Cybersecurity Training and Best Practices

Katie Kane, Senior Manager
11.30.22

CAPINTECH

The content of this presentation, whether communicated in writing or verbally by partners, employees, or representatives of Capin Crouse LLP, is provided solely for educational purposes. This presentation is not intended to provide legal, accounting, investment, or fiduciary advice. Please contact your attorney, accountant, or other professional advisor to discuss the application of this material to your particular facts and circumstances.

Polling Question 1

Do you want CPE credit?

- Yes
- No

Discussion for Today

- Current Threats
- Employee Roles
- Best Practices and Security Controls
- How to Apply Within Your Organization

Cost of a Data Breach

$9.44M

Average cost of a data breach in the United States

$4.35M

Global average total cost of a data breach

IBM Security – Cost of a Data Breach Report 2022

Cyber Attacks

- Most common cyber attacks used in data breaches:
  - Ransomware
  - Malware
  - Phishing and email impersonation

Top 5 Industries

- Healthcare
- Finance and insurance
- Government
- Education
- Critical infrastructure

Polling Question 2

How prepared do you feel your organization is?

- Very prepared; we do not need any more assistance.
- We could use a little guidance.
- We are completely unprepared and need as much help as possible.

Recent Breaches

Colonial Pipeline Company May 2021

- Result of a single compromised VPN password that granted access on April 29, 2021
  - Account was enabled but not active
- Password since discovered inside a batch of leaked passwords on the dark web
  - Colonial employee may have used the same password on another account that was previously hacked

Microsoft Power Apps — August 2021

- Approximately 38 million records across 47+ organizations
- Various types of records exposed
  - Employee records; COVID testing, tracing, and vaccinations; names, dates of birth, Social Security numbers, addresses, and demographic details
- Misconfiguration was by third party, not Microsoft directly

Block (Square) — December 2021

- Breached by a former employee in December 2021
- Included customer names, brokerage account numbers, and other data, such as portfolio value and stock trading activity
- Number of customers not disclosed, but contacted over 8 million customers to inform them of the incident

Crypto.com — January 2022

- Took advantage of a vulnerability and hacked the exchange
- Over $34 million in cryptocurrency stolen from the wallets of 483 users
- Multi-factor authentication controls were bypassed
- All withdrawals were halted for approximately 14 hours while investigation took place

Okta — March 2022

- Attacker posted on Telegram channel that they breached Okta
- Approximately 2.5% of customers have been exposed
- Breached through Okta's third-party customer support provider
- Attacker criticized Okta's security practices in their Telegram post

Microsoft March 2022

- Attacker posted on Telegram channel that they breached Microsoft
- Only a single account was compromised
- Security team was able to stop the attack before the hacker could move further
- The hacker group has stated that their motivations were purely financial

OneTouchPoint April 2022

- Vendor providing printing and mailing services to its clients
- Apparent ransomware incident affecting more than three dozen of its health insurer clients and nearly 1.1 million individuals
- In April, discovered encrypted files on certain computer systems
- Affected systems contained information provided by health insurer customers, but it was not determined what personal information was accessed

Flagstar Bank June 2022

- 1.5 million customers affected in a data breach detected in June 2022
- Second incident in a year
- Attack originally occurred in December 2021, and first incident occurred in March 2021
- Breach was due to an Accellion software zero-day vulnerability

Avamere Health Services LLC July 2022

- Business associate providing IT services to healthcare entities
- Resulted in two related health data breaches affecting nearly 100 covered entities and a total of nearly 381,000 individuals being reported to federal regulators
- Included full names, addresses, dates of birth, driver's license or state identification numbers, Social Security numbers, claims information, financial account numbers, medication information, lab results, and medical diagnosis/conditions information

Cisco — August 2022

- Yanluowang ransomware gang breached the corporate network by gaining access to servers via an employee's personal Google account
- Breach was detected after the group published data stolen during the breach online
- Security experts have suggested the data is not of "great importance or sensitivity" and that the hackers may have been looking for credibility

