MN ISACA

Information/Cyber Security Awareness

June 2020

Stop, Think, Connect

Be Aware or Beware

Think Before You Click

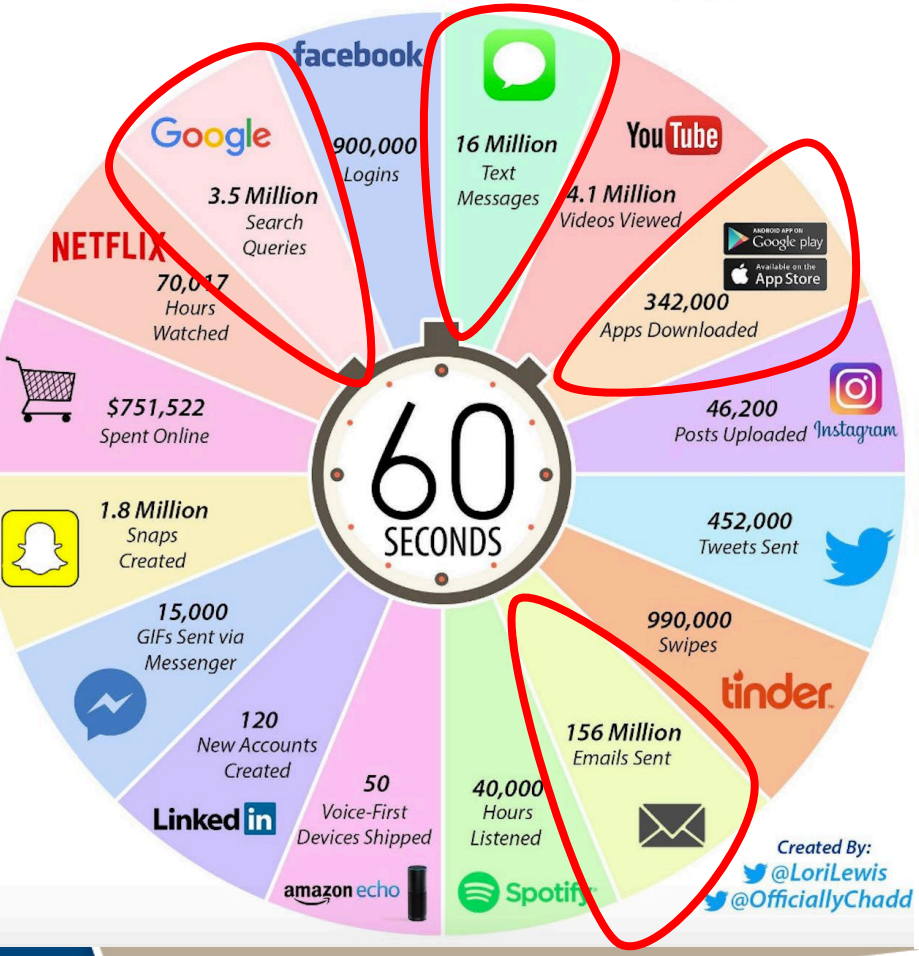
Make Security Part of Your DNA

Ken M. Shaurette
CISSP, CISA, CISM, CRISC, NSA IAM
FIPCO
Director InfoSec and Audit
kshaurette@fipco.com
(608) 441-1251

Some Key Takeaways

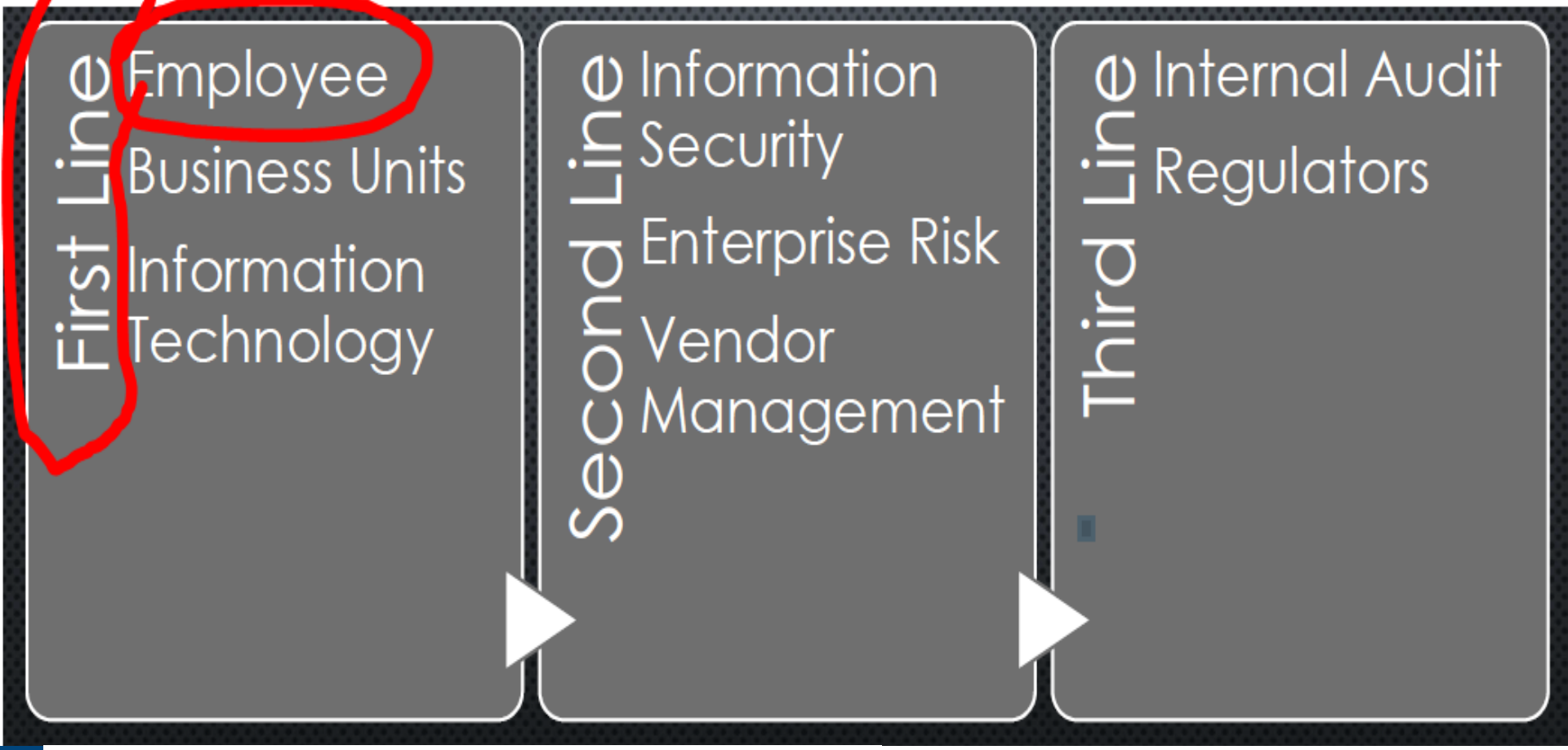
- When you leave today you will:
  - Be armed with resources to:
    - Educate the Board
    - Educate Employees – Make Security More User Friendly
    - Educate Customers
    - Learn Something Yourself
  - Better protect personal identity
  - Protect staff, customer's and partner's private information
  - Make better Cyber-Employee/Citizen?
  - Rate your personal exposure

2017 This Is What Happens In An Internet Minute



2019 This Is What Happens In An Internet Minute

The Three Lines of Defense!

