

The True cost of a Data Breach

James Taylor
Sr. IT Security Consultant
Vantage Point Solutions
2211 N. Minnesota St.
Mitchell, SD 57301

(605) 995-1829
James.taylor@vantagepnt.com





Today's Speaker

James Taylor


Sr. IT Security Consultant

Vantage Point Solutions

About Me

- Father of 3 boys (18, 17, 15, my wife is a saint) and 2 dogs
- Graduate of Dakota State University, Bachelors Degrees in Computer Science (Information Security)
- Loves Capture The Flag (CTF is like a scavenger hunt with computers) competitions and gaming





“There are only two types of companies:
those that have been hacked
and those that will be.”

Robert Mueller – FBI Director 2012

What is a Data Breach?

- **Formal Definition:**
 - An intentional or unintentional release of secure or private/confidential information to the general public
- **Information Targeted:**
 - Social Security Number
 - Credit/Debit Card
 - Protected Health Information (PHI)
 - DMV Records
 - Email / Password / Usernames
 - Personally Identifiable Information (PII)



Who provides the rules and standards

- **Federal Financial Institutions Examination Council (FFIEC)** - A formal interagency body empowered to prescribe uniform principles, standards, and report forms for the federal examination of financial institutions.
- **National Institute of Standards and Technologies (NIST)** – Creates standards in technology and provides special publications to manage risk and security controls.
- **Federal Deposit Insurance Corporation (FDIC)** – Creates and promotes sound banking practices and provides insurance and audits.
- **Federal Communications Commission (FCC)** - Regulates interstate and international communications
- **Center for Internet Security (CIS)** – Creates benchmarks, best practices and tools to safeguard systems against cyber threats.
- **Office of the Comptroller of Currency (OCC)** - Charters, regulates, and supervises all national banks, federal savings associations, and federal branches and agencies of foreign banks.
- **Federal Trade Commission (FTC)** – Creates and develops policy and research tools to protect consumers.

How do they protect data

- Provide standards for cyber security process and technologies
- Audit specific industries and entities
- Impose fines for improper handling of personal data
- Information sharing and analysis

But...

It is our responsibility
to defend and harden

The True Cost

- **Even With:**
 - Board-level Involvement
 - Business Continuity Management
 - Annual Employee Training
 - Extensive Tests of the IR Plan
 - Insurance Protection
 - Use of Security Analytics
- **Cost Components**
 - Detection and Escalation
 - Post Data Breach Response
 - Notification
 - Lost Business – 36%



A bit deeper...



