our Cookie Use.

Create a Page for a celebrity, band or business.



:: WELCOME TO BOA :: - Powered by CO.CC - Mozilla Firefox

http://www.b-of-america.co.cc/

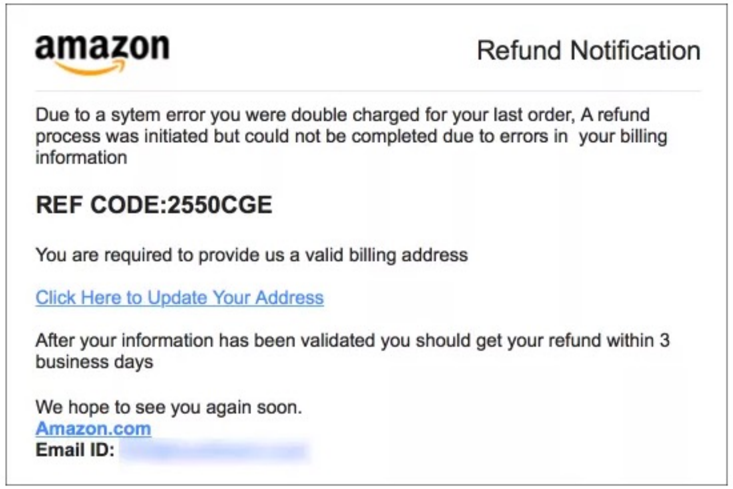
Bank of America welcomes former Countrywide customers. Your accounts are all available in Online Banking. Sign in on this page using your Username.

Commission-Free Online Equity Trades with our Self-Directed Brokerage Account

Let's work together to make your trial loan modification permanent. Act now »

Protect Your Own Asset (cont.)

- Reduce the possibility of exposure to potential hacks
  - A lot of phishing emails



amazon Refund Notification

Due to a sytem error you were double charged for your last order, A refund process was initiated but could not be completed due to errors in your billing information

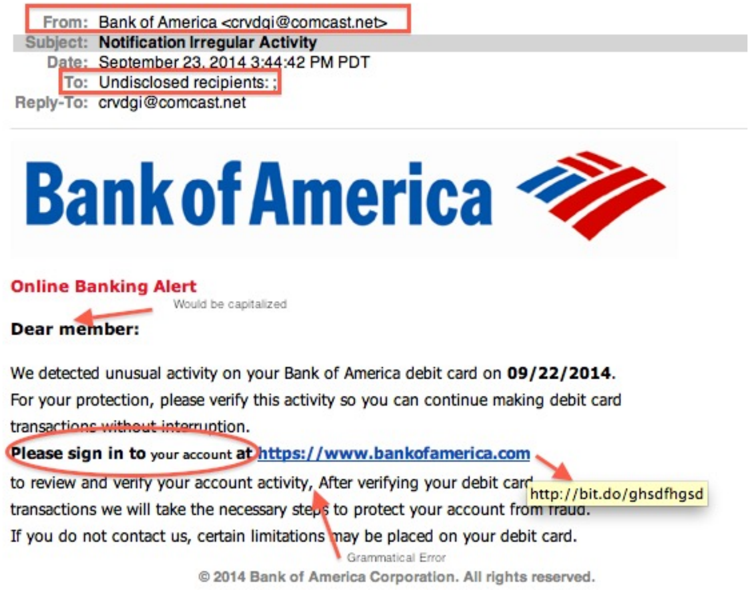
REF CODE:2550CGE

You are required to provide us a valid billing address

Click Here to Update Your Address

After your information has been validated you should get your refund within 3 business days

We hope to see you again soon.
Amazon.com
Email ID: [redacted]



From: Bank of America <crvdgi@comcast.net>
Subject: **Notification Irregular Activity**
Date: September 23, 2014 3:44:42 PM PDT
To: Undisclosed recipients: ;
Reply-To: crvdgi@comcast.net

Bank of America

Online Banking Alert

Would be capitalized

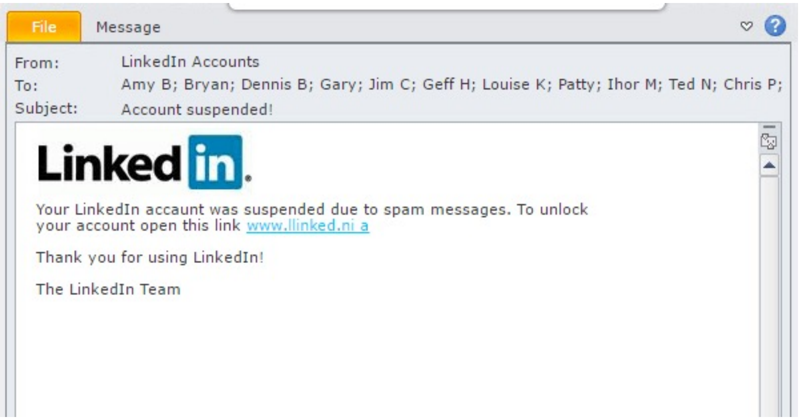
Dear member:

