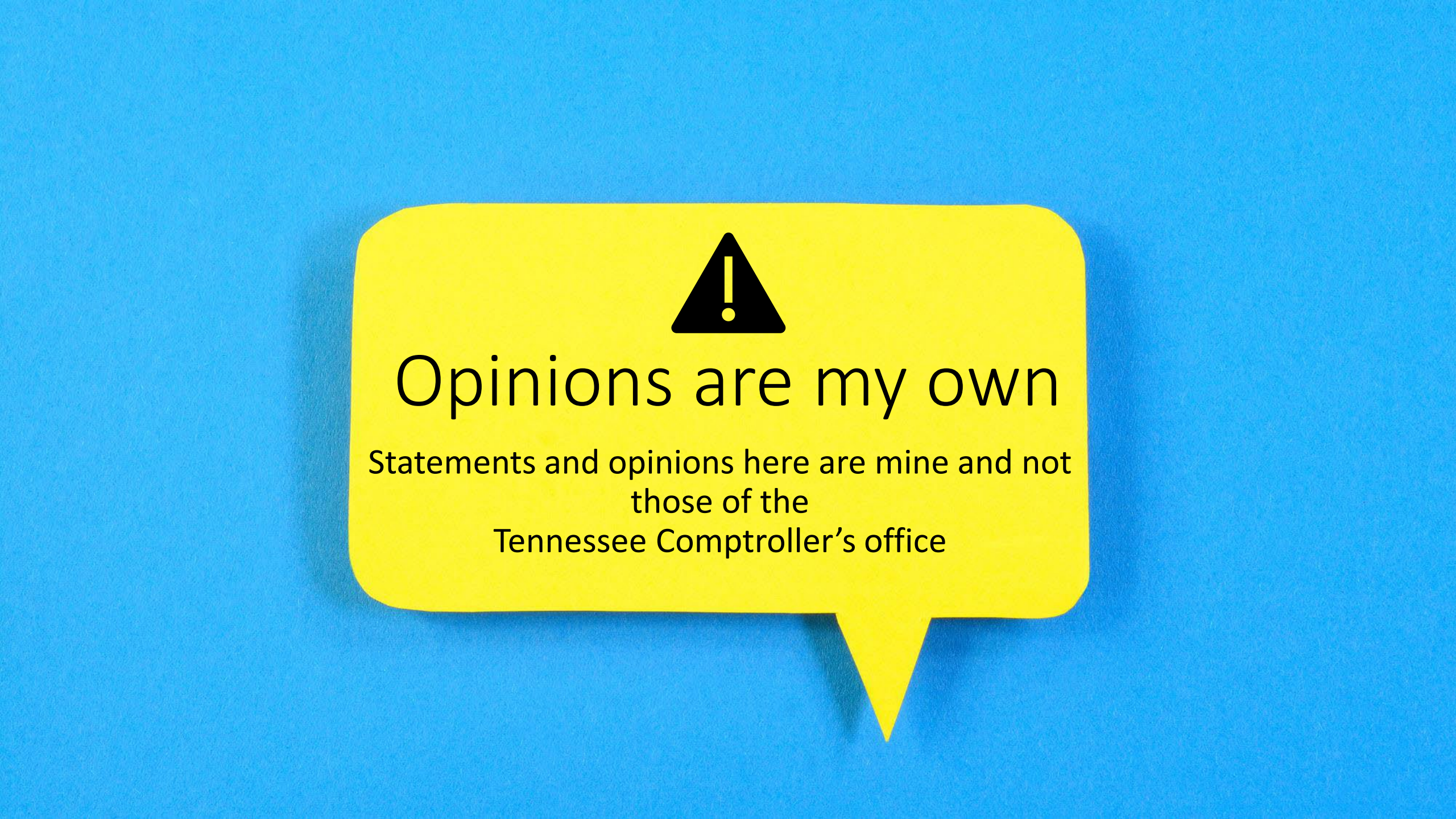
Cyberthreats

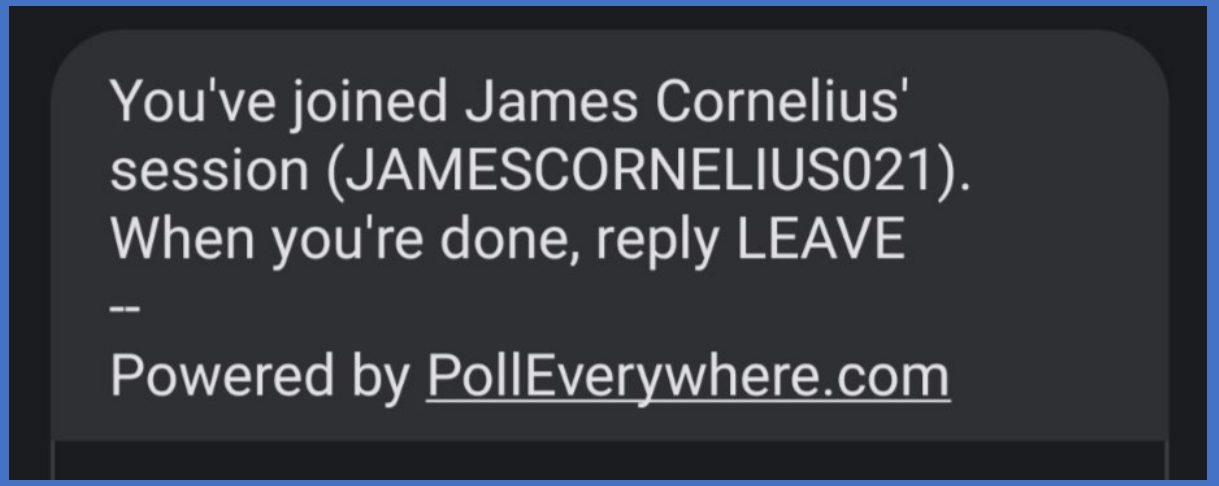
The more things change the more they stay the same.

So many threats,
So little time.


Opinions are my own
Statements and opinions here are mine and not those of the
Tennessee Comptroller’s office

Let’s Interact

Text **jamescornelius021** to **22333**



Your favorite of the four seasons?

- Spring
- Summer
- Fall
- Winter
- None of the above. Tennessee only has two seasons, humid and cold.

Your favorite of the four seasons?

Spring

Summer

Fall

Winter

None of the above. Tennessee only has two seasons, humid and cold.

Your favorite college team?

