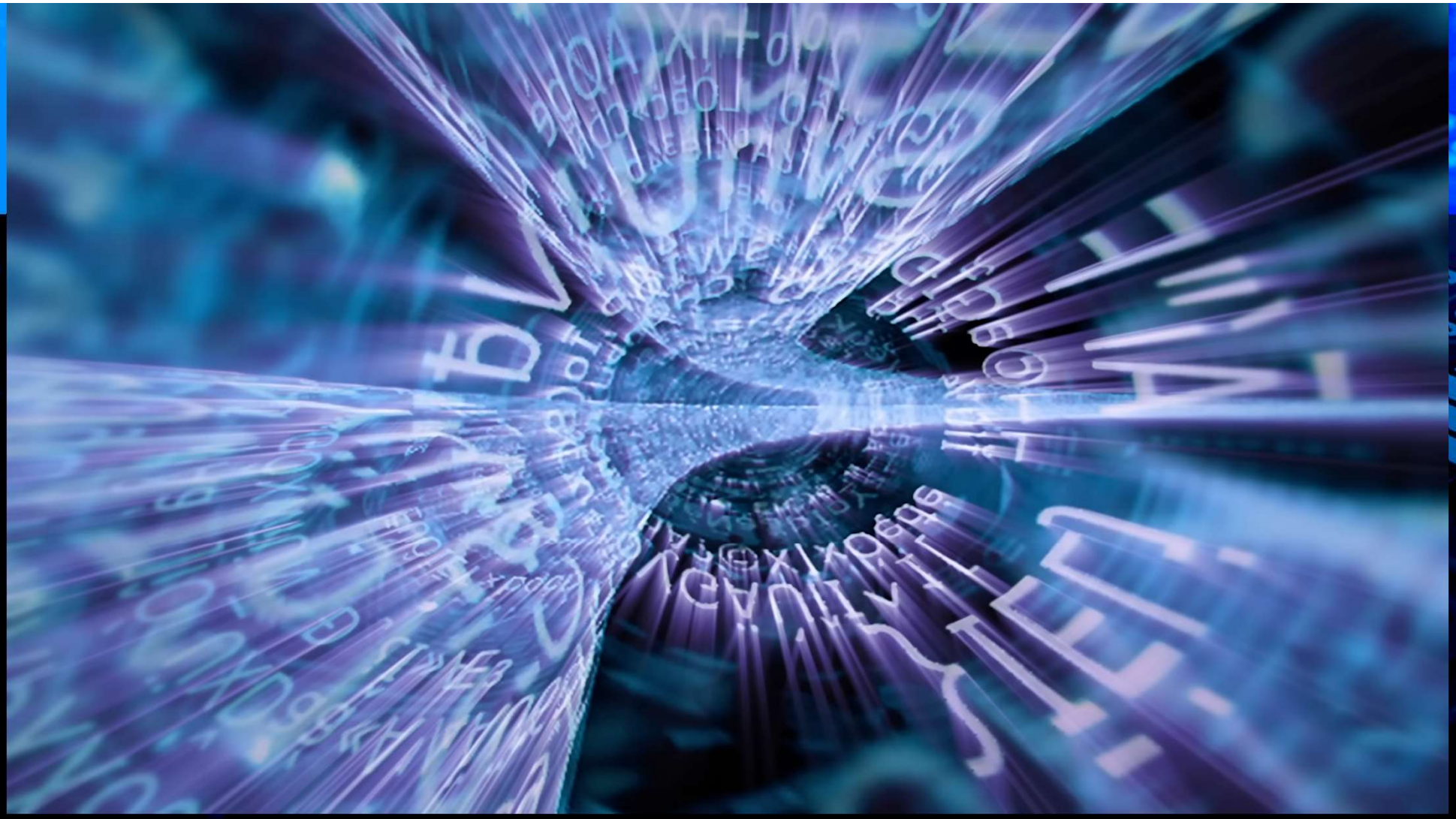
- https://neal.fun/password-game/

Cybersecurity 2023

Presenter: Jared Nishimoto



https://www.youtube.com/watch?v=-UrdExQW0cs

Conventional Computing

NUMBER OF CHARACTERS	NUMBERS ONLY	UPPER OR LOWERCASE LETTERS	UPPER OR LOWERCASE LETTERS MIXED	NUMBERS, UPPER & LOWERCASE LETTERS	NUMBERS, UPPER & LOWERCASE LETTERS, SYMBOLS
3	INSTANTLY	INSTANTLY	INSTANTLY	INSTANTLY	INSTANTLY
4	INSTANTLY	INSTANTLY	INSTANTLY	INSTANTLY	INSTANTLY
5	INSTANTLY	INSTANTLY	INSTANTLY	3 SECS	10 SECS
6	INSTANTLY	INSTANTLY	8 SECS	3 MINS	13 MINS
7	INSTANTLY	INSTANDLY	5 MINS	3 HOURS	17 HOURS
8	INSTANTLY	13 MINS	3 HOURS	10 DAYS	57 DAYS
9	4 SECS	6 HOURS	4 DAYS	1 YEAR	12 YEARS
10	40 SECS	6 DAYS	169 DAYS	106 YEARS	928 YEARS
11	6 MINS	169 DAYS	16 YEARS	6K YEARS	71K YEARS
12	1 HOUR	12 YEARS	600 YEARS	108K YEARS	5M YEARS