We detected unusual activity on your Bank of America debit card on **09/22/2014**. For your protection, please verify this activity so you can continue making debit card transactions without interruption.
Please sign in to your account **at** https://www.bankofamerica.com to review and verify your account activity, After verifying your debit card transactions we will take the necessary steps to protect your account from fraud. If you do not contact us, certain limitations may be placed on your debit card.

http://bit.do/ghsdfhgsd

Grammatical Error

© 2014 Bank of America Corporation. All rights reserved.



From: LinkedIn Accounts
To: Amy B; Bryan; Dennis B; Gary; Jim C; Geff H; Louise K; Patty; Ihor M; Ted N; Chris P;
Subject: Account suspended!

LinkedIn.

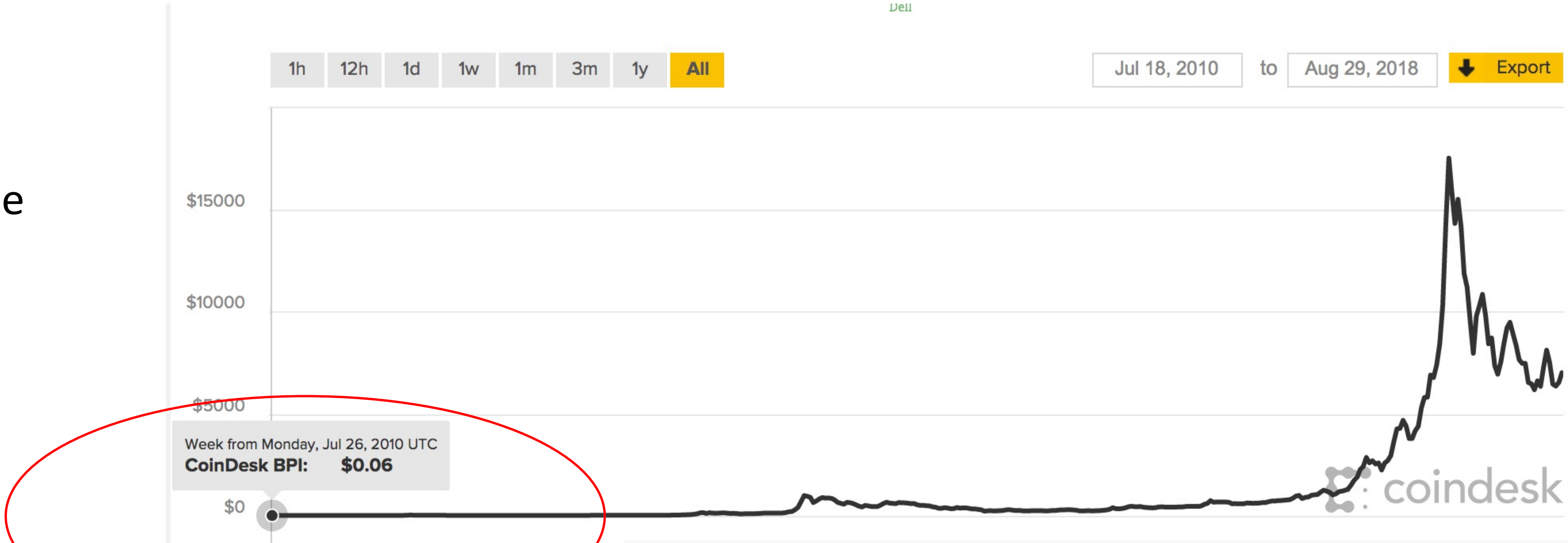
Your LinkedIn accaunt was suspended due to spam messages. To unlock your account open this link www.llinked.ni a

Thank you for using LinkedIn!