- Alabama
- Florida
- Kentucky
- Tennessee
- Georgia
- How dare you not list my team!

Your favorite college team?

Alabama

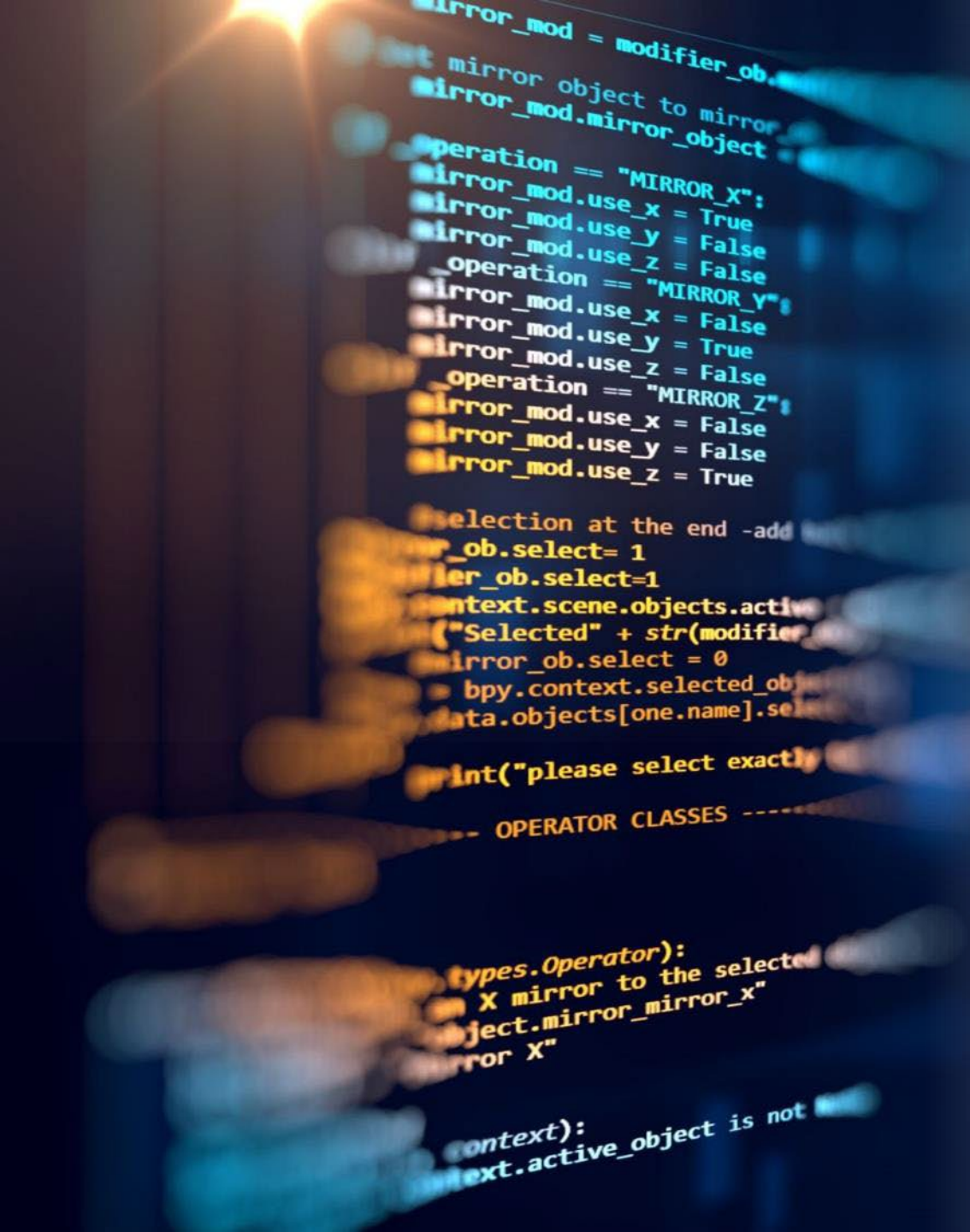
Florida

Kentucky

Tennessee

Georgia

How dare you not list my team!



So, what is a cyberthreat?

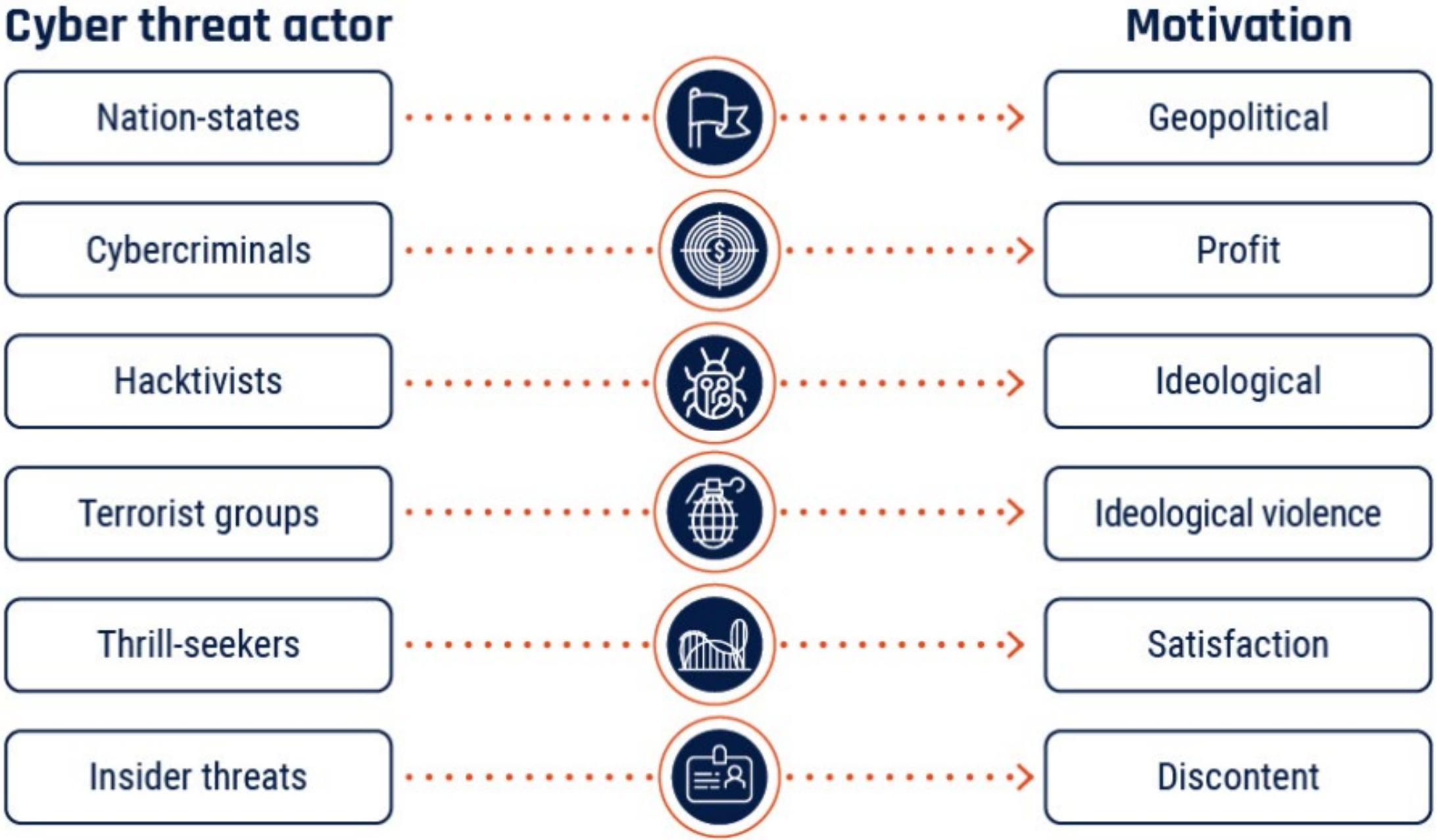
The possibility of a malicious attempt to damage or disrupt a computer network or system. – Oxford Dictionary