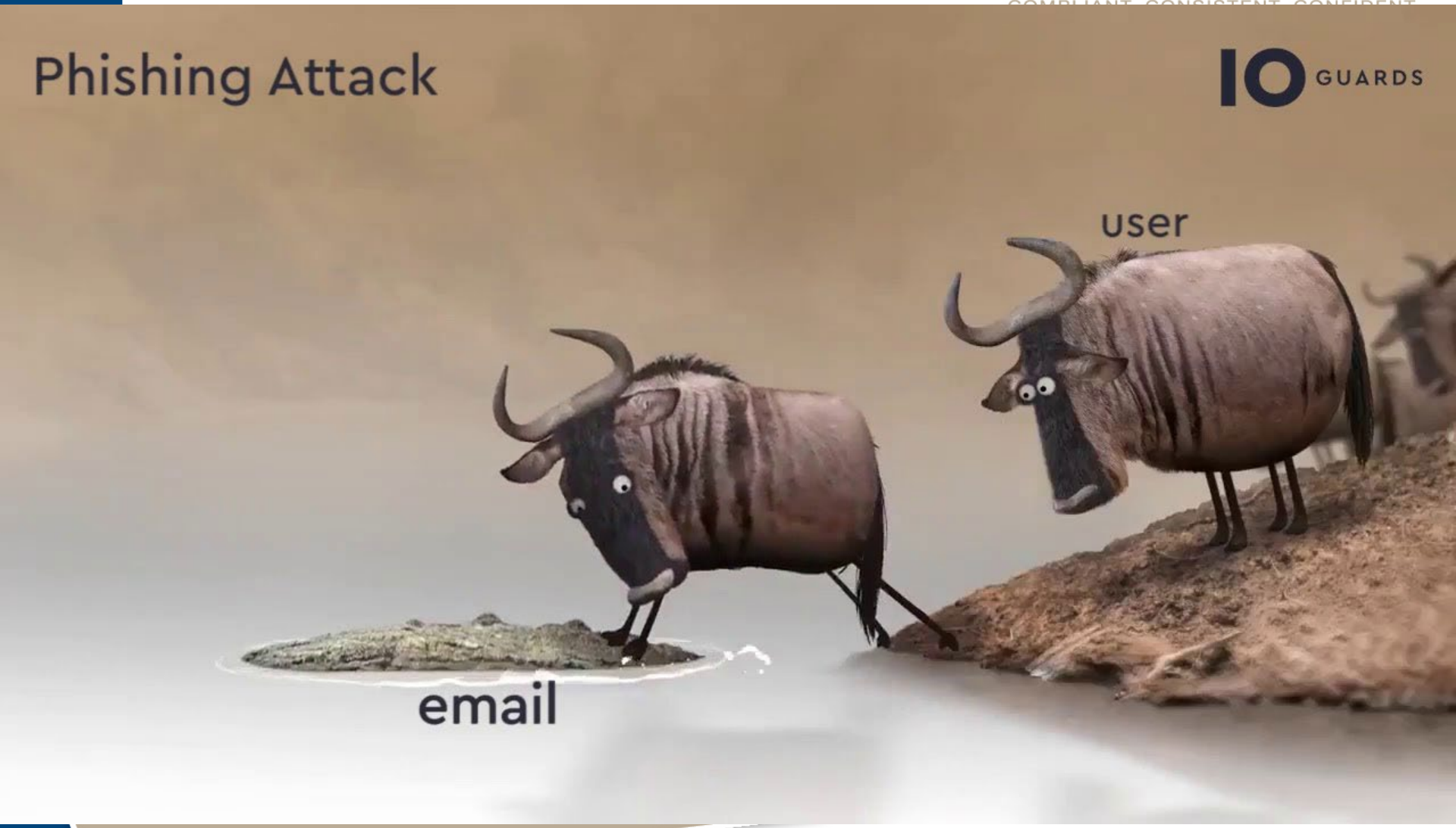


Thanks to Brent Maher – CISO Johnson Bank

Trojan Horses for The Mind

"When designed well, our messaging can sneak past mental defenses and noise. In other words, the way we design and deliver our messages can become a Trojan Horse."

- Perry Carpenter, InfoSec Island, 12/07, 2018



https://www.youtube.com/watch?v=yMnUEXhCenA

Do you Like Statistics / Metrics?

- Things to consider:
  - What is the purpose or the Metric?
  - Scare / FUD / Support for more staff?
  - Defend a project

Security Awareness Training - SAT (ROI)

Costs Before and After Security Awareness Training for 50-99 Employees

TOTAL COSTS PER EMAIL USER BEFORE SAT	$286.14

Source: Osterman Research, Inc.

TOTAL COSTS PER EMPLOYEE AFTER SAT	$136.17

Source: Osterman Research, Inc. 2018

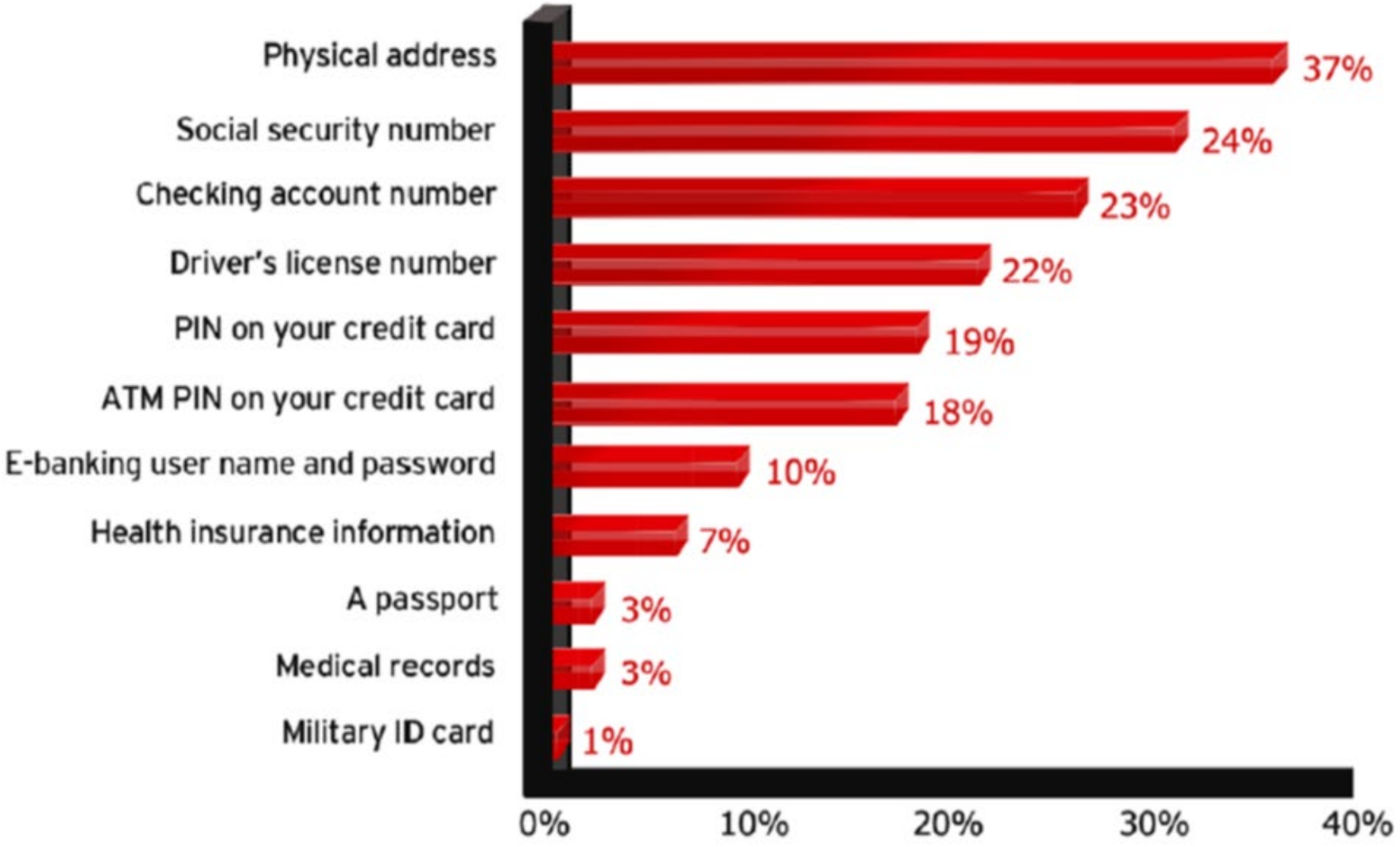
Trends in cyber attacks

ISSA

- Top 5 attacks by number of cyber insurance insurance claims as reported by AIG Insurance
  - Business email compromise – 23%
  - Ransomware – 18%
  - Data breach by outsider – 14%
  - Data breach by insider – 14%
  - Impersonation fraud – 8%
  - Denial of Service – 4%

2018

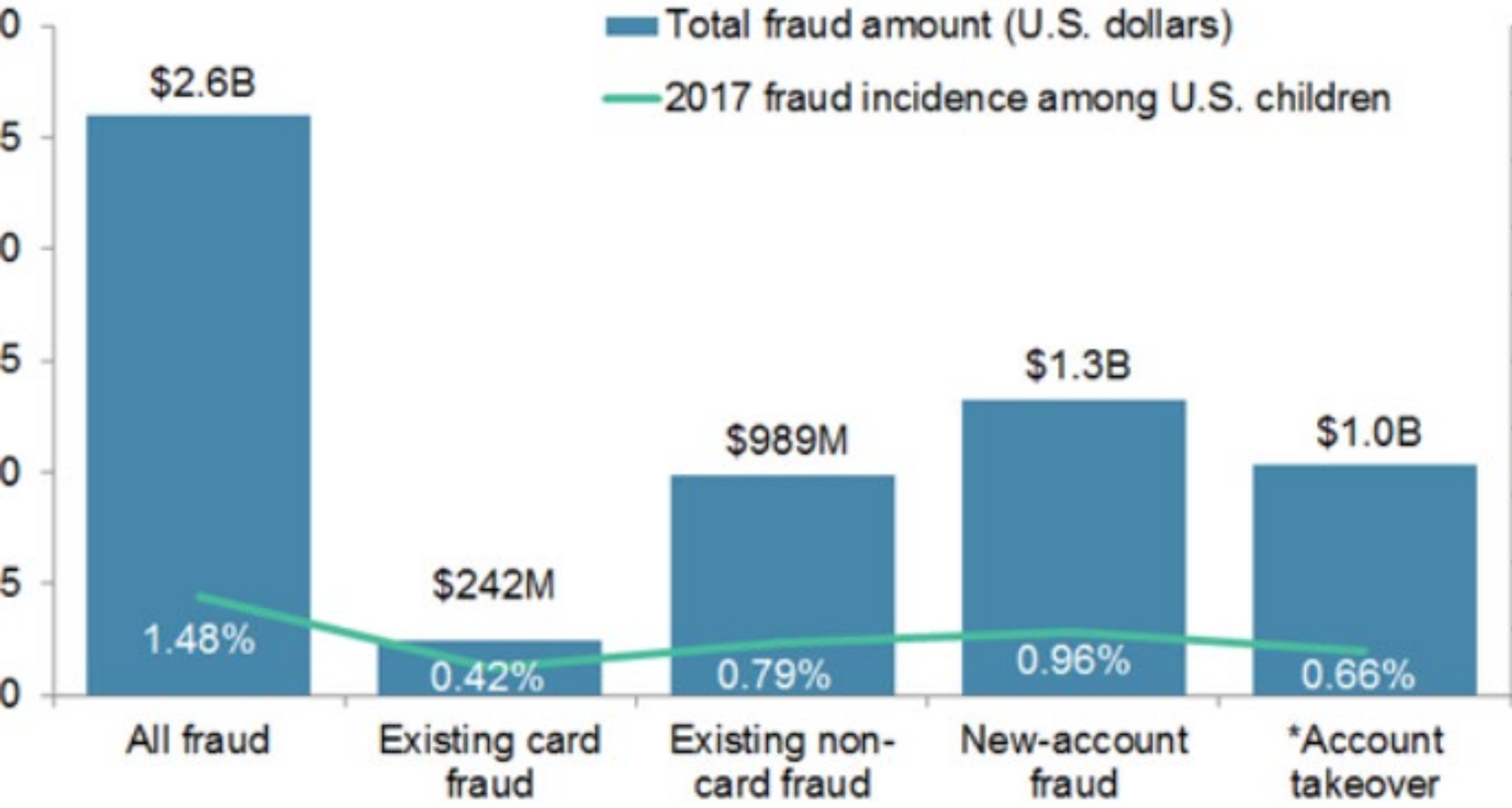
Business Breaches of Personal Information