13	11 HOURS	314 YEARS	21K YEARS	25M YEARS	423M YEARS
14	4 DAYS	8K YEARS	778K YEARS	1BN YEARS	5BN YEARS
15	46 DAYS	212K YEARS	28M YEARS	97BN YEARS	2TN YEARS
16	1 YEAR	512M YEARS	1BN YEARS	6TN YEARS	193TN YEARS
17	12 YEARS	143M YEARS	36BN YEARS	374TN YEARS	14QD YEARS
18	126 YEARS	3BN YEARS	1TN YEARS	23QD YEARS	1QT YEARS

Quantum Computing

Password Length	Possible Combinations	Time To Crack (S = Seconds, M = Minutes, H = Hours, Y = Years)
4	45697	<1 S
5	11881376	<1 S
6	308915776	<1 S
7	8031810176	~4 S
8	208827064576	~1.5 M
9	5429503678976	~45 M
10	141167709565337 6	~19 H
11	3670344486987780	~.1 Y
*12	95428956661682200	~1.5 Y
13	2481152873203 74E4	~39.3 Y
14	6450997470329 72E5	~1,022.8 Y
15	1677259342285 73E7	~26,592.8 Y
16	4360874289942 89E8	~691,412.1 Y
17	1133827315385 15E10	~17,976,714 Y
18	2947951020001 390E10	~467,394,568 Y