They perform cyberattacks and cause cybersecurity incidents.

The bad guys that do bad things to your computers.

Cyberthreat Actors

Who are they and why are they doing it?


Cyber threat actor
Motivation
Nation-states
Geopolitical
Cybercriminals
Profit
Hacktivists
Ideological
Terrorist groups
Ideological violence
Thrill-seekers
Satisfaction
Insider threats
Discontent

Nation States

- State-Sponsored Cybercrime
- Espionage
- Cyberwar

This Photo from WIRED, Conde Nast

Cybercriminals

All About the Benjamins

$8 Trillion – estimate cost in 2023

$10.5 Trillion – estimate cost in 2025

Hacktivism

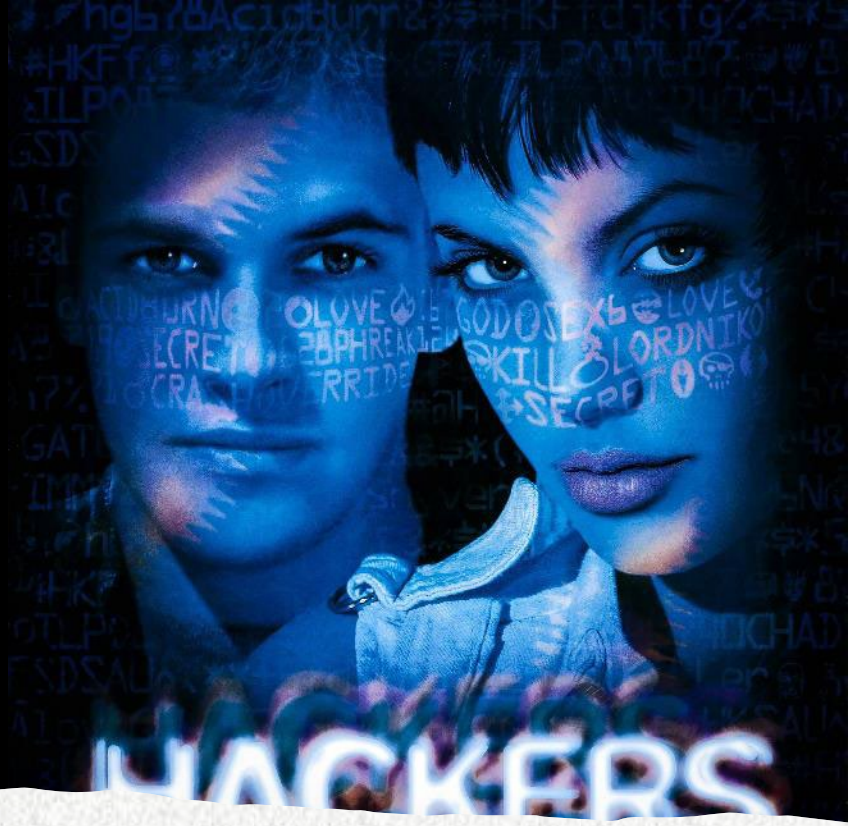
Ideologically motivated

- Wikileaks
- Anonymous
- LulzSec
- IT Army

Terrorist Groups

Primarily used to recruit and spread their views

- FBI and other law enforcement groups perform takedowns of the sites when possible.



Thrill Seekers

Because it's there and someone said it shouldn’t or it can’t be done.

- Lots of overlap with Hacktivists
- Sometimes become the next generation of security professionals

Insider Threats

Intentional

- Sabotage, Theft, Espionage, Fraud, and Competitive advantage

Unintentional

- Mistakes, Carelessness, Policy Violation

Most active cyberthreat actor?

- Nation-states
- Cybercriminals
- Hacktivists
- Terrorists groups
- Thrill-seekers
- Insider threats

Most active cyberthreat actor?