Base = all fraud respondents;
n = 393; year = 2009
Source: Javelin Strategy & Research

https://www.javelinstrategy.com/

Fraud Against Children Totaled $2.6 Billion in 2017



elin Strategy & Research, 2018

What do you Consider in SAT?

Early in your Presentation

Provide definitions of key terms

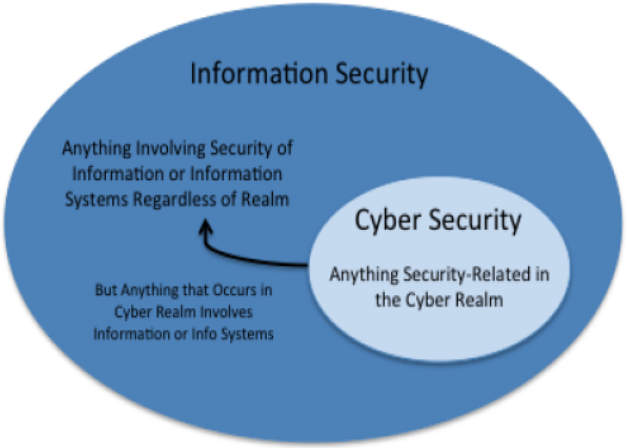
Definitions may seem obvious, TO YOU but don't assume people's understanding of terms……

Definitions

FIPCO
COMPLIANT. CONSISTENT. CONFIDENT.

Where Does Cybersecurity Fit

- **Cyber:** Of, relating to, or characteristic of the culture of computers, information technology and virtual reality.
- **Information Security:** is the practice of defending **information** from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction in order to provide confidentiality, integrity, and availability.
- **Cybersecurity:** The ability to protect or defend the use of cyberspace from cyber attacks.



Definitions (cont.)

- **Firewall**
  An application or hardware device installed either on your pc or between your pc and the internet that allows you to monitor and block unwanted traffic.

- **Skimming**
  Stealing information usually with a hardware device, Installed on an ATM or any card reader.

Definitions

- **Malicious Code - MALWARE**

(Virus - Spyware – Trojan – BOT – Ransomware)

Short for **malicious software**, is any software used to disrupt computer or mobile operations, gather sensitive information, gain access to private computer systems, or display unwanted advertising.[1]

Threats

Approach

How

- **Malware** : Short for **malicious software** is any software that does bad things to your computer.
- **Virus:** A computer program that can replicate itself and spread from one computer to another.
- **Scareware:** Scam software with malicious payloads or of no benefit, that are sold to consumers via certain unethical marketing practices.
- **Spyware:** A type of malware used to collect information without your knowledge.

Thanks to Peter Garancis – Commerce State Bank Awareness Presentation to Business

NIST Cybersecurity Framework

Information Security Awareness Crosses all Phases

https://www.us-cert.gov/ics/Assessments

Who Needs Awareness?

- Employees
- Customers
  - Business
  - Consumers
- Management
- Vendors
- Board
- Other

What Awareness?

- Employees
  - IRP
  - BCP/DR
  - Policy
  - Safe Computing Practices
  - Authentication Dos and Don’ts
  - Scam, Fraud and Alerts

What Awareness?

- Customers
  - Business
    - Email Compromise
    - Account Takeover
    - How to be aware for their customers
- Customers
  - Consumers
    - Scams, Alerts
    - Identity Theft Resources
    - ATM, Debit, Credit Card Safety

What Awareness?

- Vendors
  - Policy, Procedure and Standards
  - Incident Response / Security Breach
  - Authentication – remote access

What Awareness?

- Management
  - Everything you train everyone else
- Board : https://www.csbs.org/cyber101 (good for more than banking)
  - Cybersecurity (Information Security with a Twist)
    - NIST CSF
  - Information Security Program
    - Ongoing Posture
    - Scams, Incidents, Threat Intelligence
    - Annual Update
    - How can the Board help your InfoSec Program be successful?

Scams - Alerts

FIPCO
COMPLIANT. CONSISTENT. CONFIDENT.

Example:

DataSpii data leak Browser extensions impacting Chrome and Firefox

8 browser Extensions stealing information!!!!

---- NEXT PAGE ----

https://lifehacker.com/uninstall-these-eight-browser-extensions-that-stole-dat-1836539093

Scam Information

The extensions in question include for Chrome:

- Hover Zoom – 800,000+ users
- SpeakIt! – 1.4+ million users
- SuperZoom – 329,000+ users
- FairShare Unlock – Over 1 million users
- PanelMeasurement – Over 500,000 users
- Branded Surveys – 8 users
- Panel Community Surveys – 1 user

Scam Information

Extensions of Concern:

For Firefox:

SuperZoom – 329,000+ users

SaveFrom.net Helper – Around 140,000 users

FairShare Unlock – Over 1 million users

UPDATE 6/22/2020 –

Malicious Extensions Downloaded 30 Million Times Found In Chrome Web Store

https://www.sosdailynews.com/news.jspx?&articleid=827D2290EF3A47CDA4916669CA91DB13&sx=79

FIPCO
COMPLIANT. CONSISTENT. CONFIDENT.

Where the Attack Threat Starts

- Deception and Technology Tricks
  - Social Engineering = Persuasion
  - Infected websites…..
  - Look for weak practices to get into places
  - Hackers expect people not to be familiar with weak areas of our technology and practices

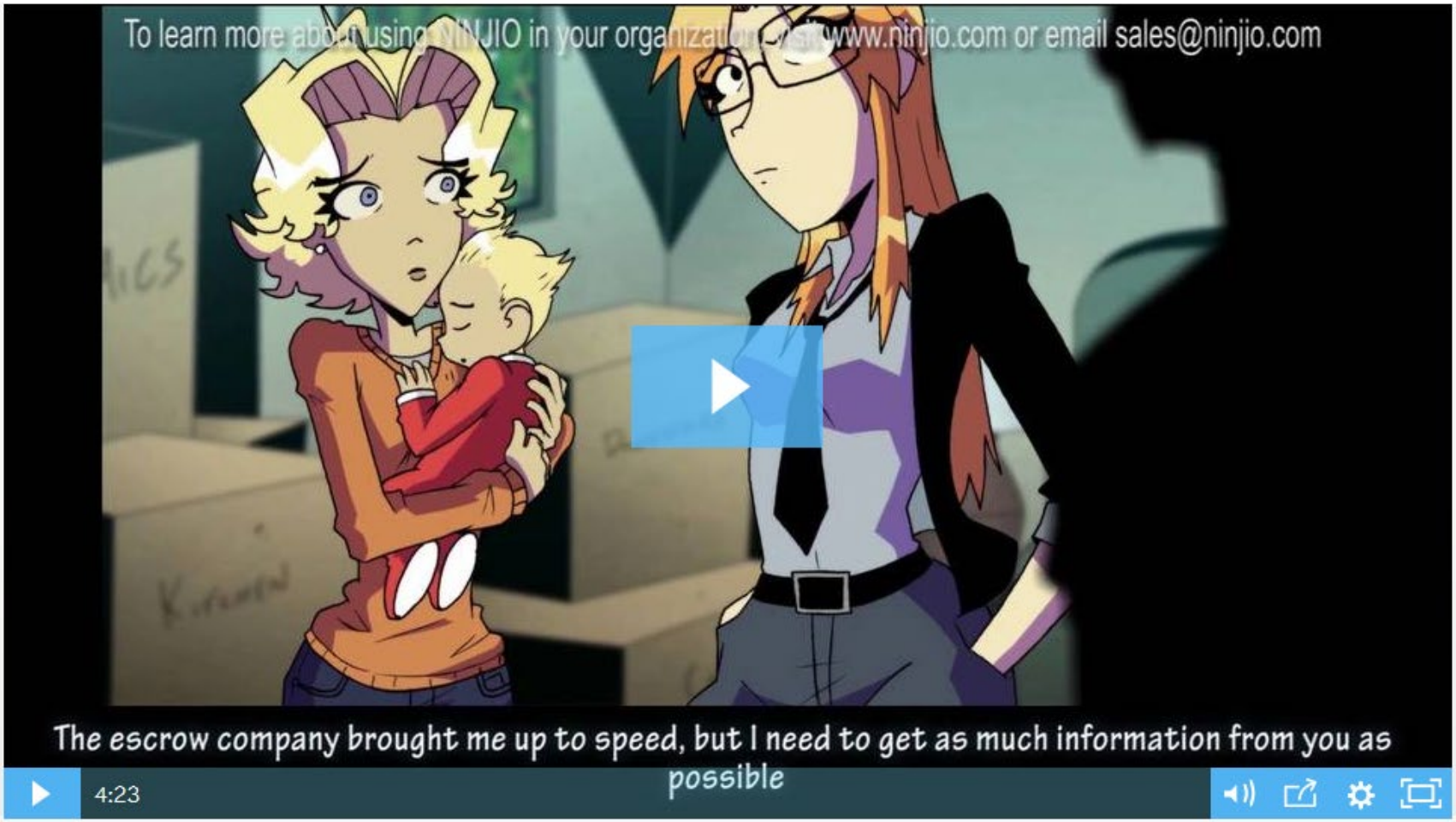
Phishing..... (3 min - crooks)

https://www.youtube.com/watch?v=sed6rtDBuHk

This Has happened?