Average cost US in 2006 - \$3.54M, 2019- \$8.19M



Organizations with >25,000 employees is \$204 per, >500 was \$5,480 per employee



Organization with 500 employees, average cost \$2.74M



Average number of records per data set, US – 32,434

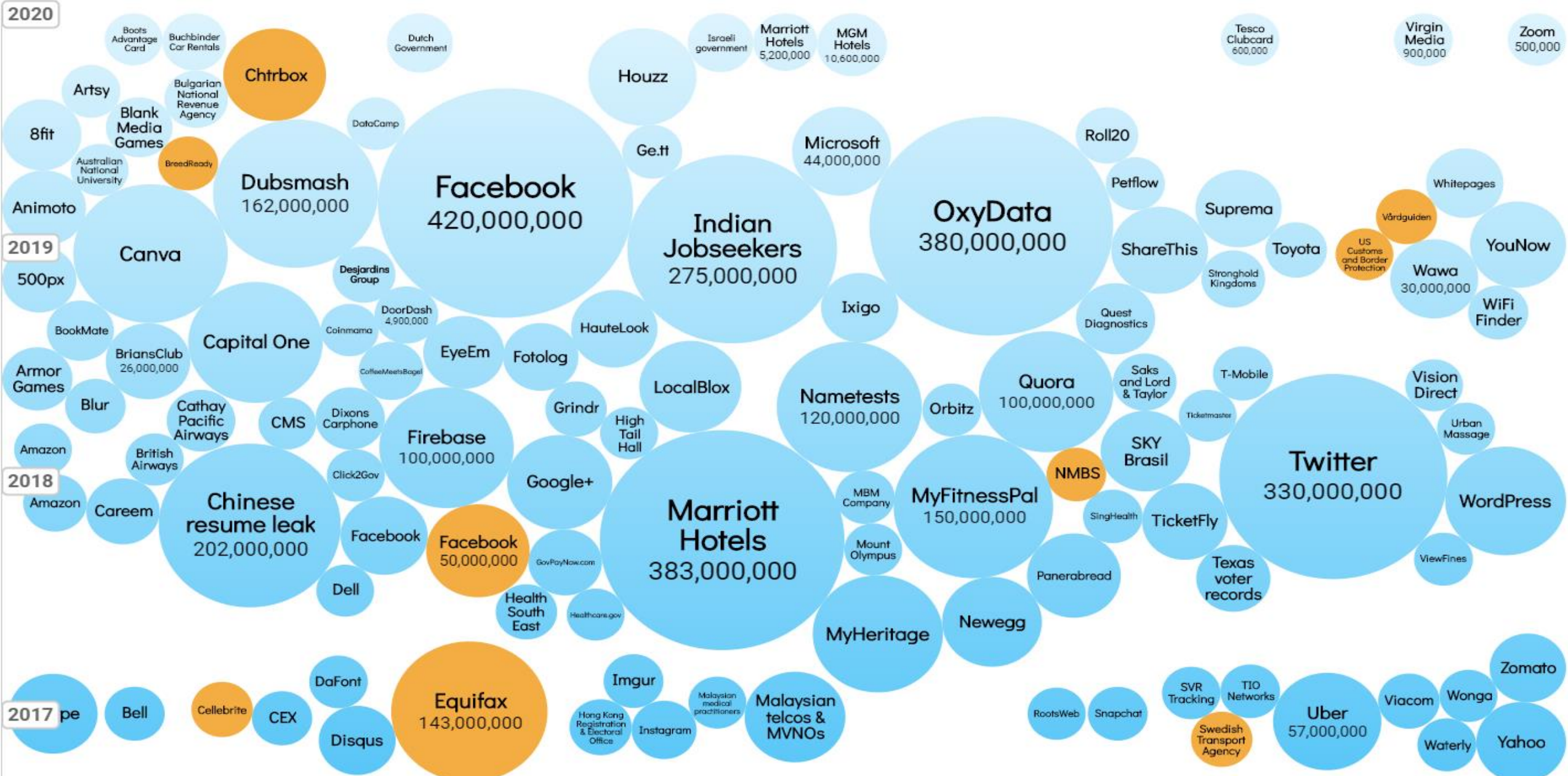


Average cost of breach 1st – Healthcare \$6.45M, 2nd – Financial \$5.86M

Why is this data so valuable

- Contains valuable information
- Data is a new form of currency
- Allow criminals to steal identities
- No transparency in data collected
- Data can be very expensive

Biggest Breaches



2020 so far...

- T-Mobile – Massive cell service provider
- Whisper – “Anonymous” secret-sharing app
- TrueFire – Online Guitar Lesson Website
- General Electric – Technology Conglomerate
- Marriot International – Hotel Conglomerate
- Key Ring – Digital wallet app
- San Francisco International Airport (SFO)
- Zoom – Web meeting Communications Provider
- Quidd – Online Market place
- Beaumont Health - Michigan’s largest healthcare system
- Facebook – Massive Social Media Conglomerate
- Paay – Card Processor Startup
- Nintendo – Game and Game System Conglomerate
- Ambry Genetics – Genetic Testing Lab
- Go Daddy – Web hosting and Domain Authority/SSL Cert Provider

2020 so far cont....