Nation-states

Cybercriminals

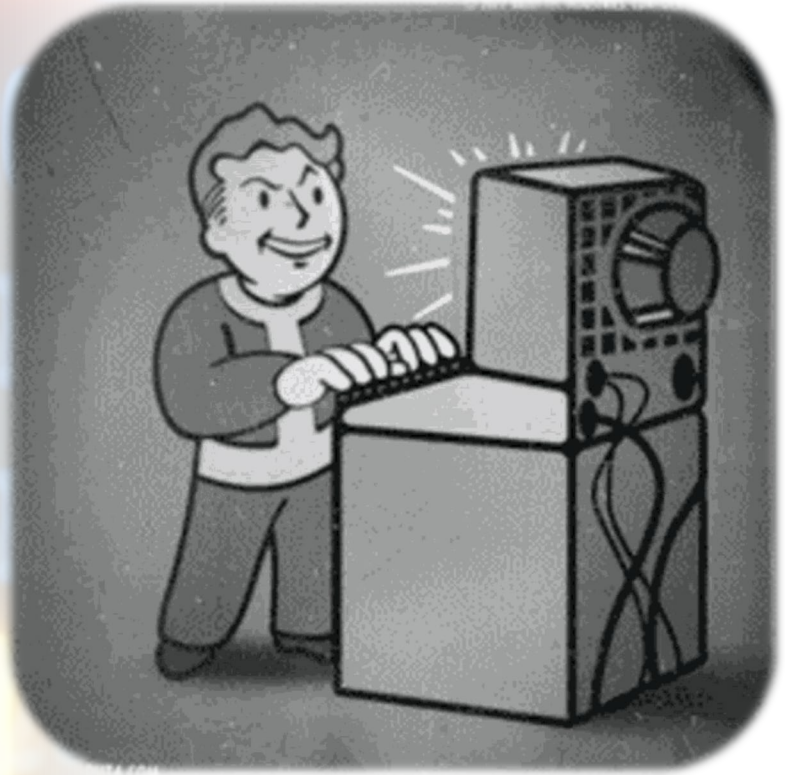
Hacktivists

Terrorists groups

Thrill-seekers

Insider threats

Cyberattacks



Social Engineering – A Not So Cyberattack

noun: social engineering

The use of deception to manipulate individuals into divulging confidential or personal information that may be used for fraudulent purposes. – Oxford Dictionary

Social Engineering attacks use the same techniques as a good old fashion con-artist.

“Sooner or later, everything old is new again.”

- Stephen King

Elements of a Social Engineering Attack

Reciprocity – People tend to return a favor.

Commitment and Consistency – In general people attempt to follow through on something they said they would do.

Social Proof – People will do things that they see other people are doing.

Authority – People will tend to obey authority figures, even if they are asked to perform objectionable acts.

Liking – People are easily persuaded by other people whom they like.

Scarcity – Perceived scarcity will generate demand.

- Influence: The Psychology of Persuasion, Robert Cialdini

Social Engineering Cyberattacks

Phishing – Spear Phishing – Whaling – Business Email Compromise

Baiting – Get a free chicken sandwich!!!

Malware – Ransomware, Spyware, Stalkerware, Adware – docx, xlsx, pdf

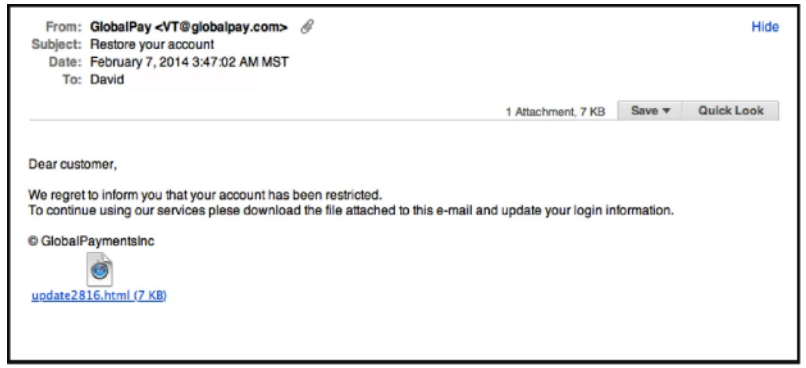
Pretexting – Per our last email…

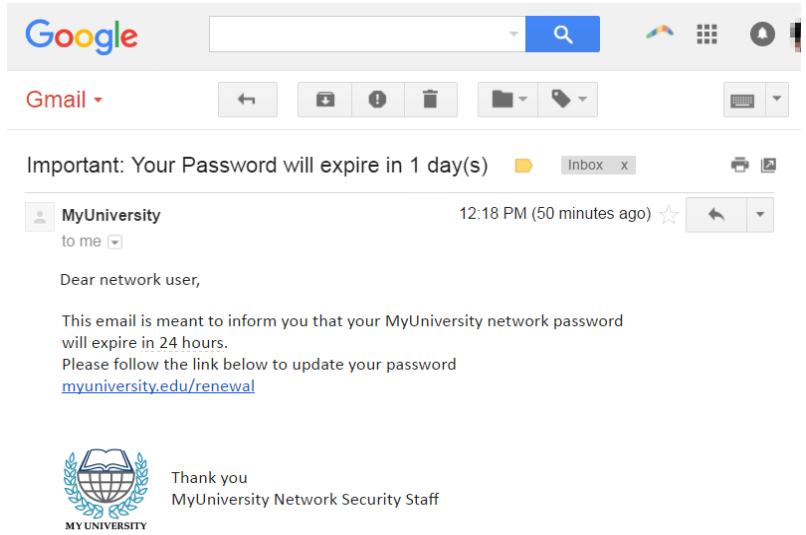
Quid Pro Quo – We have prevented a security attack; we need you to…

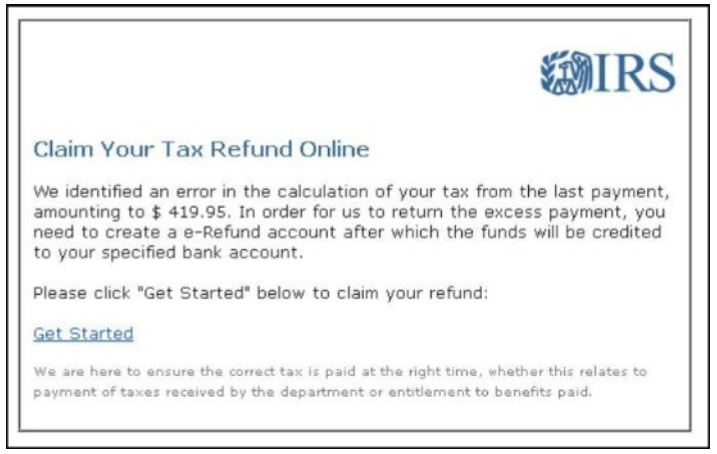
Vishing – Phone calls – The FBI has closed your Social Security Account…