The LinkedIn Team

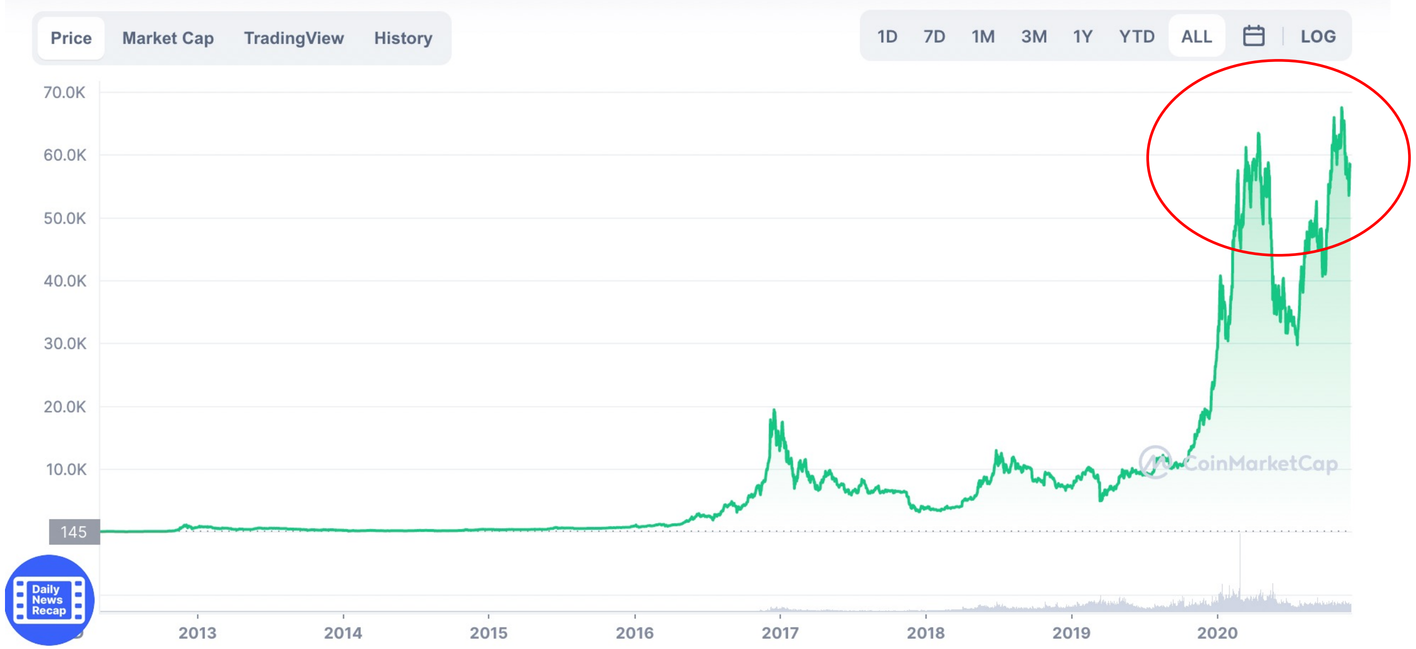
Security Technology Is Money Sometimes

Bitcoin price



Week from Monday, Jul 26, 2010 UTC
CoinDesk BPI: $0.06

Bitcoin price



How to Learn Cybersecurity in MTU?

Cybersecurity Programs in MTU

- Cybersecurity BS

Campus Health and Safety Level: Level Three

College of Computing

> College of Computing > Undergraduate > **Cybersecurity—BS**

B.S. in Cybersecurity

Because the future is computational.

Cybersecurity Programs in MTU

- Cybersecurity MS

Graduate School

Graduate School > Degree Programs > **Cybersecurity Graduate Programs**

Cybersecurity—MS

Security Courses in MTU for Undergraduates

- CS 4471 - Computer Security
- CS 4740 - Development of Trusted Software
- CS/EE 4723 - Network Security
- MA 3203 - Cryptography
- SAT 3812 - Cybersecurity I
- SAT 4812 - Cybersecurity II
- ...

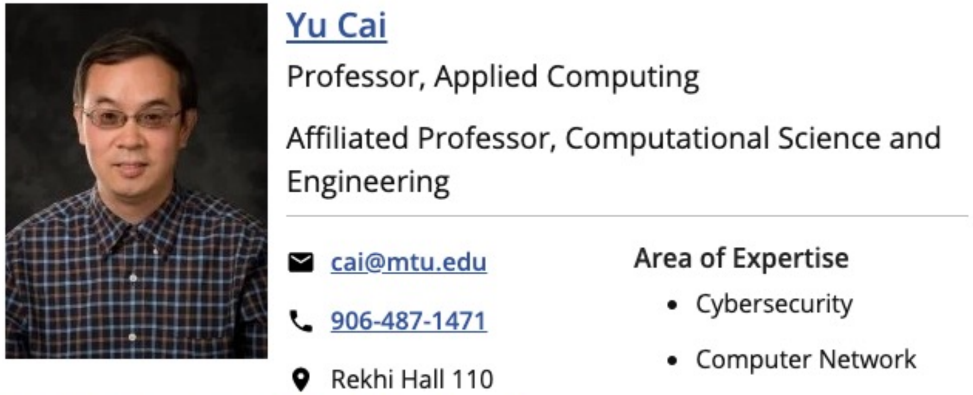
Other Resources for Cybersecurity Learning