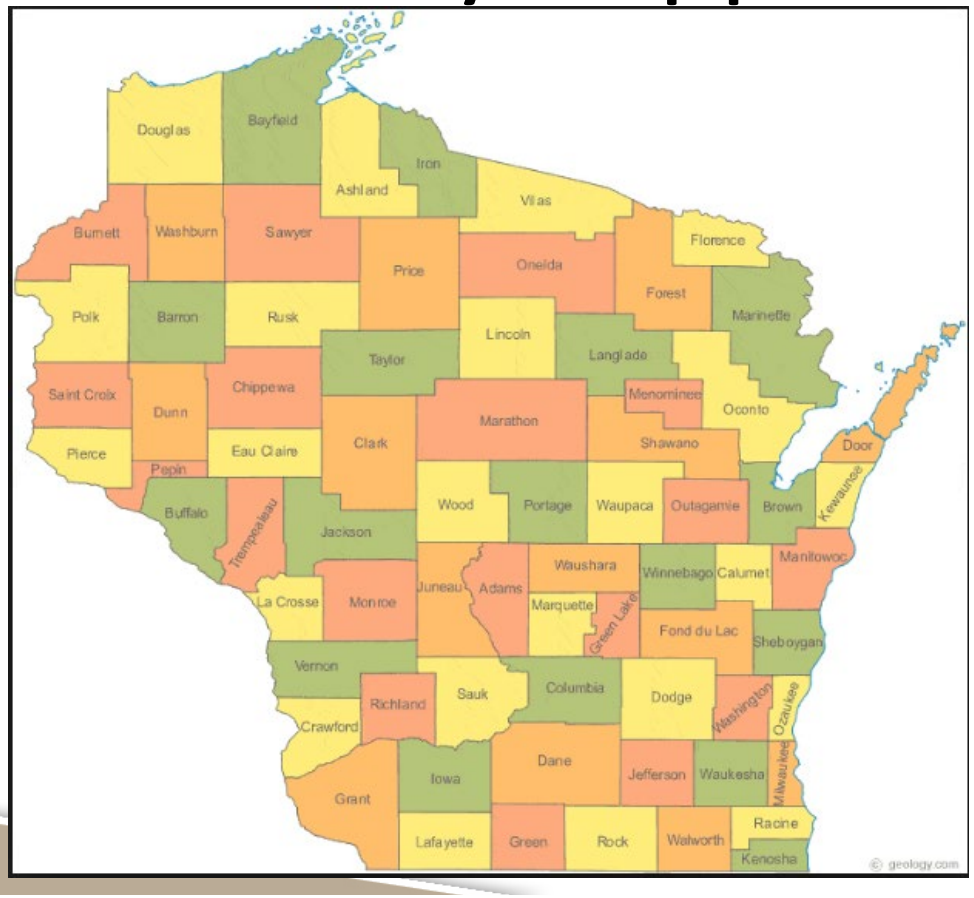
FIPCO
COMPLIANT. CONSISTENT. CONFIDENT.

NINJIO



NINJIO AWARE S2-E2 - The Homeless Homebuyer www.ninjio.com/ep202

Are Scams Really Happening?



https://www.bbb.org/scamtracker/us

ATM Skimming….

https://www.youtube.com/watch?v=gJo9PfsplsY

http://www.identitytheft.info/personalsecurity.aspx

Awareness…

Know your rights!

- Banks and legitimate organizations do not typically collect confidential information using email.
- You can always go direct to the organization like your bank to make sure it is legitimate.
- Be Cautious, Be Paranoid, Be Careful!!
- Beware & Be very Aware

Does Shock & Awe Work? (FUD)

- Consider how fear would impact delivery of a message.
- Fear, Uncertainty and Doubt (FUD)
- Reward versus the Big Stick

Passwords Still The Keys To the Kingdom

- Minimize Reuse of Passwords
  - Don't use your Corporate Passwords at home or vice versa, separate passwords….

    1. Banking (One for the Money)
    2. Entertainment (Two for the Friends)
    3. Email (Three for the Email)
    4. For the Corporation (at work)

- Use Password Vaults (aka Password Managers)
  - Lastpass, 1Password, Dashlane, Keepass, etc..

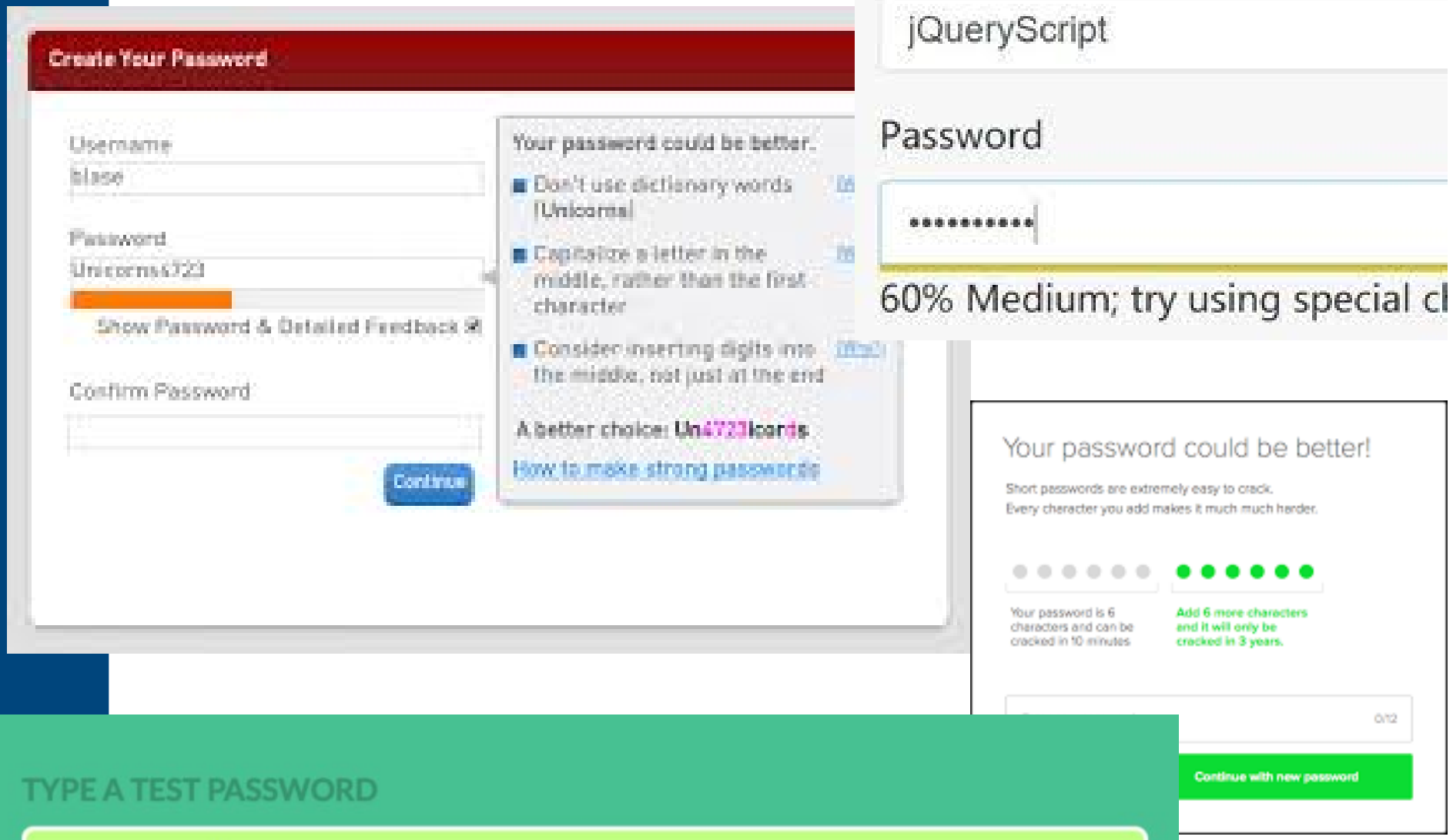
https://www.digitaltrends.com/computing/best-password-managers/
https://www.pcmag.com/roundup/300318/the-best-password-managers
https://www.wired.com/story/best-password-managers/

Create strong passwords

Which passwords are weak?

Don’t Trust Password Strength Meters

WHY?