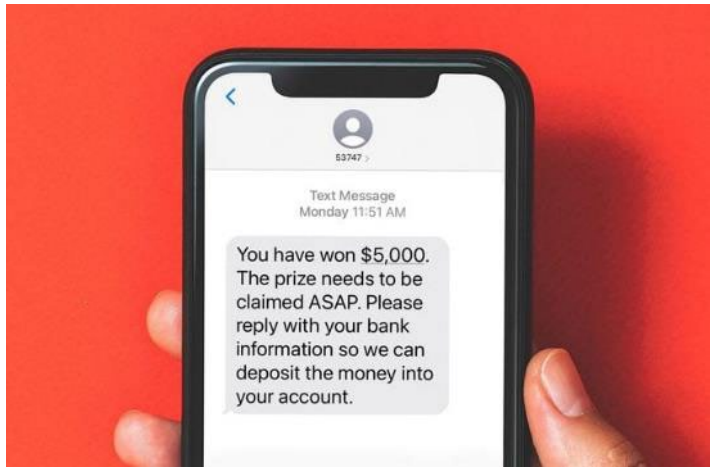
Water-Holing – Doctor's hate these tricks. Number 7 will shock you…

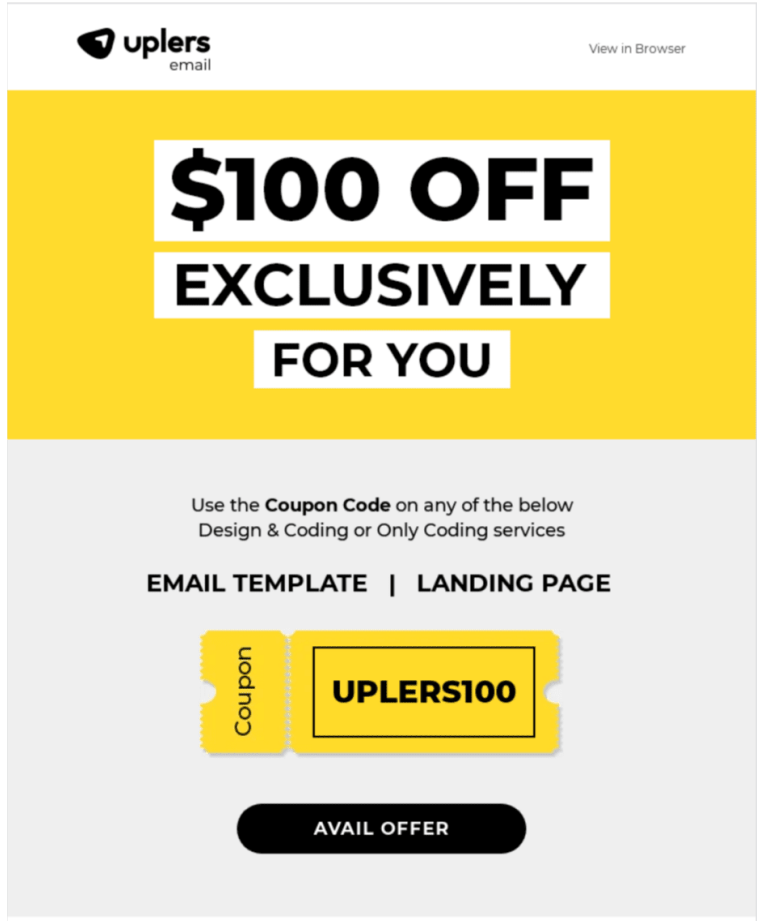
Smishing – Text messages – Your Amazon account has been accessed…



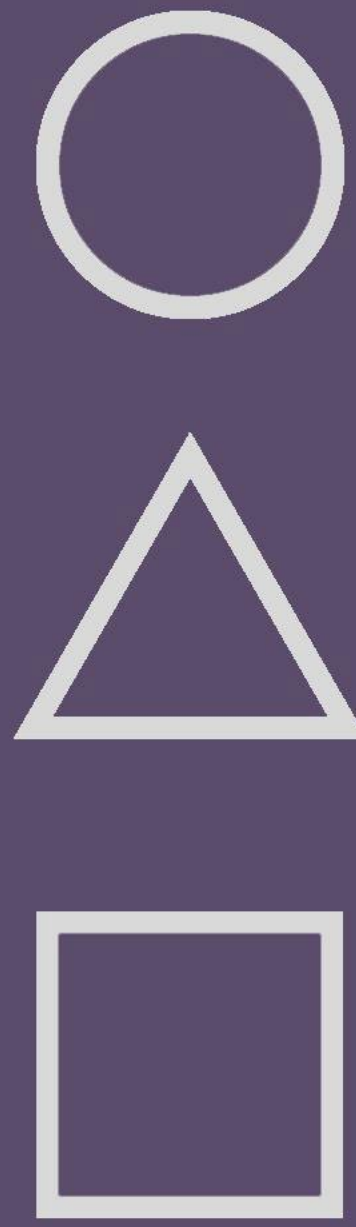






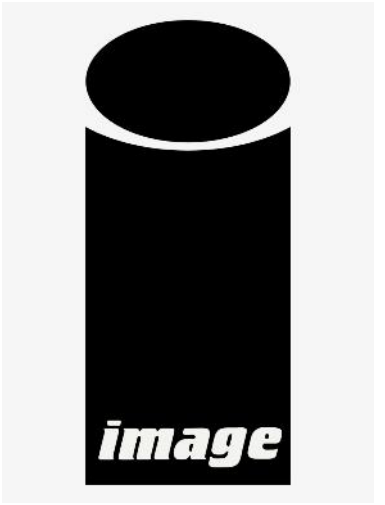


Digital Social Engineering Attacks



Let's Play a Game

Rapid fire round.