LastPass — August 2022

- Attackers stole source code as well as some proprietary technical information
- A developer's user account was compromised two weeks prior to the hack
- Customer data was not involved in the hack

Optus September 2022

- Australian telecom company, which has 9.7 million subscribers, suffered a large data breach
- Names, dates of birth, phone numbers, and email addresses may have been exposed, along with some physical addresses and documents (drivers licenses and passport numbers)
- Breached firewall

Revolut September 2022

- Financial services organization
- An unauthorized third party accessed personal information pertaining to tens of thousands of the app's clients
- 50,150 customers reportedly impacted. The State Data Protection Inspectorate in Lithuania stated email addresses, full names, postal addresses, phone numbers, limited payment card data, and account data were likely exposed.

Uber September 2022

- Uber's computer network was breached
- Several engineering and communications systems taken offline while investigation took place. Deemed a "total compromise" by one researcher. Email, cloud storage, and code repositories were sent to security firms and *The New York Times* by hacker.
- Uber employees found out their systems were breached after the hacker broke into a staff member's Slack account and sent messages confirming they had compromised the network

Facebook October 2022

- Meta stated that it has identified more than 400 malicious Android and Apple apps that target online users, trying to steal their Facebook login credentials
- Apps were listed on the Google Play Store and Apple's App Store and disguised as photo editors, games, VPN services, business apps, and other utilities

Polling Question 3

Has your organization experienced any major vulnerabilities within your environment?

- Yes
- No
- Unknown


REPUTATION
RISK

Remote Work Requirements

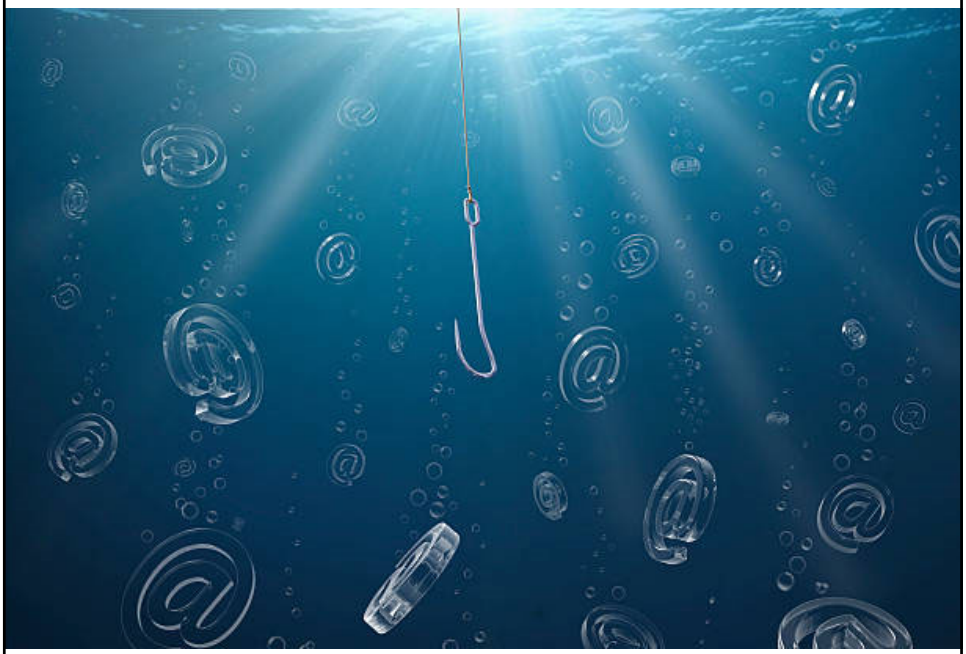
- Employees should be authorized
  - Suitability
  - Responsibilities
  - Acceptable use
- Only approved devices should be utilized
- Security authentication requirements

Remote Work Requirements

- Protect access and login details from non-authorized users
- Updates should be applied regularly to devices
- Company-owned devices should not be utilized for personal use
- Consider protection of sensitive information