Create Your Password
Username
blase
Password
Unicorns4723
Show Password & Detailed Feedback
Confirm Password
Continue
Your password could be better.
Don't use dictionary words (Unicorns)
Capitalize a letter in the middle, rather than the first character
Consider inserting digits into the middle, not just at the end
A better choice: Un4723icorns
How to make strong passwords
Username
jQueryScript
Password
60% Medium; try using special cl
Your password could be better!
Short passwords are extremely easy to crack.
Every character you add makes it much much harder.
Your password is 6 characters and can be cracked in 10 minutes
Add 6 more characters and it will only be cracked in 3 years.
Continue with new password
TYPE A TEST PASSWORD
Show password
Strength: strong

FIPCO
COMPLIANT. CONSISTENT. CONFIDENT.

Create strong passwords

Which passwords are weak?

8 Characters?

Even with Special Characters

WEAK

Create strong passwords

Which passwords are weak?

!lov3you

Or

BlueChristmasCar

Neither One or potentially BOTH

Password: !lov3you

Strength: 43%

Evaluation: Medium

Password properties

Property	Value	Comment
Password length:	8	MEDIUM LONG
Numbers:	1	USED
Letters:	6	USED
Uppercase Letters:	0	NOT USED
Lowercase Letters:	6	USED
Symbols	1	USED
Charset size	68	HIGH (symbols, a-z, 0-9)
TOP 10000 password	NO	Password is NOT one of the most frequently used passwords.

Brute-force attack cracking time estimate

Machine	Time
Standard Desktop PC	About 2 months
Fast Desktop PC	About 13 days
GPU	About 5 days
Fast GPU	About 3 days
Parallel GPUs	About 6 hours
Medium size botnet	5 seconds

http://password-checker.online-domain-tools.com/

Oh no - !lov3you — pwned!
This password has been seen 39 times before.

This password has previously appeared in a data breach and should never be used. If you've ever used it anywhere before, change it!

https://haveibeenpwned.com/Passwords

Password:	BlueChristmasCar
Strength:	91%
Evaluation:	Excellent!

Password properties

Property	Value	Comment
Password length:	16	OK
Numbers:	0	NOT USED
Letters:	16	USED
Uppercase Letters:	3	USED
Lowercase Letters:	13	USED
Symbols	0	NOT USED
Charset size	52	MEDIUM (A-Z, a-z)
TOP 10000 password	NO	Password is NOT one of the most frequently used passwords.

Brute-force attack cracking time estimate

Machine	Time
Standard Desktop PC	About 11 trillion years
Fast Desktop PC	About 3 trillion years
GPU	About 1 trillion year
Fast GPU	About 551 billion years
Parallel GPUs	About 55 billion years
Medium size botnet	About 11 million years

http://password-checker.online-domain-tools.com/

Create strong passwords

Which passwords are strong?

THINK LONG

Uncompromised as STRONG

15 characters +

STRONG

Even a 50 character password isn't secure if it was previously compromised

https://nakedsecurity.sophos.com/2015/03/02/why-you-cant-trust-password-strength-meters/

Make Security More User Friendly

https://www.grc.com/haystack.htm

How Big is Your Haystack?

... and how well hidden is **YOUR** needle?

If every possible password is tried, sooner or later yours **will** be found.
The question is: Will that be **too** soon . . . or **enough** later?

… Users have to help!!!!!!!

2015 Before Equifax

2017 After Equifax

https://www.youtube.com/watch?v=opRMrEfAIiI
https://www.youtube.com/watch?v=UzvPP6_LRHc

Have you Ever?

- **Received Spam email that contains your password**
  - It's asking me to send money.
  - What should I do?

555,278,657 real world passwords exposed in data breaches.

This exposure makes them unsuitable for ongoing use

https://haveibeenpwned.com/Passwords

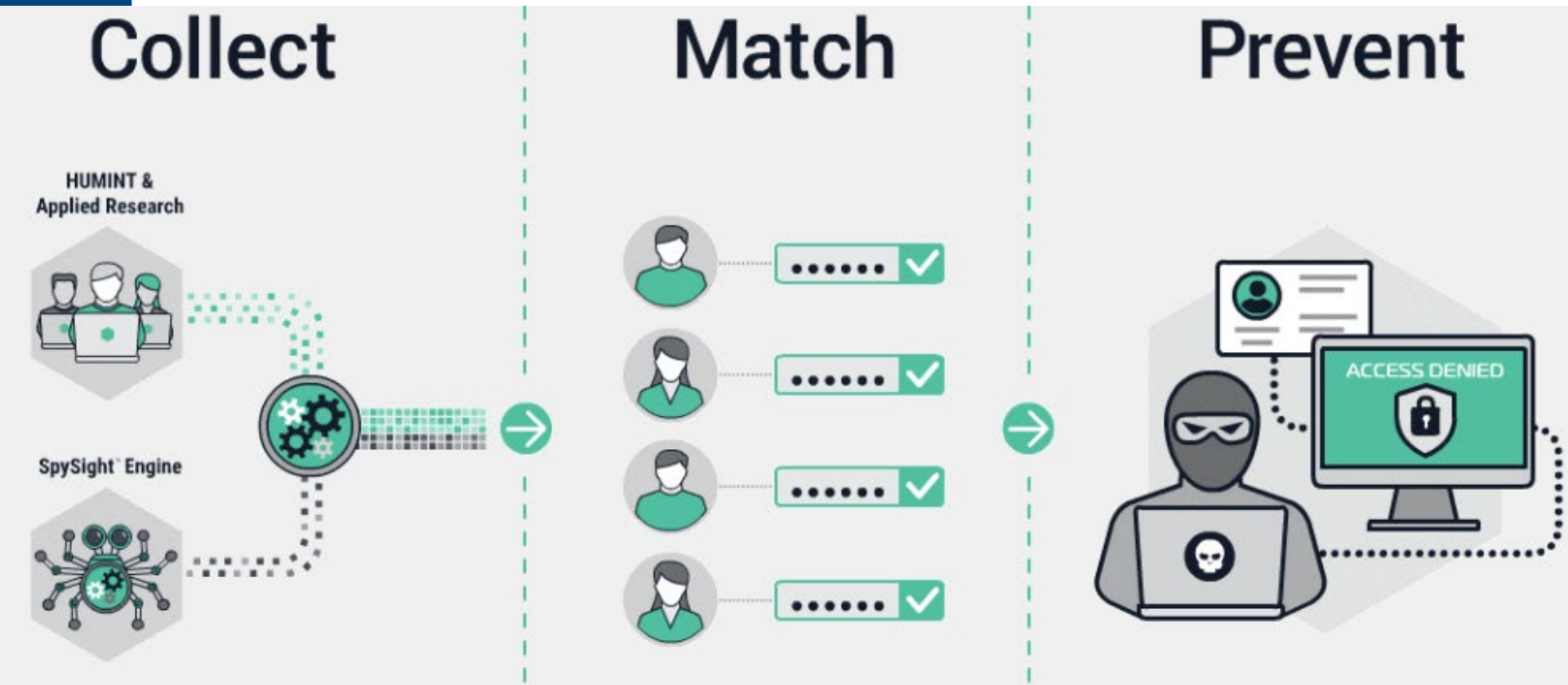
Passwords Still The Keys To the Kingdom

- Minimize Reuse of Passwords
  - Don't use your Corporate Passwords at home or vice versa, separate passwords….

    1. Banking (One for the Money)
    2. Entertainment (Two for the Friends)
    3. Email (Three for the Email)
    4. For the Corporation (at work)

- Use Password Vaults (aka Password Managers)
  - Lastpass, 1Password, Dashlane, etc..

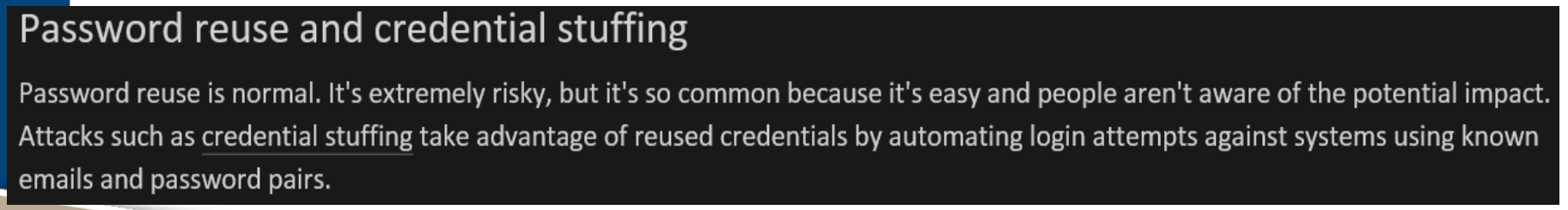
https://www.digitaltrends.com/computing/best-password-managers/
https://www.pcmag.com/roundup/300318/the-best-password-managers
https://www.wired.com/story/best-password-managers/


Collect
Match
Prevent
HUMINT &
Applied Research
SpySight Engine
ACCESS DENIED

Testing Exposure of Passwords

https://portal.spycloud.com
https://monitor.firefox.com/
https://haveibeenpwned.com/

Verizon's Data Breach Report showed that **81% of hacking-related breaches** used stolen or weak passwords.



https://enterprise.verizon.com/resources/reports/dbir/

Some Examples…..

Other Breach and Fraud Detection Tools:

- Truidentify.com (Transunion)
- Kroll - enroll.idmonitoringservice.com
- Discover Card
- Other Credit Cards – Capital One

Some Examples.....