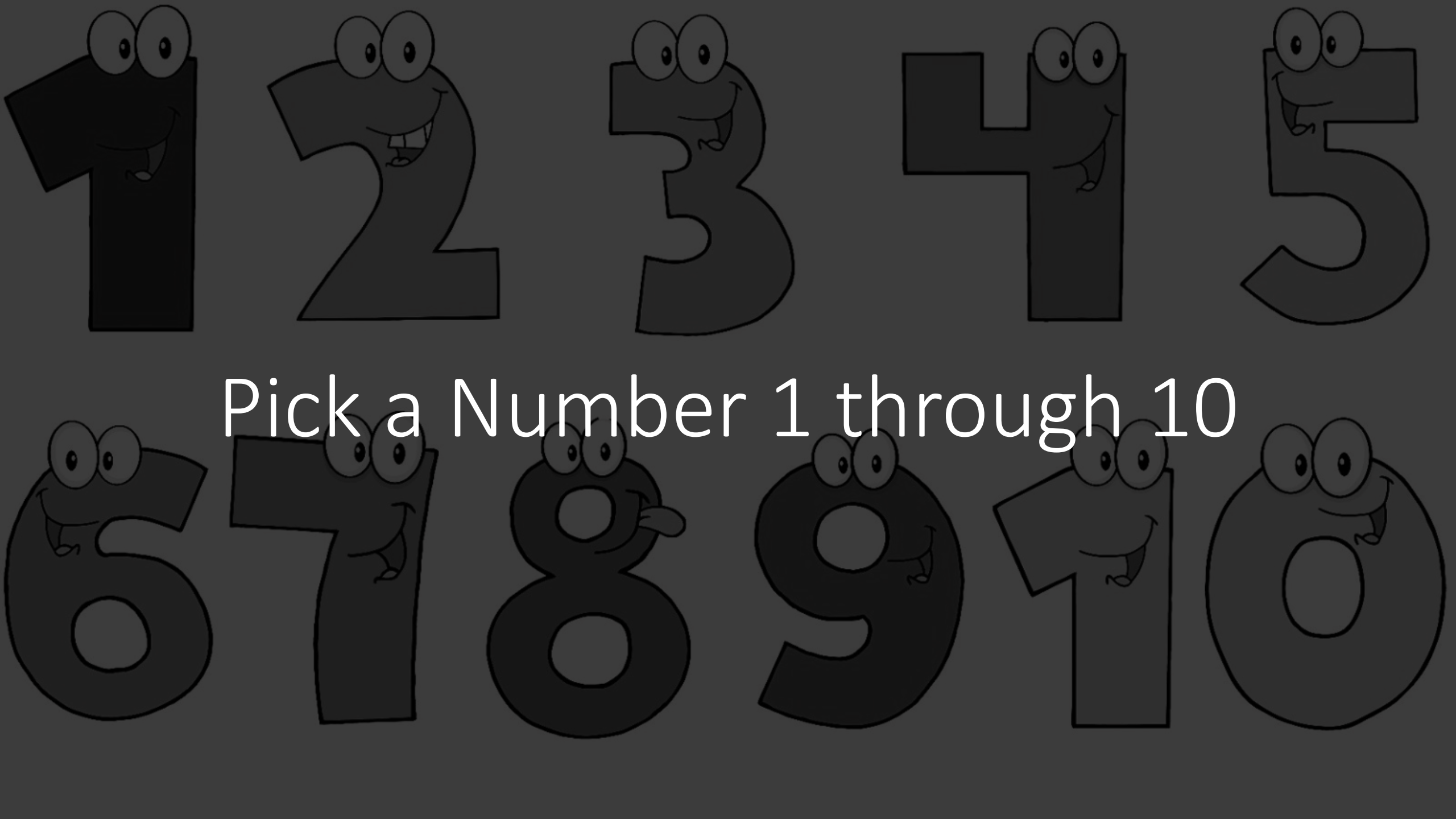
Think of a Superhero

Which hero did you pick?

Batman, Superman, Ironman, Hawkeye, Spiderman

Wolverine, Thor, Deadpool, Punisher, Black Widow

None of those


Pick a Number 1 through 10

Was your number

7?

3?

2?

Nope!

What is Your Favorite Color?

Which color did you pick?

Red, Blue, Black, Green, White

Pink, Orange, Brown, Purple, Yellow

None of those basic colors...

Let’s talk about passwords

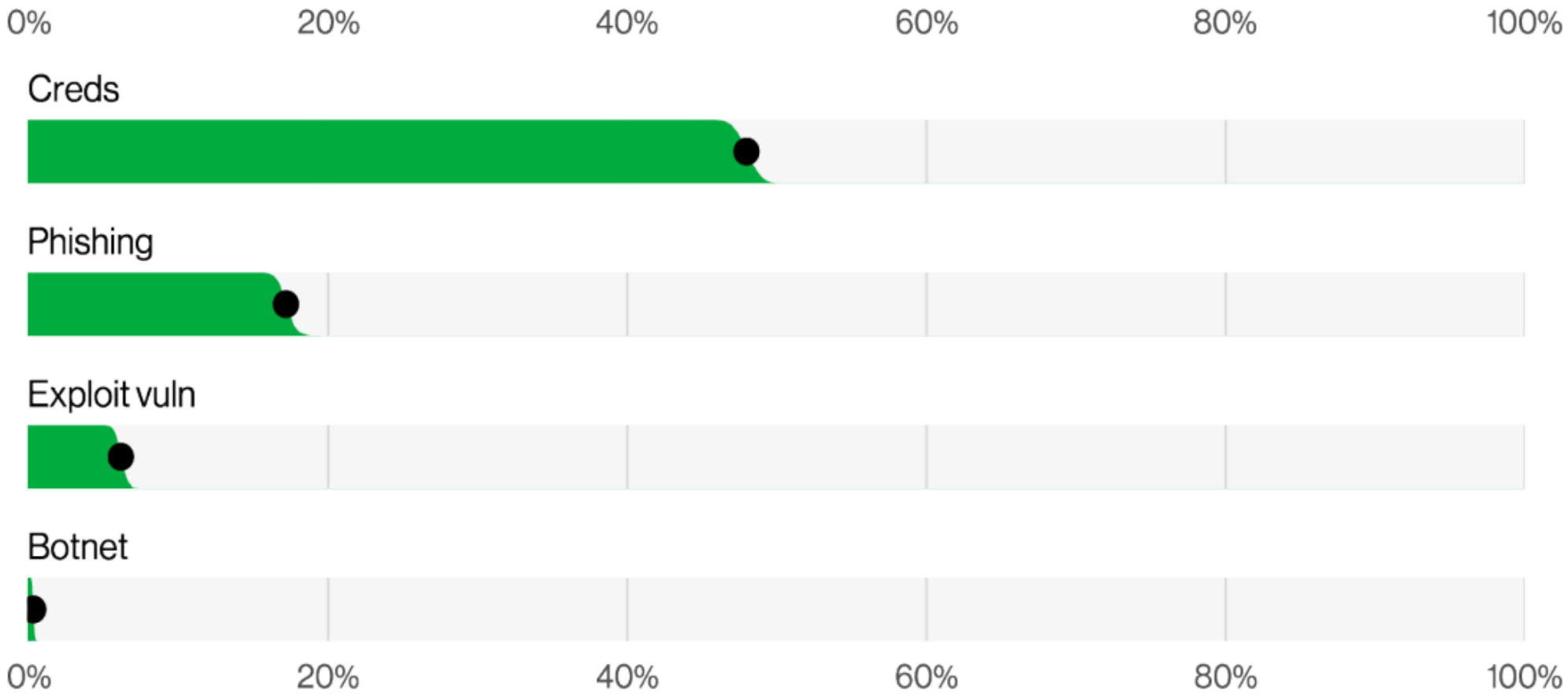
Top 10 most common passwords from a list of 10 million from data breaches.