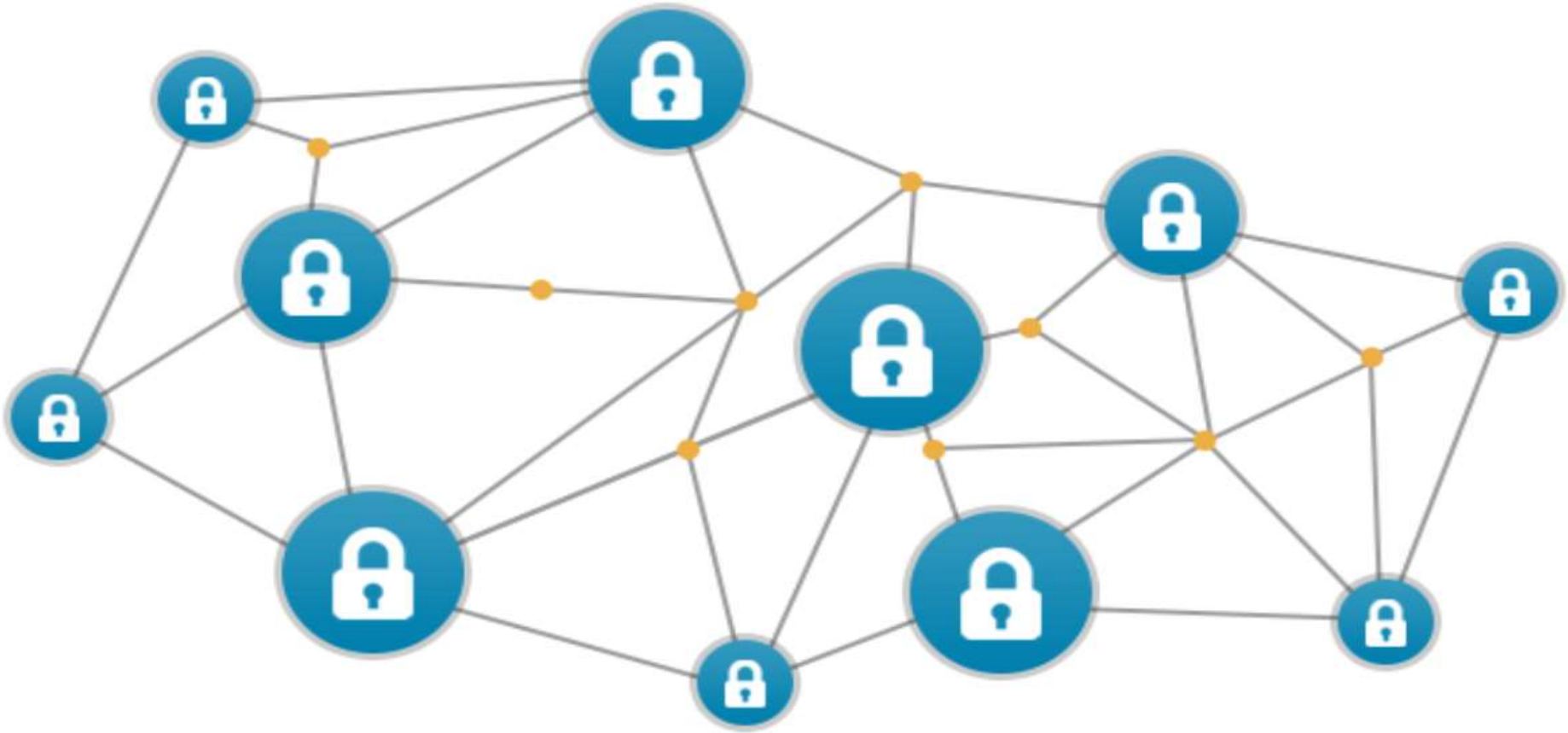
Multi-Factor Authentication

- where a system requires a user to present a combination of two or more credentials to verify a user's identity for login
  - Cybersecurity & Infrastructure Security Agency (CISA)