You've been pwned!

You signed up for notifications when your account was pwned in a data breach and unfortunately, it's happened. Here's what's known about the breach:

Email found:	kshaurette@fipco.com
Breach:	db8151dd
Date of breach:	20 Feb 2020
Number of accounts:	22,802,117
Compromised data:	Email addresses, Job titles, Names, Phone numbers, Physical addresses, Social media profiles
Description:	In February 2020, a massive trove of personal information referred to as "db8151dd" was provided to HIBP after being found left exposed on a publicly facing Elasticsearch server. The exposed data could not be attributed to an owner and appears to be related to a CRM which aggregated personal information and customer interactions. The data was provided to HIBP by dehashed.com.

Some Examples…..

- Make passwords strong – **Long is Strong**
- Keep them private
- Use unique passwords

As a Company:

Password Policy Enforcers

Personally and as a Company

Password Managers

NIST Guidelines – SP800-63a-c

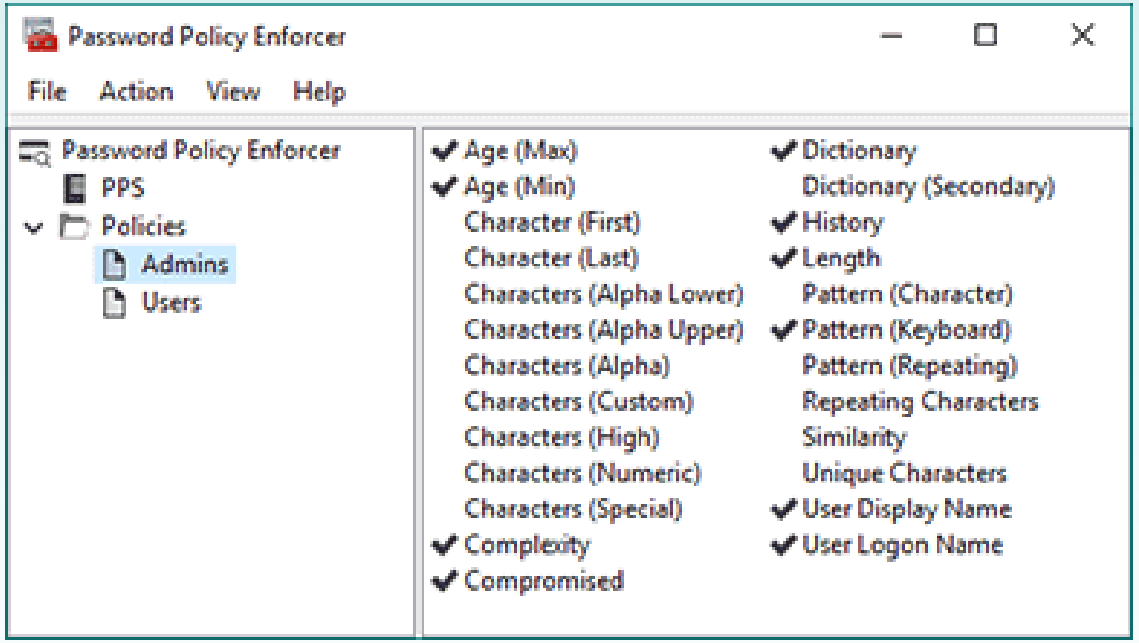
Password Policy Enforcer

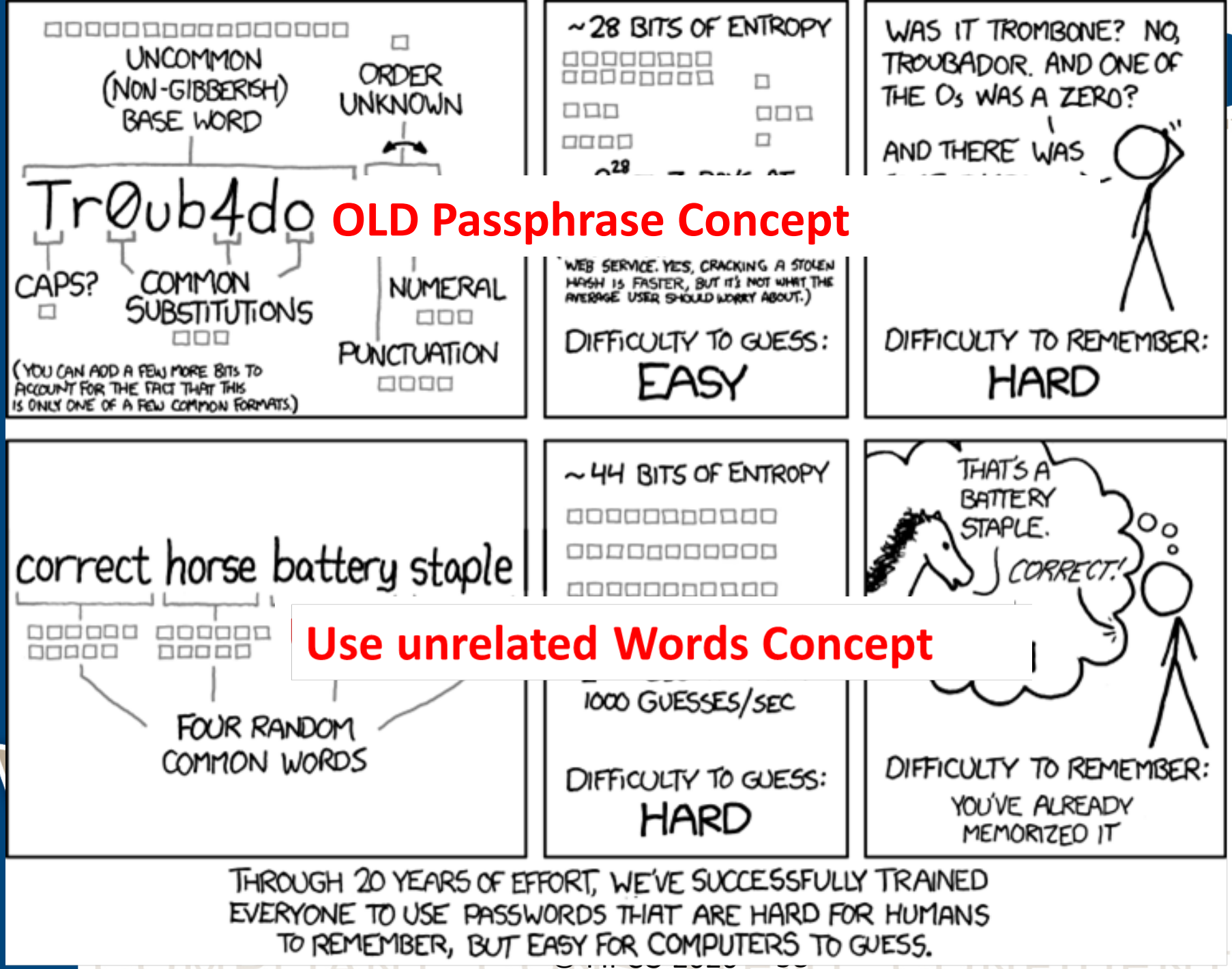
Create and enforce a password policy

Enforce granular password policies to protect Active Directory from password attacks.

Granular password policies for Windows

Password Policy Enforcer improves security by ensuring that users choose strong passwords. PPE checks new passwords for compliance with your password policy and immediately rejects non-compliant passwords.




UNCOMMON (NON-GIBBERISH) BASE WORD
ORDER UNKNOWN
Tr0ub4do
CAPS?
COMMON SUBSTITUTIONS
NUMERAL
PUNCTUATION
(YOU CAN ADD A FEW MORE BITS TO ACCOUNT FOR THE FACT THAT THIS IS ONLY ONE OF A FEW COMMON FORMATS.)
~28 BITS OF ENTROPY
WEB SERVICE. YES, CRACKING A STOLEN HASH IS FASTER, BUT IT'S NOT WHAT THE AVERAGE USER SHOULD WORRY ABOUT.)
DIFFICULTY TO GUESS:
EASY
WAS IT TROMBONE? NO, TROUBADOR. AND ONE OF THE Os WAS A ZERO?
AND THERE WAS
DIFFICULTY TO REMEMBER:
HARD
OLD Passphrase Concept
correct horse battery staple
FOUR RANDOM COMMON WORDS
~44 BITS OF ENTROPY
1000 GUESSES/SEC
DIFFICULTY TO GUESS:
HARD
THAT'S A BATTERY STAPLE.
CORRECT!
DIFFICULTY TO REMEMBER:
YOU'VE ALREADY MEMORIZED IT
Use unrelated Words Concept
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.

Shifting Gears Again

Preventing CyberSpying…..

- Look around you right now. Do you have a camera or your laptop nearby? How about your cell phone? If so, who's watching you?