- Landry's – Restaurant Conglomerate
- Peekaboo Moments – Family Sharing App
- Hanna Anderson – Children's Clothing Retailer
- Microsoft – Biggest software company IN THE WORLD
- THSuite - Point-of-sale system provider
- Estee Lauder – Makeup Company
- Fifth Third Bank – Financial Institute, 1150 Branches
- Health Share of Oregon - Medicaid coordinated care organization
- MGM Resorts – Hotel Conglomerate
- PhotoSquared – Photography App
- SlickWraps – Online Tech Customization Store
- Walgreens – 2nd Largest US Pharmacy Chain
- Carnival Cruise Lines - one of the largest cruise ship operator
- J-Crew – Apparel Retailer
- Roblox – Online Gaming Platform

Biggest Breaches “the numbers”

Microsoft – 280M records

Estee Lauder – 440M records

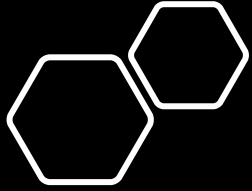
Fifth Third Bank – 30M records

Marriot International – 5.2M records

Facebook – 267M records

Paay – 2.5M records

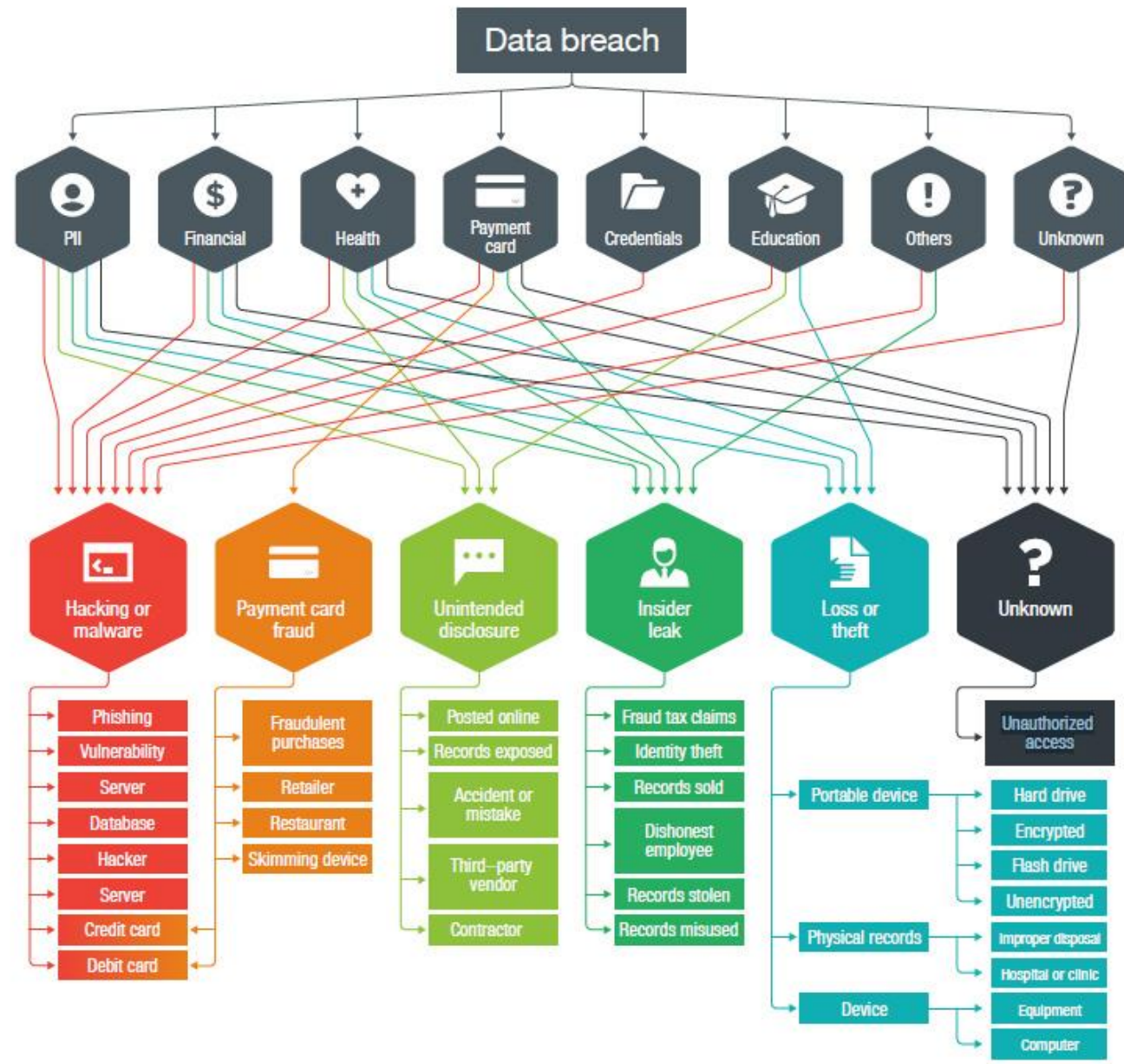




Data
Storage

Elasticsearch servers
SQL servers
Cloud services (AWS,
Azure, Google)