Using the top 10 would let you guess 16 out of 1000 passwords.

1. 123456
2. password
3. 12345678
4. qwerty
5. 123456789
6. 12345
7. 1234
8. 111111
9. 1234567
10. dragon

Cyberattacks by the numbers

Top methods to compromise an organization and steal data.



Defending Against Cyberattacks

Protecting the human

Security Awareness is the beginning.

- Trying to prevent security incidents with technology alone will fail.

Look for the manipulation elements.

When you get a strange email, phone call, or text message take time to consider if it is trying to manipulate you.

Protecting the computer

Exploits – Update devices and applications – Use auto-update.

- Restart devices at least once a week to ensure updates are fully applied.

Password Attacks – Strong and Unique for each one

- At least 16 characters long, not a single dictionary word, not personal information.
- Multi-factor authentication
  - Test message (SMS), one-time code, hardware key
- Password manager
  - One password, have random ones for everything else.

Misconfigured Systems

- Use instructions for correct configurations
- Vendor websites
- Trusted technical resources

Resources

Stop | Think | Connect

https://www.stopthinkconnect.org/tips-advice/general-tips-and-advice

National Cyber Security Alliance

https://staysafeonline.org/

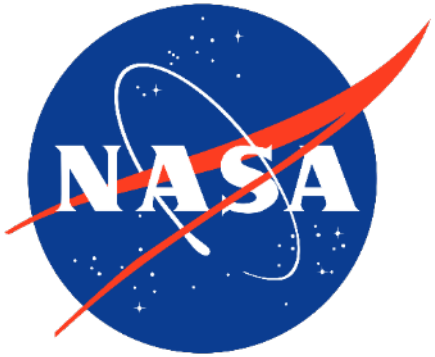
Damage from Cyberattacks

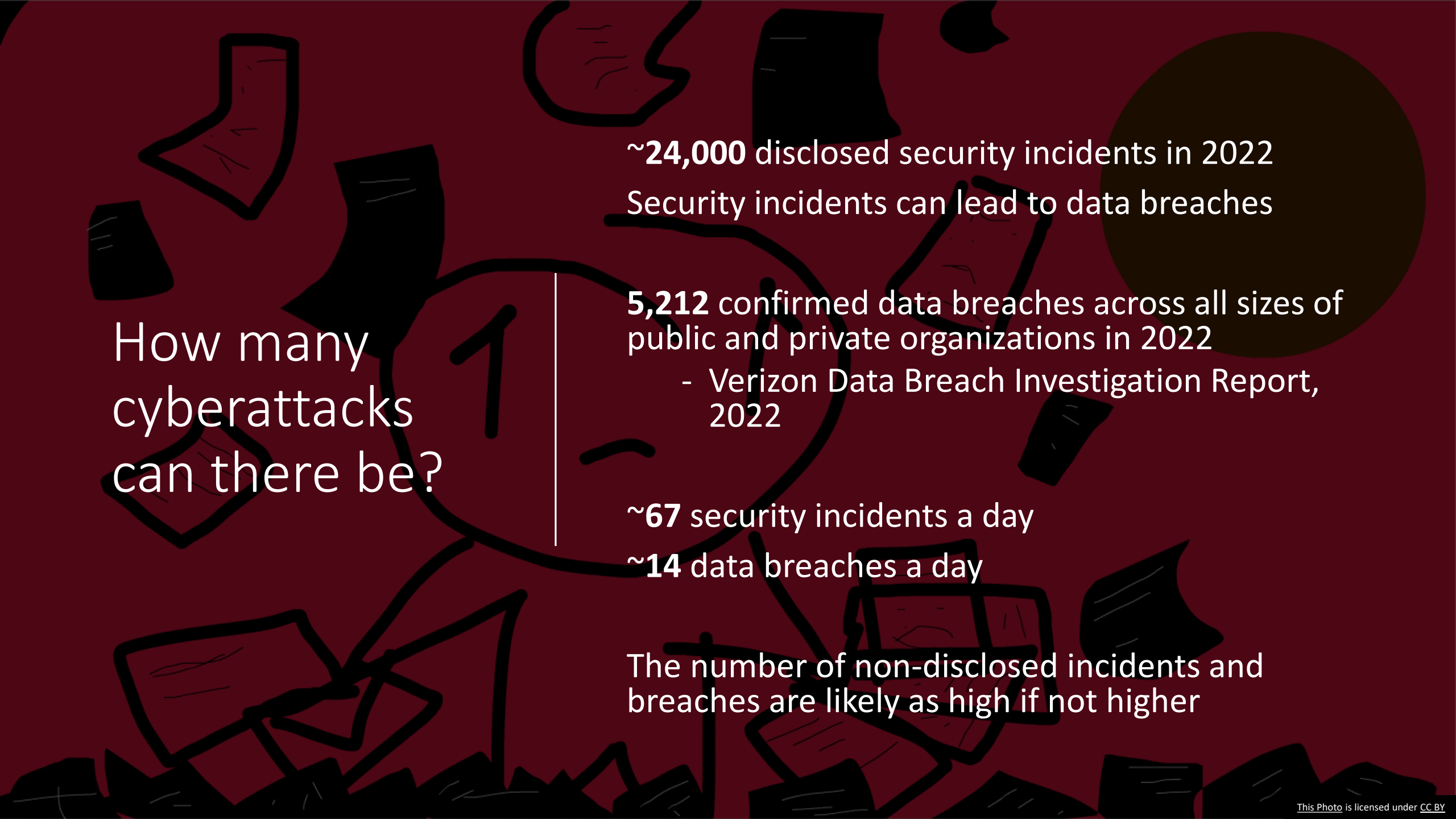
Oof, right in the wallet!

EQUIFAX

Yahoo!

Colonial Pipeline Company





How many cyberattacks can there be?

~24,000 disclosed security incidents in 2022

Security incidents can lead to data breaches

5,212 confirmed data breaches across all sizes of public and private organizations in 2022

- Verizon Data Breach Investigation Report, 2022

~67 security incidents a day

~14 data breaches a day

The number of non-disclosed incidents and breaches are likely as high if not higher

Ransomware
Pay up or else

2593 – Victims announced by ransomware groups. True number unknown likely higher.