CLICK HERE

Fox Contact 6: Cyber Spying

Cyber Criminal Motives

- Money
- Politics
- Personal Recognition
- Identity Theft
- Knowing They Can

It's Worth More

- An identity is stolen every 4 seconds in the US.
- The average cost to restore a stolen identity is $8,000.
- Victims spend an average of 600 hours recovering from this crime.
- Lose once likely to lose again

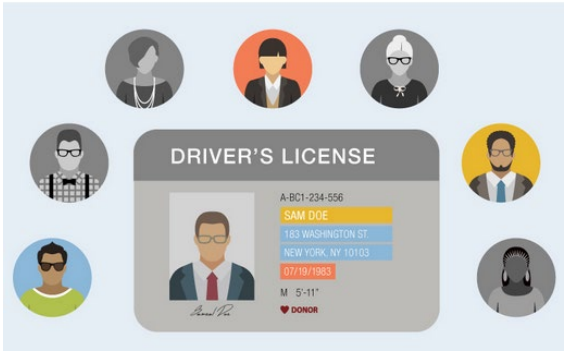
Criminal Identity Theft

Synthetic IDs: Great For Fraudsters, Bad For Victims

Identity theft… without your full identity

It's called synthetic identity theft. Whether by a phishing scam, data breach, hack or physical theft, your information becomes compromised and falls into the wrong hands. Criminals use this stolen information to mix and match names, birthdays, Social Security numbers and addresses with other fabricated information to create synthetic IDs.

Once the synthetic identity is made, criminals can make fraudulent charges to your bank account, open new lines of credit, order prescriptions and even commit crimes under your name.



https://www.fightingidentitycrimes.com/synthetic-ids-great-for-fraudsters-bad-for-victims/

Criminal Identity Theft

http://www.identitytheft.info/criminal.aspx

Cyber Criminal Methods

- Review Web Sites
- Search Internet for information
- Call and email the Bank attempting to trick us
- Read our trash, desktops, and workspace area
- Look for weaknesses in Bank technology,

  And People!!
- Look for weakness in Bank change and configuration management practices

Personalize the Message

- If an employee handles data like it is their data or that of their family they will treat it well.
- If an employee uses Facebook, Instagram or Pinterest etc.. Safely; they will likely be a safe Online Banker or employee.

Ways That Employees Can Contribute

- **Do not:**
  - Use Bank e-mail ID's for non-business use
    - Reuse your passwords on multiple websites to log in regardless if you use a different user account
  - Share accounts and passwords with ANYONE

Identity Theft Protection Tips

Always use strong passwords

We all have a lot of passwords to remember, but are yours strong enough? Strong passwords generally have a minimum of eight characters and include a mix of upper and lowercase letters, numbers and special characters. Avoid using passwords that are easy to guess—these include birthdays, addresses, phone numbers, and even pet names.

https://www.equifax.com/personal/education/identity-theft/?Et_cid=554678&Et_rid=46007779

Identity Theft Protection Tips

Be alert for phishing schemes

Phishing messages are used by scammers to trick you into clicking a link or attachment in an email or text that will provide scammers access to your personal information. Phishing messages can download malware onto your computer to snare your personal or financial information. You should carefully review the email address of the sender to determine if you have an account with the business or know the individual sending the email or text before opening an attachment or link.

https://www.equifax.com/personal/education/identity-theft/?Et_cid=554678&Et_rid=46007779

Identity Theft Protection Tips

Carefully dispose of documents that contain personal information

Bank and credit card statements, pre-approved credit card offers and other papers and mail with your personal information may be tempting to identity thieves and can be taken from your mailbox or trash. Be sure to destroy these sensitive documents and cross-shred, if possible.

https://www.equifax.com/personal/education/identity-theft/?Et_cid=554678&Et_rid=46007779

Employee
Actions That Make a Difference

- Appropriate Use Policy– What you should and shouldn't do with technology systems (Computers, Laptops, notebooks, Cell Phones, Printers)
- Security Responsibility – How you can contribute to Bank success in protecting information and systems

Employee
Actions That Make a Difference

- Password Usage – Ways to protect your password and identity
- Internet Usage – Ways you can protect yourself while on the Internet
- Email Usage – Ways that you can protect information while using email
- Careful where you Surf – Websites that is!

Encourage Participation

Ways That You Can Contribute

Do not:

- Open *unexpected* e-mail attachments, *even if they are from someone you know – danger of imposters – phishers*
- Open attachments of types that are not of common types
- Respond to spam, **do not "unsubscribe"**

Testing and training with tools like ThreatAdvice LMS

Ways That You Can Contribute

Do not:

- Send non-public data through email or other technology unless it is encrypted
- Visit Internet sites that could cause systems harm
- Install non-credible software from any website
  - Keep this in mind with Mobile Apps

Ways That You Can Contribute

- Guard against being deceived or accidentally disclosing information

  Do Not:

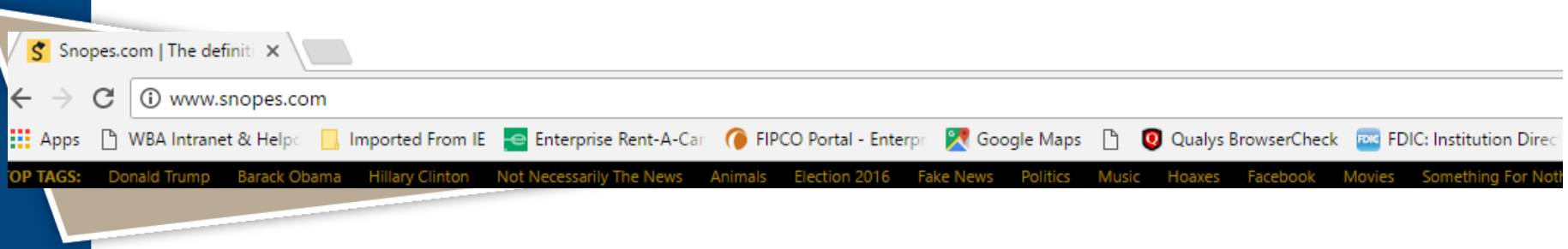
  - ❖ Give Out Personal Information Over the Phone
  - ❖ Ask for personal computer information from another co-worker
    (There are special circumstances. Verify Requestor)
  - ❖ Let unrecognized guests go without escort

Ways That You Can Contribute

- Protect Paper Copies

  Do Not:

  - ❖ Throw away non-public information without shredding
  - ❖ Leave unattended for a long period of time
  - ❖ Provide to Third-Party unless approval has been obtained



Answers – Caution & Paranoia

- Hopefully you weren't looking for an answer to protect you from you.
- The industry doesn't have a technology answer yet, but you can be either part of the solution or part of the challenge.
- Be Aware & Beware

Teach Phishing

- Do’s and Don’ts

https://www.phishing.org/what-is-phishing

Phishing Attacks Dos and Donts

Five DO's:

1. **Review the email for grammar and spelling**
   While many attackers have improved over the years, some attacks still have pretty noticeable misspellings and other grammatical errors. Abnormal spacing and formatting may also be a sign of a phishing email.
2. **Inspect the links**
   Attackers will embed malicious URLs into seemingly legit ones within their emails. Use the mouse to hover over the hyperlink to determine if there is an embedded URL.
3. **Validate the request**
   If you receive an email from a fellow employee or vendor requesting information, pick up the phone and verify the request. Always use contact numbers from external websites – NOT the ones included in the potential phishing email.

Phishing Attacks Dos and Donts

Five DO's:

4. **Alert the appropriate personnel**
   If you think you have received a phishing email, getting it to the proper person in the IT department is critical. They may be able to block others from receiving it or block access to any links that were included in the phishing email. Don't hesitate to forward suspicious emails to the appropriate IT staff!
5. **Use common sense**
   If a vendor of three years has never asked for your password information through email, they probably wouldn't be starting today. If a coworker of two years has never sent you an attachment and sends you one today and tells you to enable macros, don't. Question requests that are outside the norm and use common sense when fulfilling requests.

Phishing Attacks Dos and Donts

Five Don’ts:

1. **Don’t trust the sender**

   It doesn’t take any time or skill to “spoof” or impersonate the sender of an email. From the president of your organization to the President of the United States, attackers can assume the identity of anyone.

2. **Don’t be so quick to reply**

   Sometimes attackers are just looking to find valid email addresses within an organization or to identify the naming convention used within an organization. By replying to an email like this, even if it’s only to give the would-be attacker a piece of your mind, you only help the attacker determine that the email reached a recipient.

3. **Don’t open that attachment**

   Attachments that were once thought of as harmless (Word, Excel, PDF) are now being used to launch various types of attacks against end-users. If you weren’t expecting that attachment – don’t open it!

Phishing Attacks Dos and Donts

Five Don’ts:

4. **Don’t give out personal information**

   Most companies will not ask you to transmit personal information, account information, or account passwords via email. Any requests similar in nature should raise suspicions and be reported.

5. **Don’t be embarrassed**

   These attacks work, which is why we’ve seen an increase in the amount of phishing attacks. Don’t be embarrassed that you fell for it. Don’t try to fix it yourself. Don’t assume you’ll be in trouble. Alert the appropriate IT personnel immediately and wait for further instructions. The faster they become aware of the issue the greater chance they can reduce the number of users that will be affected.

Rate Your Personal Exposure?

Environment

Which of the following statements best describes your personal cyber environment?

- ✓ I have multiple devices, usually of the latest offerings, that I keep connected whether in social, work, or home environments. **(9)**
- ✓ I have multiple devices but keep their use appropriate to the situation. **(7)**
- ✓ I have a few devices that I use only in the appropriate settings and with the proper security. **(4)**
- ✓ I have a older PC and a simple cell phone **(1)**

Rate Your Personal Exposure?

Connectivity

Which of the following statements best describes how you connect and use technologies in your personal and work environments.

- ✓ I like to stay connected whether at home, work or travelling. I am always connected and like to find free hot spots. **(9)**
- ✓ I try to stay connected and use trusted networks at home and work but will use what is at hand when I travel. **(7)**
- ✓ I like to be connected and use the secure networks at home and work but when travelling try and find secure networks to connect to. **(4)**
- ✓ I only connect and use technology when I am sure I am on a safe and secure network. **(1)**

Rate Your Personal Exposure?