Attack Methods



Common Attack Avenues

- Malware Infections
- Criminal Insiders
- Social Engineering
- SQL Injections
- Cross-site Scripting
- Negligence
- Vulnerabilities not Previously Known
- Loss or Stolen
- Physical Records



Malware Infections

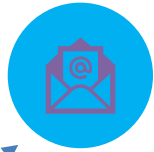
Malware is mal(icious)-(soft)ware that includes virus, ransomware, spyware, trojans

```
mirror_mod = modifier_ob.  
set mirror object to mirror.  
mirror_mod.mirror_object =  
operation == "MIRROR_X":  
mirror_mod.use_x = True  
mirror_mod.use_y = False  
mirror_mod.use_z = False  
operation == "MIRROR_Y":  
mirror_mod.use_x = False  
mirror_mod.use_y = True  
mirror_mod.use_z = False  
operation == "MIRROR_Z":  
mirror_mod.use_x = False  
mirror_mod.use_y = False  
mirror_mod.use_z = True  
  
selection at the end -add  
ob.select= 1  
modifier_ob.select=1  
context.scene.objects.active  
("Selected" + str(modifier_ob.  
mirror_ob.select = 0  
bpy.context.selected_object  
data.objects[one.name].select  
  
print("please select exactly  
  
-- OPERATOR CLASSES ----  
  
types.Operator):  
X mirror to the selected  
object.mirror_mirror_x"  
mirror X"  
  
context):  
context.active_object is not
```

Criminal Insiders

Employees, Contractors or 3rd Parties
who are trusted relationships





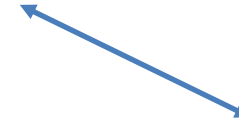
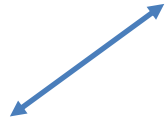
Phishing



Vishing



Impersonation




Hello James.Taylor,

A new document has been shared with you in OneDrive. Click the button below to access the document.

Thank you,
OneDrive Team

https://reasonablediscovery1-my.sharepoint.com/:b:g/personal/anne_reasonablediscovery_com/ewik5zvwjgh9ml2j0k6v1qy8b5kcms1oqsqr1wfi5vviw1q?e=Izqahl
Click or tap to follow link.

[View In OneDrive Business](#)



Free online storage for your files.
Microsoft respects your privacy. To learn more, please visit our website.
Microsoft Corporation, One Microsoft Way, Redmond, WA, 98052



Social Engineering

Physical Attacks or Impersonations

Attackers can pretend to be anyone from internal users to a third party wearing a high visibility jacket.

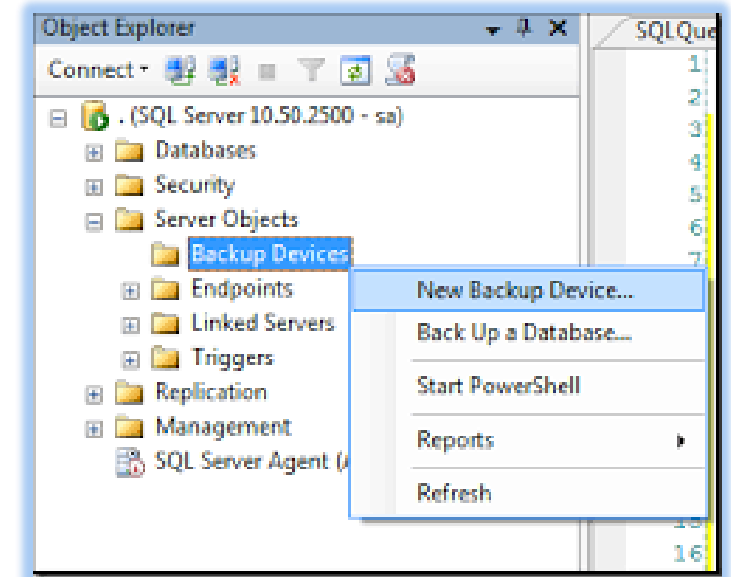
They may even attempt to break in with RFID cloning or even pick locks.