- MTU RedTeam
  - https://snp.cs.mtu.edu/education/#competition
  - 20+ undergraduate students which are enthusiastic for hacking and defending
  - Have been getting involved in various cybersecurity competitions including NCL cyber competition, CYPHERCON, etc.
  - The team ranked 3rd out of 922 teams across the US in Spring 2021, and ranked 10th out of 3910 teams in Fall 2021

- Cyber security reading group @CS
  - https://snp.cs.mtu.edu/education/#rg
  - A forum consists of both graduate and undergraduate students. Students sit together biweekly to present and discuss the most recent security instances/research

Feel free to contact me if you want to join either

Faculty Members in MTU Working on Cybersecurity



Yu Cai

Professor, Applied Computing

Affiliated Professor, Computational Science and Engineering

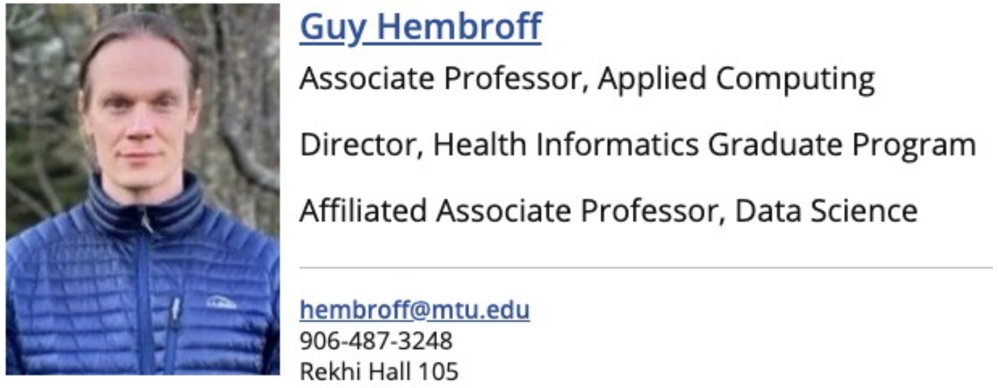
✉ cai@mtu.edu

☎ 906-487-1471

📍 Rekhi Hall 110

Area of Expertise

- Cybersecurity
- Computer Network



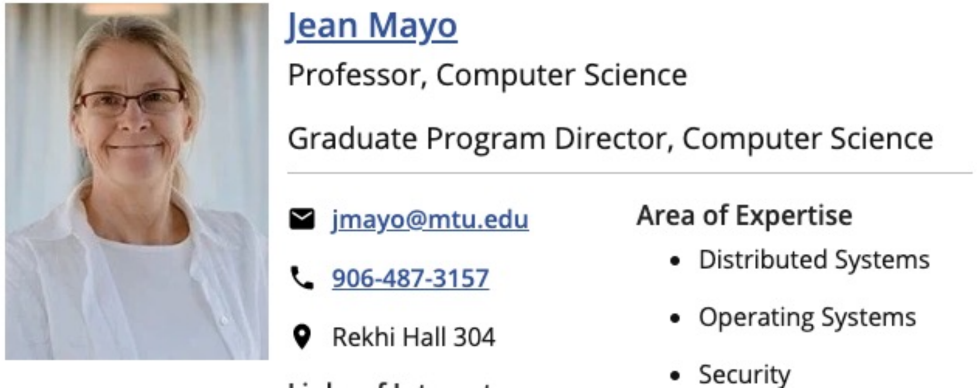
Guy Hembroff

Associate Professor, Applied Computing

Director, Health Informatics Graduate Program

Affiliated Associate Professor, Data Science

hembroff@mtu.edu
906-487-3248
Rekhi Hall 105



Jean Mayo

Professor, Computer Science

