POMS

Reducing Cyber Risk Through Training, Policy & Controls

1

POMS

Upcoming Webinar: Best Practices for Creating Policies Around Employee Misconduct and Child Abuse
Thursday April 27th 11am MST/10am PDT

2

## Contributor

**New Mexico**
- Grant Banash – Senior Risk Control Manager – Technology
  gbanash@pomsassoc.com



3

## What we are going to talk about today

- Training
- Policies
- Controls




4

## What do you have connected to the Internet of Things (IoT) in your home?

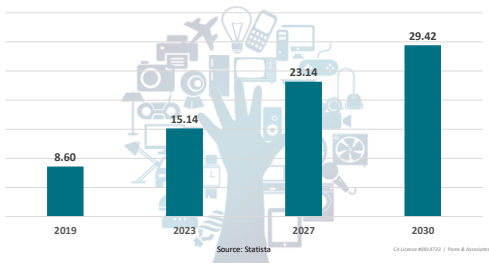
What is the average number of connected devices per household in the US?

**22**



5

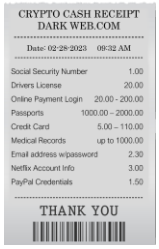
## The number of IoT devices installed worldwide






6

## What is your personal information worth?

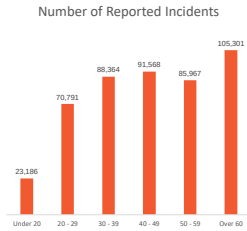


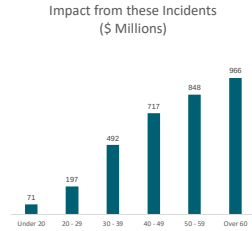

Source: Experian



7

## Who is at most risk of getting hacked?



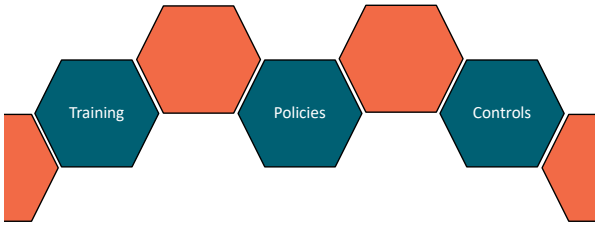




FBI Internet Crime Complaint Center: Internet Crime Report 2020
https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf



8

## How can cybersecurity attacks be best managed?






9


Artificial Intelligence
Deep Fakes



10

## Types of Threats




11

## Not all bad actors gain access within a network

- USB drives
- Public charging stations
- Charging cords
- High powered binoculars or spotting scopes
- Easily accessible doors
- Drones
- Dumpster diving
- Tailgating and piggy backing
- Cell Phones



12

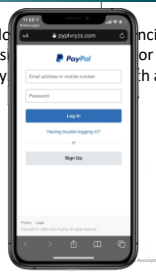
# TRENDS



13

## Phishing

The practice of tricking an internet user into disclo ncial or confidential information. This is usually accomplis or websites. Most common type of attack. 91% of cy h a phishing email.



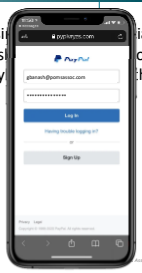
- Spear Phishing
- Whaling
- Pharming – creating fake websites
- Smishing



14

## Phishing

The practice of tricking an internet user in disclosi ial or confidential information. This is usually accomplis or websites. Most common type of attack. 91% of cy h a phishing email.



- Spear Phishing
- Whaling
- Pharming – creating fake websites
- Smishing



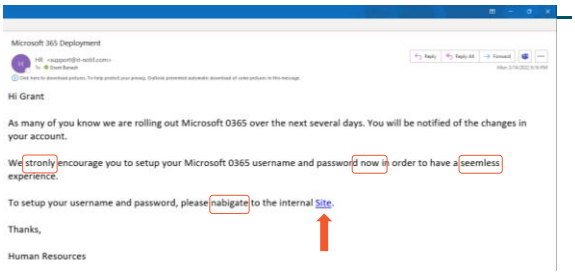
15

## Phishing indicators

- Urgency
- Authority statements
- Poor spelling and grammar
- If something does not feel right, it probably isn't
- Don't be embarrassed to ask for help, Report it if you Click it



16






17

## Social engineering

Is one of the most common and successful malicious techniques. It can also be referred to as "Hacking the Human". It is used to manipulate people into doing things that they do not suspect to be harmful.