Will probably utilize Open-Source Intelligence (OSINT)



SQL Injection (SQLi)

Insertion of a Structure Query Language (SQL), Can Exploit and Read Sensitive Data



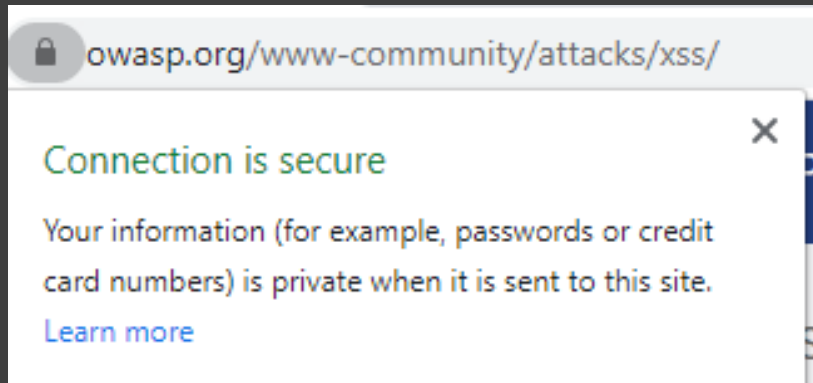
User ID:

ID: 1' union select 1,2 #
First name: admin
Surname: admin

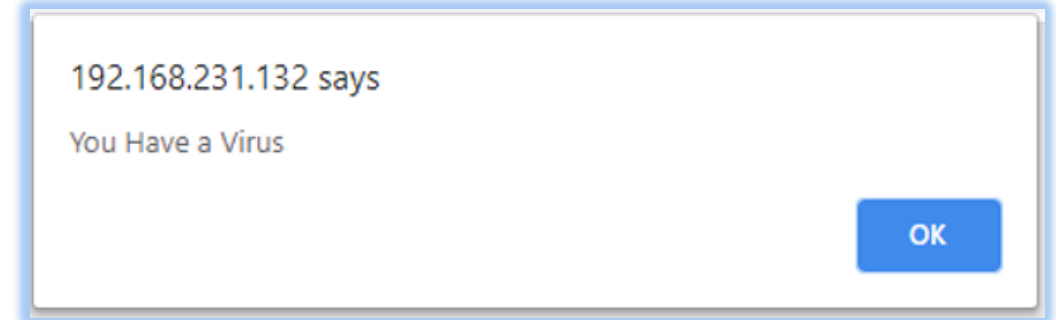
ID: 1' union select 1,2 #
First name: 1
Surname: 2

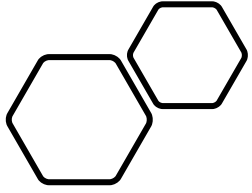
Cross-site Scripting (XSS)

Type of Injection Attack, Usually Web Browser Side



```
<script>alert("You Have a Virus")</script>
```

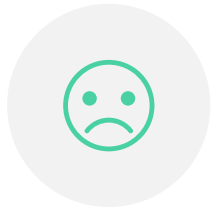




Negligence



BAD SECURITY
PRACTICES



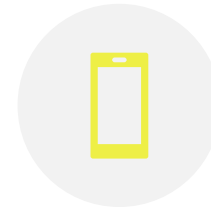
BAD BUSINESS
PROCESSES



SECURITY
FAILURES



ZERO DAY OR
KNOWN
VULNERABILITIES



LOST OR STOLEN
DEVICES



PHYSICAL
RECORDS

Where do data breaches go

pwndb

bitcoin:12cC7BdkBbru6JGsWvTx4PPM5LjLX8g49X - <3thx

```
SELECT /*+ MAX_EXECUTION_TIME(45000) */ id, luser, domain, password FROM lusers WHERE domain = ? LIMIT 200
```

26 rows.