FIPCO
COMPLIANT. CONSISTENT. CONFIDENT.

Firewalls and Security

Which of the following statements best describes how you deal with firewalls and security.

- ✓ I use firewalls and other security with settings that allow me the greatest freedom. I assume networks that I use have good firewalls and security. **(10)**
- ✓ I use firewalls and other security with settings that provide good protection. I assume networks that I use have good firewalls and security. **(8)**
- ✓ I prefer to work in environments that have good, known protection. This means firewalls with the highest setting and other security to stop intrusions and other malware. **(4)**
- ✓ I will only work in environments that have the highest protection. This means firewalls with the highest setting and other security to stop intrusions and other malware. **(1)**

Rate Your Personal Exposure?

Social Media

Which of the following statements best describes your participation in various social media?

- ✓ I am an avid participant in social media and am in several. I generally allow my information to be shared and open to the public. **(10)**
- ✓ I participate in social media and am in several. I generally restrict my information to friends and contacts. **(7)**
- ✓ I participate in social media and restrict my information to a few friends and contacts. **(4)**
- ✓ I do not use social media for any purpose **(1)**

Rate Your Personal Exposure?

Back Up and Security

Choose the statement that best describes your approach to backing and protecting your info.

- ✓ I know I should back up my personal information and encrypt some of it, however, I never seem to find the time or have other issues that get in the way. I rely on the staff at work to do the appropriate back up and encrypting. **(9)**
- ✓ I back up my personal information and encrypt some of it, however, I do not do it as often as I would like, nor do I do it on a regular basis. I discuss with the staff at work the appropriate back up and encrypting. **(7)**
- ✓ I back up and encrypt my sensitive and important personal information, however, I do not do it as regularly as I would like. I work with staff at work the appropriate back up and encrypting. **(5)**
- ✓ I perform backups on a regular basis and encrypt all sensitive information at work and at home. **(1)**

Rate Your Personal Exposure?

FIPCO
COMPLIANT. CONSISTENT. CONFIDENT.

On Line Activity

Which of the following best describes your on-line activity?

- ✓ My life is on line. I do on line banking, shopping, social media, gaming, email and other activities. **(10)**
- ✓ I do a fair amount on line and try to use trusted and secure sites. **(7)**
- ✓ I do some on line activities and only use trusted and secure sites. **(4)**
- ✓ I minimize my on line activity to those activities that do not require giving any personal identifying information. **(1)**

Rate Your Personal Exposure?

Wi-fi usage

Select the statement that best describes your wi-fi network usage.

- ✓ I love being connected so I connect to wi-fi hot spots wherever and whenever. **(10)**
- ✓ I like to be connected and will connect to wi-fi hot spots when necessary. **(8)**
- ✓ I like to be connected but will only connect to wi-fi networks when I know it is trusted and secure. **(5)**
- ✓ I rarely connect to wi-fi but if I do I make sure it is a secure with a complex password. And even then I encrypt all sensitive information. **(3)**
- ✓ I never use Wi-fi. **(1)**

Rate Your Personal Exposure?

Passwords

Select the statement that best describes your approach to passwords.

- ✓ I view passwords as a necessary evil and use ones I can easily remember and reuse whenever possible. **(10)**
- ✓ I view passwords as necessary and use ones I can remember. **(8)**
- ✓ I understand the need for passwords and do my best to create good ones. **(5)**
- ✓ I have a system for creating and using complex passwords. I change them frequently and always change default settings as well. **(1)**

Rate Your Personal Exposure?

BYOD Activity

Choose the statement that best describes how you use your own device when at work.

- ✓ I much prefer to use my own device at work and connect it to the work network despite the IT department saying I can't and work around their security. **(10)**
- ✓ I prefer to use my own device at work and connect it to the work network and work within the IT department guidelines. **(8)**
- ✓ I occasionally use my own device at work and connect it to the work network using the portals and security provided by our IT department. **(5)**
- ✓ I never use my own devices on the work network. **(2)**

Rate Your Personal Exposure?

BYOD Activity

Choose the statement that best describes how you use your own device when at work.

- ✓ I much prefer to use my own device at work and connect it to the work network despite the IT department saying I can't and work around their security. **(10)**
- ✓ I prefer to use my own device at work and connect it to the work network and work within the the IT department guidelines. **(8)**
- ✓ I occasionally use my own device at work and connect it to the work network using the portals and security provided by our IT department. **(5)**
- ✓ I never use my own devices on the work network. **(2)**

Rate Your Personal Exposure?

Cloud Computing

Choose the statement that best describes how you use “cloud” resources. (Onedrive, GooglePic, Dropbox)

- ✓ I make extensive use of cloud resources both in my personal life and for work as well. It makes it much easier to upload work to the cloud so I can work on it in the evenings or weekends. **(10)**
- ✓ I use cloud resources both in my personal life and for work. I occasionally upload work to the cloud so I can work on it in the evenings or weekends. **(8)**
- ✓ I use cloud resources for my personal life but not for work unless it is part of the approved work environment. I never upload work to the cloud so I can work on it in the evenings or weekends. **(4)**
- ✓ I do not use any cloud resources. **(1)**

Add up the scores in **RED**

Score Personal Exposure?

FIPCO
COMPLIANT. CONSISTENT. CONFIDENT.

- Highest Cyber Exposure **(100-80)**
  - You certainly like to live large but this carries with it the likelihood you will run into some of the cyber predators in the near future. You can only lessen your exposure by modifying your behavior but based on your responses you won't like doing that. We strongly recommend you consider changing your cyber behavior.
- High/Moderate Cyber Exposure **(79-60)**
  - Your responses tell us that it is more than likely you will run into some of the cyber predators in the near future. You can lessen your cyber exposure by modifying your behavior and implementing some additional protections the choice is yours. We recommend you consider changing your cyber behavior.

Score Personal Exposure?

- Moderate Cyber Exposure **(59-40)** - Your behavior tells us that you may run into some of the cyber predators in the future. You can lessen your exposure by modifying your behavior and adopting some additional protections. We encourage you to consider changing your cyber behavior
- Moderate/Low Cyber Exposure **(39-20)** - You have, by your own behavior lowered your cyber exposures. However, realize that no one, if they participate in the cyber environment, can eliminate all exposure. Keep working to improve your behaviors and it is likely the cyber predators will look for easier targets. Remember the old joke you don't have to out run the bear just your companion.
- Lowest **(19-10)** – You have, by your own behavior minimized you cyber exposures. However, realize that no one, if they participate in the cyber environment, can eliminate all exposure. Keep up your good work and it is likely the cyber predators will look for easier targets.

Resources for Training

Tools – CATO – Password Enforcers

https://haveibeenpwned.com/Passwords

https://spycloud.com/

https://www.enzoic.com/

https://www.anixis.com/default.htm

How to Tell if a Website is Safe -

https://www.avg.com/en/signal/website-safety

Osterman Research Whitepaper - ROI for SecAwareness

https://www2.infosecinstitute.com/l/12882/2019-08-27/frwc2f

Resources for Training

Videos

- **What is 2 Factor?** https://www.youtube.com/watch?v=EXbjJUD2sH0 (2 Min)
- **Ellen's Password Keeper** https://www.youtube.com/watch?v=_u8Rss3W4Wg (3 min)
- **ATM Skimmers** https://www.youtube.com/watch?v=rgVDRCp6B3Y (2 Min)
- **Cybersecurity 101 produced by PBS Nova:** https://www.youtube.com/watch?v=sdpxddDzXfE (4 Min)

Resources for Training

Other

- **Nova Cybersecurity Lab Games - http://www.pbs.org/wgbh/nova/labs/lab/cyber/**
- **Parents Know More - http://parentsknowmore.com/resources/**
- **LIST OF Videos and Games to Help Protect Yourself - http://www.onguardonline.gov/media **
- **Nova Cybersecurity Lab Games- http://www.pbs.org/wgbh/nova/labs/lab/cyber/**
- **Fixes for Identity Theft - http://www.identitytheftfixes.com/**
- **Free Posters:**
  - SANS - https://securingthehuman.sans.org/resources/posters
  - Native Intelligence - http://www.nativeintelligence.com/ni-free/ni-free-posters.asp
  - Department of Energy - https://energy.gov/cio/downloads/cybersecurity-awareness-posters
  - Center for Development of Security Excellence - https://www.cdse.edu/resources/posters-all.html

Resources for Training

Other

- **Password lists for Brute Force Attack -**
  https://github.com/danielmiessler/SecLists/tree/master/Passwords

- **Ezshield – Fighting Identity Crimes**
- **https://secure.ezshield.com/pub/cc?_ri_=X0Gzc2X%3DYQpglLjHJlTQGrzbiK5Ot6P5zdMTYRk5WYAyUmE05WSeL1gGkTLL5FbWnDzfaymOk6yMOVXtpKX%3DSADRTUCS&_ei_=Eq2tf9zs59idfPO1Sc_9BblT2U73mL48c83ZMvrAdi76NfQJPA_COGzpJRelwVHC1CVUPcHoZ1o8qSSczKFO9LaA9OJN.**

- **https://www.fightingidentitycrimes.com/breach-news-summary/?utm_campaign=Engagement.Identity_Report_C_[09-19]&utm_source=EZShield&utm_medium=email**

Thank You!