41% - Percentage of organizations paid

$228, 125 – Average ransom payment

$457 million – Estimated ransomware income

Data Breach – They lost how many?

~1.2 billion records exposed in breaches in 2022

Personally Identifiable Information (PII)

- Information that can identify a specific person
  - Name, Address, Phone number, Birthday, SSN, Gov't ID#, CC#, Tax ID#

Health Data (HIPAA)

- Dr. notes, diagnoses, medicines, injuries

Dark Web Value of Those Records

Healthcare data: $250
Credit card details and associated information: $17-$120
Online banking login information: $65
Facebook account: $45
Cloned VISA with PIN: $20
Stolen payment account details, minimum $1,000 balance: $20
Hacked web and entertainment services: Up to $40
Documents and account details allowing identity theft: $1,010

Costs of Ransomware and Data Breaches

Costs of response, recovery, lost productivity, PR, revenue

- Globally - **$4.35 Million** per incident
- Business - **$4.11 Million** per incident
- Healthcare - **$10.1 Million** per incident
- Governments - **$2.03 Million** per incident

60% of businesses increased costs to their customers

- IBM Cost of a Data Breach report, 2022

Cost of Identity Theft to an Individual?

- $250
- $700
- $1,600
- $2,300
- 4 Easy Payments of $29.99 + S&H

Cost of Identity Theft to an Individual?

- $250
- $700
- $1,600
- $2,300
- 4 Easy Payments of $29.99 + S&H

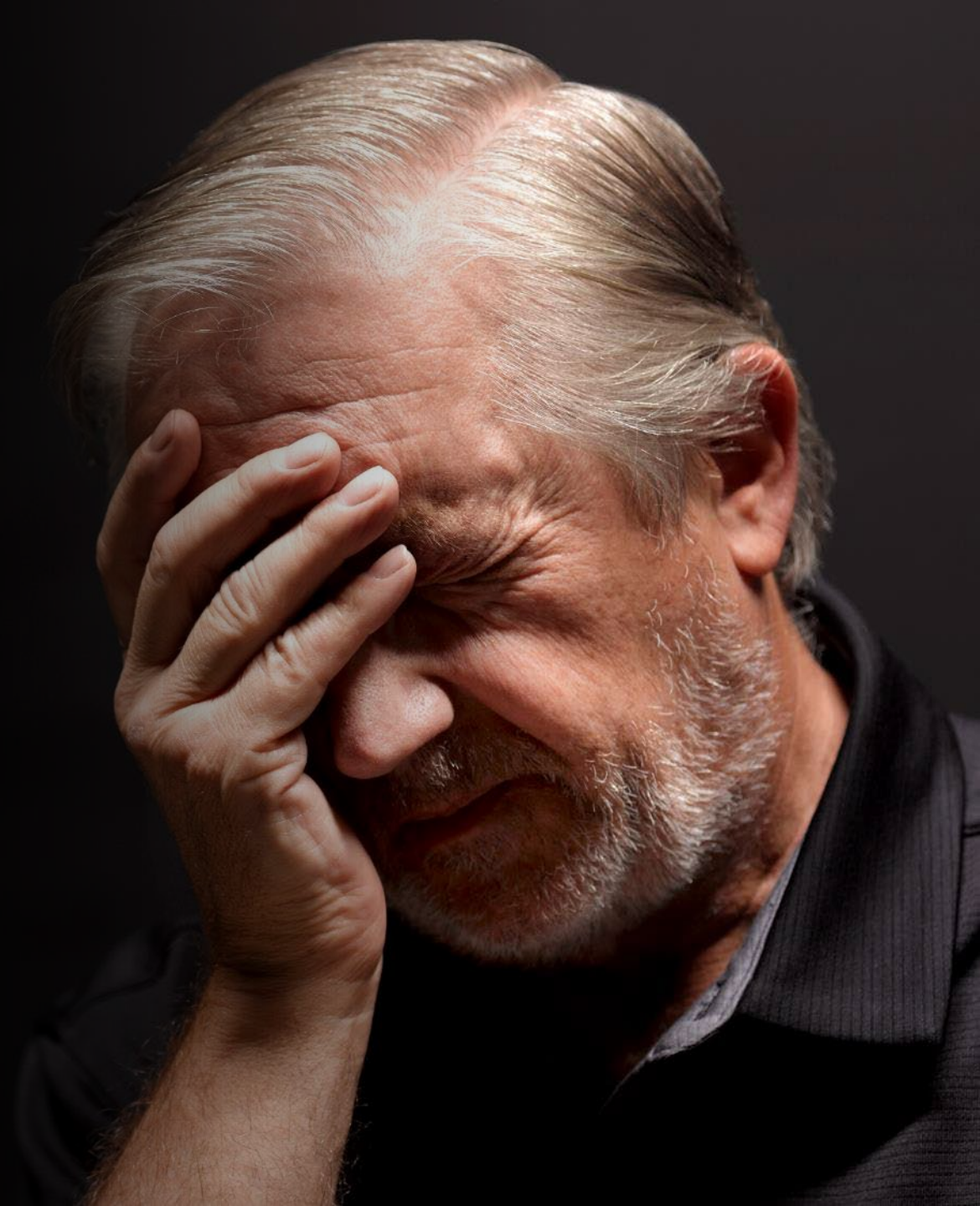
Personal costs of a data breach

$1,600 - Average cost per incident

9 hours - Average time spent working to reclaim identity

Other potential impacts

- Carry court documents to prove identity for official business
- Credit rating damage that might not be removed



Can it get worse?

A Brave New World of Cyberattacks

No War Like Cyberwar

Realm of the Nation-states

Cyberweapons

- Stuxnet
- Regin

Types of targets

- Infrastructure – power, water, food
- Media and people - propaganda

Cyber going kinetic and kinetic going cyber

They seemed so normal - Bots

Manipulation

- Attacks
  - Click/Like Farming
  - Hashtag Highjacking
  - Repost Storm
  - Sleeper Bots
  - Trend Jacking and Watering Hole Attacks
- Estimated 2/3rd of tweeted links are posted by bots
- Motivation
  - Financial, Social, Political, teh lulz

Key Points

- Things like Phishing are not new. Just new delivery methods.
- Passwords are hard but can be managed.
- More than likely your identity is already out there. Assume that and prepare accordingly.
- Cyberwarfare and Deception are the new kids in town.