0.29246997833252 seconds

Email

@ vantagepnt.com

=

email

Password

password

```
[luser] => terry.miller  
[domain] => vantagepnt.com  
[password] => walleye
```

24

Array

Deep Web

- Unindexed Websites
- Government Resource, Academic Info, Medical Records
- Still use .com, .edu, .org, etc.
- Can Use a standard Browser

Vs.

Dark Web

Unindexed Websites

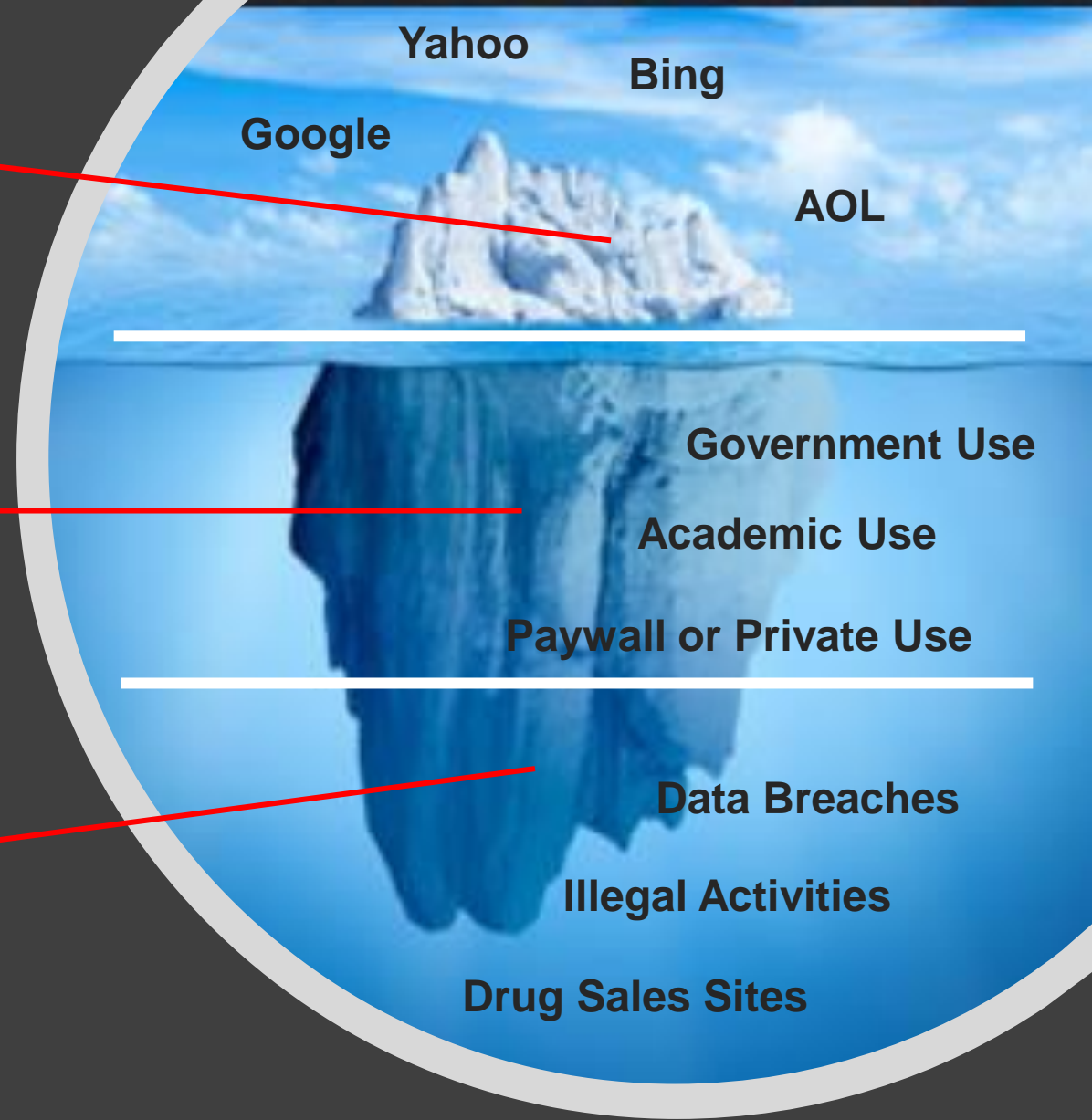
They are .onion sites not .com, .org etc.