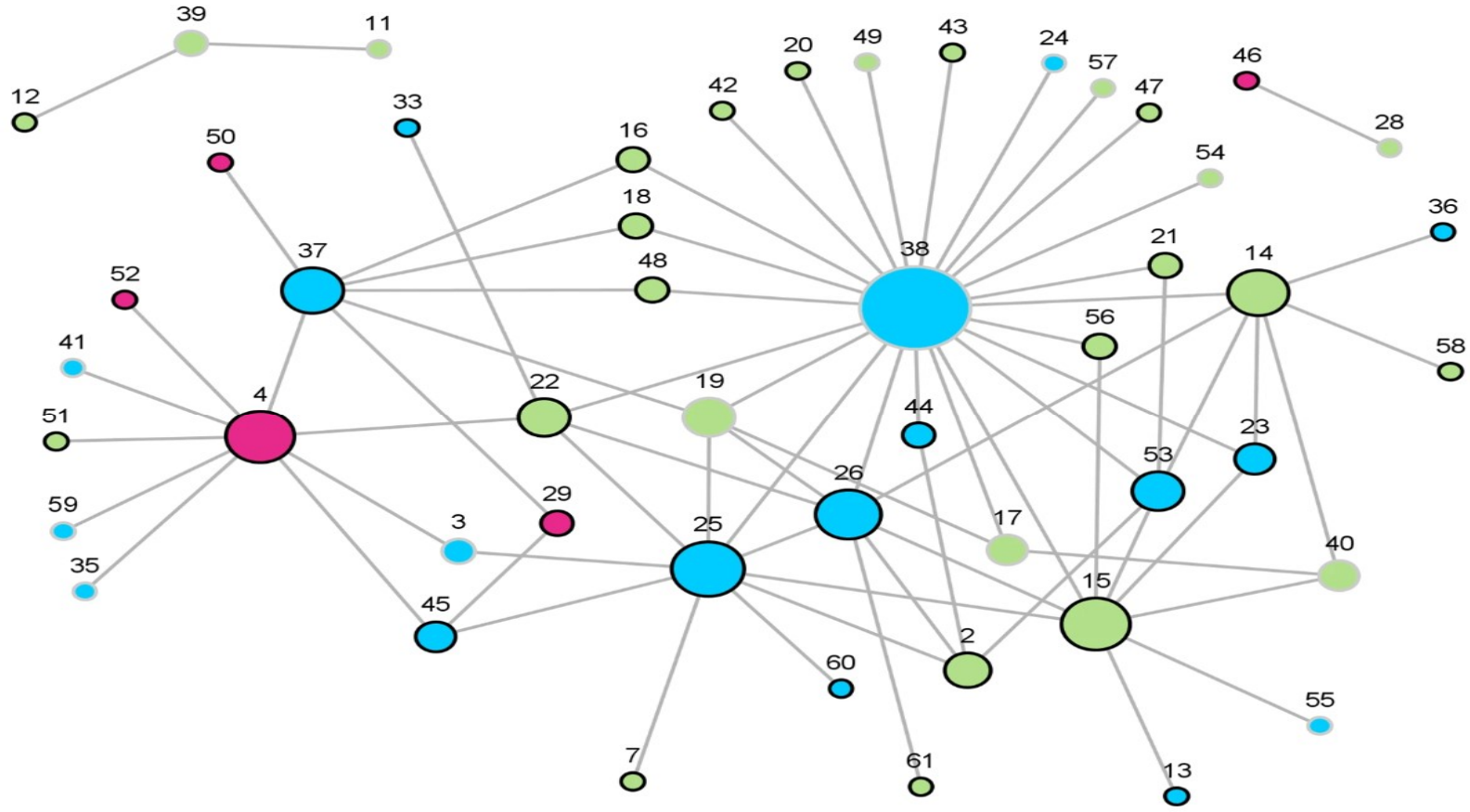
Multi-Factor Authentication

- What you know
  - Password, Pin
- What you have
  - Smart card, mobile device
- What you are
  - Fingerprint, Voice recognition, Retinal Scan