Graduate Program Director, Computer Science

✉ jmayo@mtu.edu

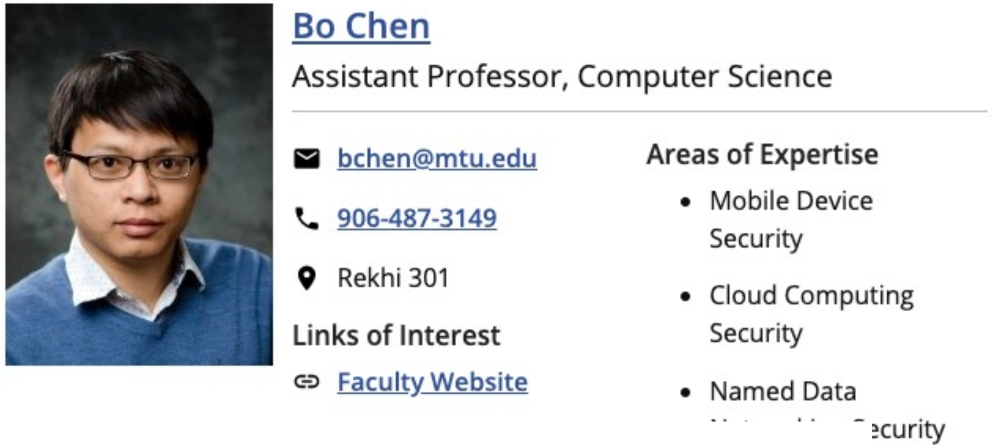
☎ 906-487-3157

📍 Rekhi Hall 304

Links of Interest

Area of Expertise

- Distributed Systems
- Operating Systems
- Security



Bo Chen

Assistant Professor, Computer Science

✉ bchen@mtu.edu

☎ 906-487-3149

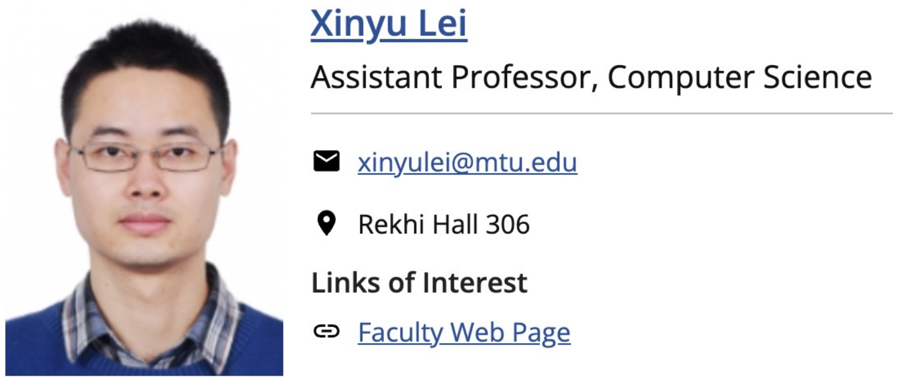
📍 Rekhi 301

Links of Interest

🔗 Faculty Website

Areas of Expertise

- Mobile Device Security
- Cloud Computing Security
- Named Data Networking Security



Xinyu Lei

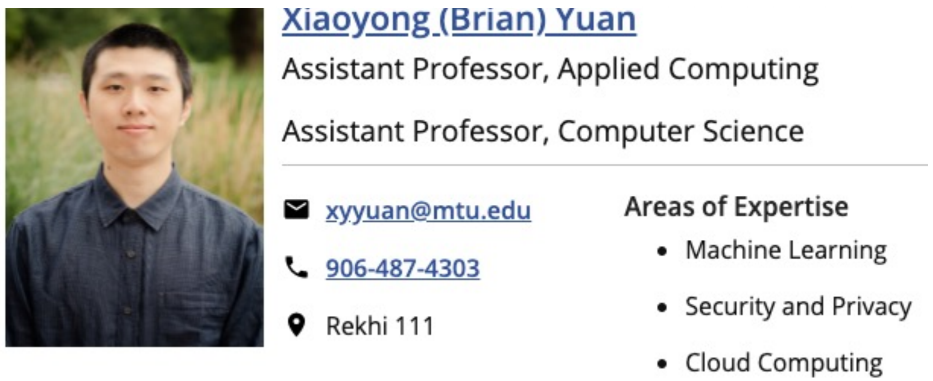
Assistant Professor, Computer Science

✉ xinyulei@mtu.edu

📍 Rekhi Hall 306

Links of Interest

🔗 Faculty Web Page



Xiaoyong (Brian) Yuan

Assistant Professor, Applied Computing

Assistant Professor, Computer Science

✉ xyyuan@mtu.edu

☎ 906-487-4303

📍 Rekhi 111

Areas of Expertise

- Machine Learning
- Security and Privacy
- Cloud Computing

Acknowledgments

- Our cybersecurity research has been supported by US National Science Foundation (NSF) under grant number 1928349-CNS and 1938130-CNS, MTU Research Excellence Fund, etc.
- Our cybersecurity education has been supported by a grant from NSF SFS and a few Gencyber grants from National Security Agency (NSA)

Q &A