Used the TOR browser to visit these sites

Surface Web 4%
of Content

Deep Web 90%
of Content

Dark Web 6%
of Content



breachalarm.com

!;--have i been pwned?

Check if you have an account that has been compromised in a data breach

hqnqdenver3rd@gmail.com

pwned?

haveibeenpwned.com

Good news — no pwnage found!

No breached accounts and no pastes (subscribe to search sensitive breaches)

3 Steps to better security

Start using 1Password.com

dehashed.com



Step 1 Protect yourself using 1Password to generate and save strong passwords for each website.



Step 2 Enable 2 factor authentication and store the codes inside your 1Password account.



Step 3 Subscribe to notifications for any other breaches. Then just change that unique password.



Future Attacks

Biometrics

Genetic Code

DNA Databases

Ways of Protecting Your Business

- **Create and Practice your IR/DR/BCP plan (Extensively)**
- **Robust and Tested Backup Plan**
- **Use of Encryption**
- **Employee Training**
- **Create and update a Hardware and Software Asset List**
- **Participate in Threat Sharing**
- **Mobile Device Management**
- **Compliance Adherence**
- **Third Party Internal Testing**
- **Vendor Management**
- **Password Management and Use**
- **Use 2FA**

Passwords vs. Passphrases

- Password = P@ssword1!
- Passphrase = MachineRiverDogPurple
- Use of Password Manager

The comic is divided into four panels. The top-left panel shows a password 'Tr0ub4dor &3' with annotations: 'UNCOMMON (NON-GIBBERISH) BASE WORD' for 'Troubador', 'ORDER UNKNOWN' for the sequence, 'COMMON SUBSTITUTIONS' for '0', '4', and '&', and 'NUMERAL' for '3'. It also notes 'PUNCTUATION' for '&3'. A note at the bottom says 'YOU CAN ADD A FEW MORE BITS TO COUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.' The top-right panel calculates '~28 BITS OF ENTROPY' and shows a search tree for 'Tr0ub4dor &3' with the calculation $2^{28} = 3 \text{ DAYS AT } 1000 \text{ GUESSES/SEC}$. It includes a note: '(PLAUSIBLE ATTACK ON A WEAK REMOTE WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)' and concludes 'DIFFICULTY TO GUESS: EASY'. The bottom-right panel shows a stick figure asking 'WAS IT TROMBONE? TROUBADOR. AND ONE THE 0s WAS A ZERO? AND THERE WAS SOME SYMBOL...' and concludes 'DIFFICULTY TO REMEMBER: HARD'. The bottom-left panel shows the passphrase 'correct horse battery staple' with annotations for 'FOUR RANDOM COMMON WORDS' and search trees for each word. The bottom-right panel shows a horse saying 'THAT'S A BATTERY STAPLE. CORRECT!' with a battery icon and concludes 'DIFFICULTY TO REMEMBER: YOU'VE ALREADY MEMORIZED IT'. The bottom-most panel contains the text: 'THROUGH 20 YEARS OF EFFORT, WE'VE SUCCESSFULLY TRAINED EVERYONE TO USE PASSWORDS THAT ARE HARD FOR HUMANS TO REMEMBER, BUT EASY FOR COMPUTERS TO GUESS.'

2FA and Authenticator Apps

- **Two Factor Authentication**
- These are normally 90 second unique time codes that are required after the correct username and password has logged in
- **Authenticators:**
 - Google
 - LastPass
 - Microsoft
 - Authy
 - Titan
 - Yubikey



Two-Factor Authentication



Two-factor authentication increases the security of your Ledyg account.