Pre-Pandemic Environment



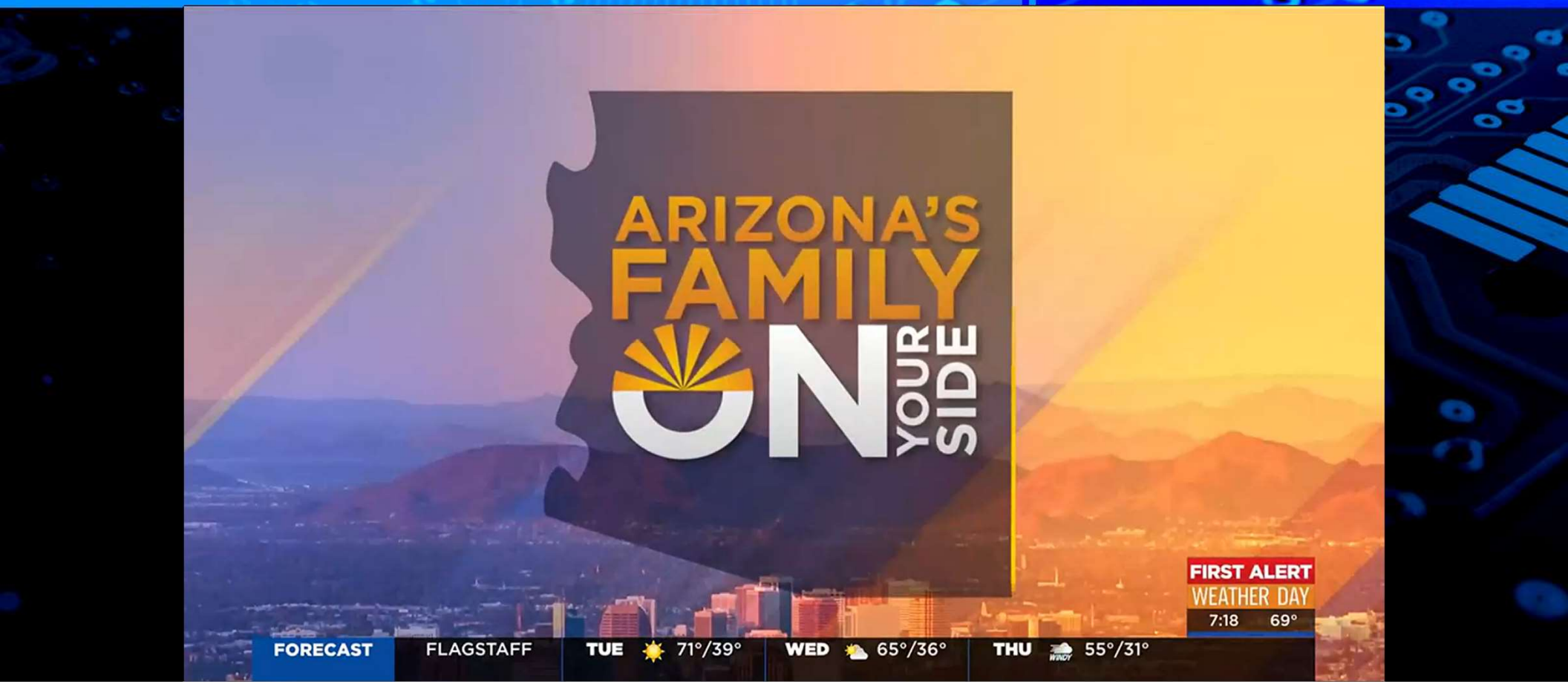
Post-Pandemic Environment



Mobile Devices

- Connecting to Open Wifi
- Data Leaks
- Malicious Apps
- Apps with weak Security
- Poor password security
- Public phone charging stations

Mobile Devices



Mobile Devices

Honwally Fast Charging USB C to C Data Blocker, Protect Against Juice Jacking, Support Safe Fast Charging up to 50V/5A (2 Pack)

4.3 ★★★★½ (69)

$8.99 ($4.50/Count)

FREE delivery **Mon, Apr 17** on $25 of items
shipped by Amazon

USB-C Data Blocker, JSAUX (2-Pack) USB-A to USB-C Female Defender Only for Quick Charge, Protect Against Juice Jacking, Refuse Hacking Provide Safe Charging- Red

4.4 ★★★★½ (106)

$8.99 ($4.50/Count)

FREE delivery **Thu, Apr 20** on $25 of items
shipped by Amazon

Insider Threats

- Who has access to what?
- Who has blanket access?
- Are proper permissions in place?

Insider Threats

- Accidental
- Negligent
- Malicious
- Third-Party

Ransomware as a Service

- is a **business model** between ransomware operators and affiliates in which **affiliates pay to launch ransomware attacks developed by operators**
- RaaS kits allow affiliates lacking the skill or time to develop their own ransomware variant to be up and running quickly and affordably.

Ransomware as a Service

- A RaaS kit may include 24/7 support, bundled offers, user reviews, forums and other features identical to those offered by legitimate SaaS providers.

  – **Crowdstrike**

Zero Trust Environment

"Zero trust is the term for an evolving set of cyber security paradigms that move defenses from static, network-based perimeters to focus on users, assets, and resources. Zero trust assumes there is no implicit trust granted to **assets or user accounts based solely on their physical or network location**.“

-National Institute of Standards and Technology(NIST)