- Familiarity/Liking
- Consensus/Social Proof
- Curiosity
- Authority and Intimidation
- Scarcity and Urgency
- Fear



18

## Spoofed Website or Pharming


19

## Malware

Software that will harm or exploit a programable device, service or networks

- Viruses
- Trojans
- Worms
- Ransomware
- Spyware
- Keyloggers
- Adware
- Botnets

20


21

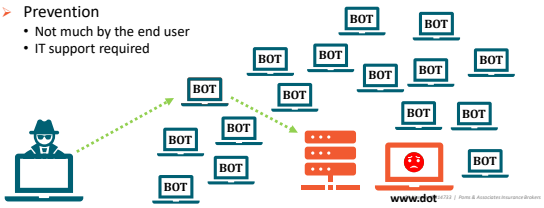
## What are your next steps?

- Who are you going to call?
- Take a picture of the screen
- Disconnect from the network
- Seek help quickly

22

## DDoS – Distributed Denial-of-Service Attack

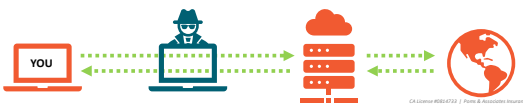
- Internet traffic to overload school network
- Prevents access to critical internet-based services
- Prevention
  - Not much by the end user
  - IT support required




23

## Man-in-the-Middle Attack

- Looking at stealing personal information like banking and login information
- Prevention
  - Avoid public and unsecured Wi-Fi for E-Commerce
  - Verify domain names and browsers before visiting unknow or insecure websites
  - Log out of all online sessions after use
  - Use strong firewalls




24

## Vishing

Or also known as “Voice Phishing”. The bad actor uses the telephone system to gain access to valuable personal or financial information.

- They are usually very nice and polite but can get aggressive and demanding.
- Phishing -Vishing Combo
- Abductions



25

## What can I do?

- Do not ignore updates and patches, Software can have flaws and vulnerability's
- Only download apps from trustworthy sources
- Avoid downloading 3rd party apps
- Use a screen lock on your mobile device
- Back up your data regularly
- If you have done something accidentally that may cause harm, Report it if you Click it



26

# POLICIES



27

## Passwords

- Use a sentence, 3 random words, misspell words, include numbers and symbols
- Long, Random, Unique (for each account)
- Don’t get personal
- Keep work and personal passwords separate
- Do not leave passwords in easy access
- Do not give student access (teacher aids)




28

## Passwords

- Do not leave your computer unlocked when unattended
- Disconnect from the network when away from your computer
- Store your passwords securely
- Use password management services
  - Bitwarden, NordPass, Keeper, LastPass

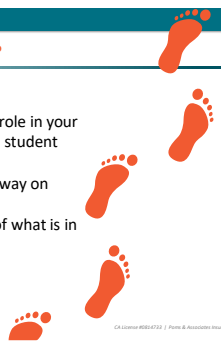
**DON’T GIVE UP…**



29

## What does your Digital Footprint look like?

- Think about what you post online
- Avoid posting information about your role in your organization if it involves working with student sensitive, financial or IT access.
- Avoid posting pictures when you are away on vacation
- During video conferencing, be aware of what is in your background





30

# CONTROLS



31

## Multifactor Authentication (MFA)

- Extra level of protection online
- Very effective even if criminals have your email and password
- Requires users to provide additional verification that is sent to their email or phone or another device
- Many organizations have these systems available to their users




32

## Disclaimer

*Please be advised that insurance coverage cannot be altered, bound, or cancelled by voicemail, email, facsimile, or online, and insurance coverage is not effective until confirmed in writing by a licensed agent. The materials contained herein do not establish a broker relationship with Poms & Associates Insurance Brokers, LLC, and is provided for informational purposes only. A representative of Poms & Associates Insurance Brokers, LLC can provide you with a personalized assessment. Please contact us at 818-449-9300.*




33

## THANK YOU

Grant Banash
Senior Risk Control Manager – Technology
Office: 505-933-6187
gbanash@pomsassoc.com



34