All you need is a compatible app on your smartphone, for example:

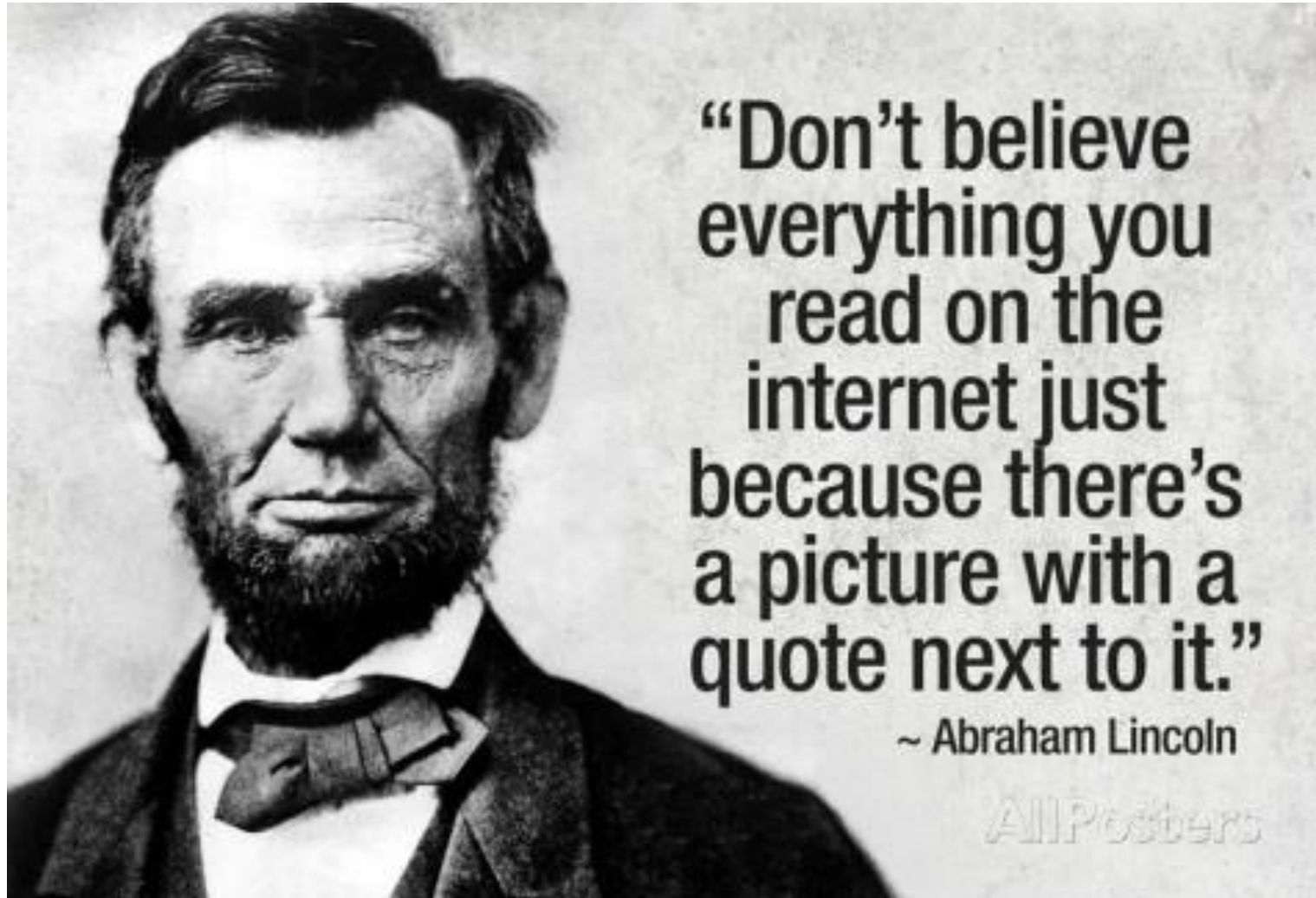
- [Google Authenticator](#)
- [Duo](#)
- [Authy](#)



Scan this image with your app. You will see a 6-digit code on your screen. Enter the code below to verify your phone and complete the setup.

123 456

Finish



Further Questions?

Email to get answers:

James.taylor@vantagepnt.com