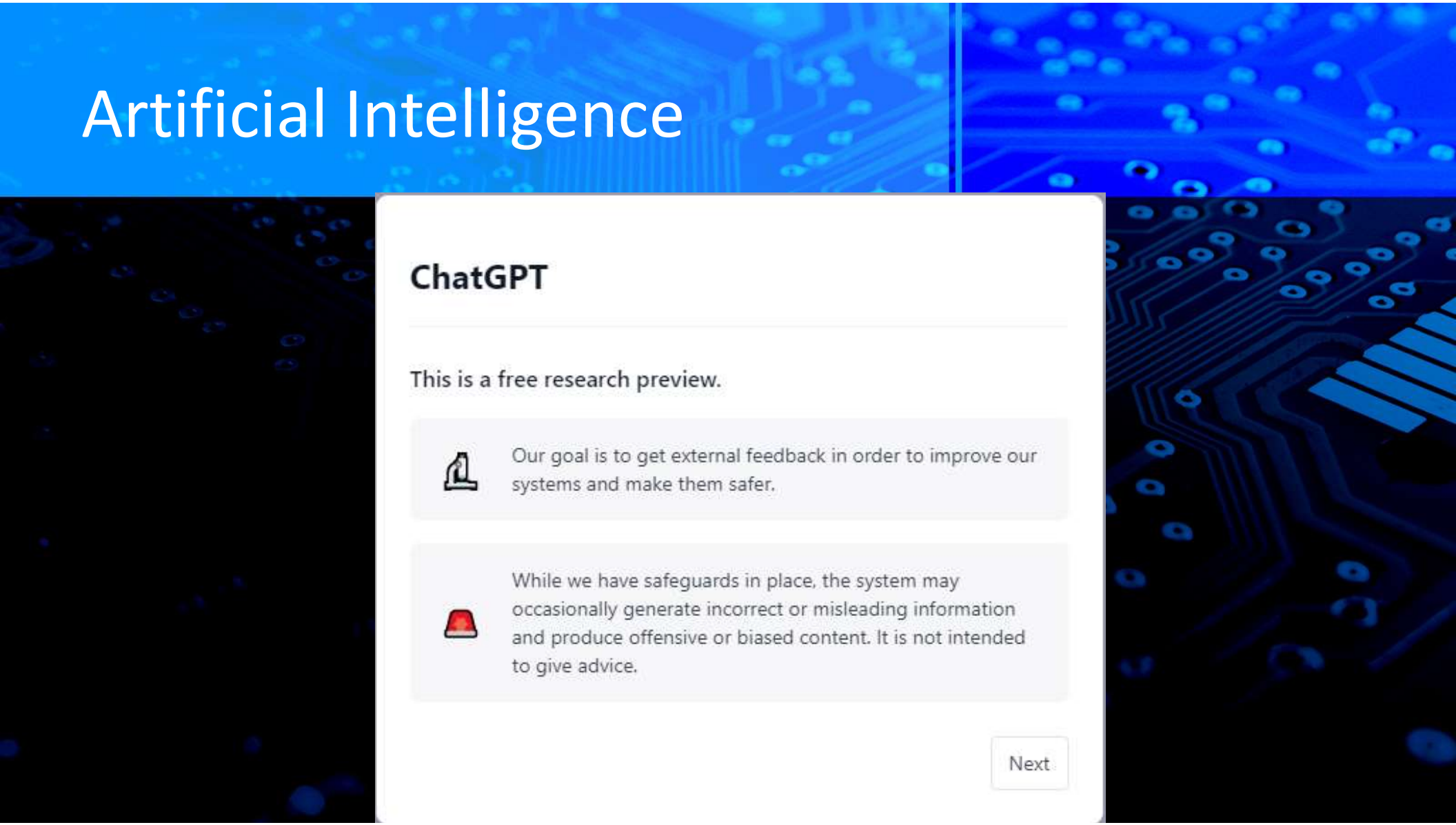
Building a Security Aware Culture

- Leadership buy-in
- Employee training
- Strong policies and procedures
- Continuous communication
- Security champions
- Continuous improvement

Artificial Intelligence

- Open AI
- Google AI Platform (Bard)
- Amazon Web Services AI
- Microsoft Azure AI
- IBM Watson
- Facebook AI

Artificial Intelligence



Artificial Intelligence

Pros of AI:

- Efficiency: AI can perform tasks faster, more accurately, and tirelessly than humans, leading to increased productivity and efficiency in many industries.
- Cost-effective: Implementing AI in many industries can be cost-effective since it can replace human labor, reducing the costs of training, salaries, and benefits.
- Improving quality of life: AI can help people with disabilities, older adults, and patients with chronic illnesses with daily tasks, monitoring health, and improving the quality of life.
- Data analysis: AI can analyze vast amounts of data, enabling businesses to gain insights, make data-driven decisions, and improve customer experience.
- Accuracy: AI can provide consistent and accurate results, minimizing the risk of errors and improving the reliability of tasks.

Artificial Intelligence

Cons of AI:

- Job displacement: The use of AI in many industries can lead to job losses and displacement of human labor, which can lead to economic and social consequences.
- Bias: AI systems can perpetuate and amplify biases and discrimination that exist in society, leading to ethical and social concerns.
- Security risks: AI systems can be vulnerable to cyber attacks, leading to the exposure of sensitive data and security breaches.
- Lack of creativity: AI systems lack the ability to be creative and innovative, which limits their applications in industries that require human intuition and creativity.
- Dependence: The over-reliance on AI systems can lead to a lack of human expertise, decision-making skills, and intuition, leading to possible mistakes and errors.
- Used for nefarious purposes: AI can be used to create phishing emails that are almost undetectable.

Artificial Intelligence

Example of OpenAI

https://chat.openai.com

Questions?