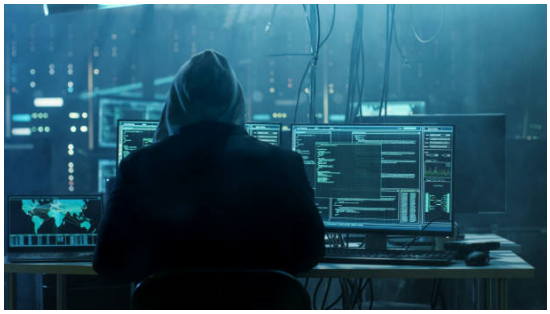
Remote Work Requirements

- Office requirements carry over to the home
- Don’t forget verification procedures where applicable
- Continue to follow the Information Security Program guidelines
- Practice skepticism; when in doubt, ask!



Phishing Objectives

- Install malware
- Steal credentials
- Obtain information
- Perform a task



Verizon Data Breach Investigation Report

- 3% of users will click on any phishing campaign
- Data compromised:
  - 85% credentials
  - 17% personal info
  - 4% medical records
- Motives:
  - 95% financial

Examples

[redacted] <box@itservermailbox.net>
Tue 12/18/2018 6:11 AM
[redacted]

EXTERNAL

Morning [redacted]

I would like to update my direct deposit details as i have just switched banks, would the change be effective for the next pay date?

Thanks

[redacted]

Examples

Zelle Payment Confirmation Needed

ZN Zelle Notifications <noreply8@onlineinfoalerts.com>
To: Katie Kane
Wednesday, July 29, 2020 at 7:26 PM

EXTERNAL

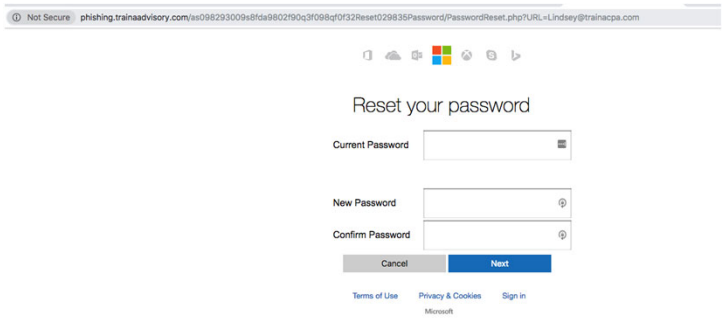
Zelle

Payment Confirmation Needed

Hi Katie,
We are emailing you to inform you receiveed a Zelle payment, but we will need you to confirm your account information before we can complete the processing of the payment.
To help us resolve this issue, please log in to your account and go to the Payment Confirmations.
If you have any questions or need assistance, please feel free to contact us, as we are glad to help.

Sincerely,
Zelle

Examples



Examples

FW: Wire request

MA

To: Katie Kane

Today at 4:33 PM

To protect your privacy, some pictures in this message were not downloaded. Download pictures

I am currently in a meeting and need your assistance. Can you please process the below request. This is urgent, as you can see from the message below. Please prepare the confirmation and send to me once you have completed this request.

Thank,

Monty

Sent from my iPhone

From: Mr. George Winter
Date: Tuesday, March 9, 2021 at 8:49 AM
To:
Subject: Personal request

I am in need of your assitance. I need to have the following funds sent to my mother's account at Progressive National Bank in the amount of $5,000.00. The form with the related account information is attached below. Please prepare a confirmation and send back to me once this has been completed. If you have any questions, please let me know. Thank you so much. This is an urgent matter, as my mother's nursing home payment is past due, and I need to get this to them ASAP. I will be on a flight for several hours and will not be available by phone or email. As you can see this is an urgent matter and will need this processed as soon as possible.

account information.pdf

Thanks,
George

Examples of ransomware phishing email

Subject: Your account is being used by another person!

EXTERNAL

Hi, stranger!

I hacked your device, because I sent you this message from your account.
If you have already changed your password, my malware will be intercepts it every time.

You may not know me, and you are most likely wondering why you are receiving this email, right?
In fact, I posted a malicious program on adults (pornography) of some websites, and you know that you visited these websites to enjoy (you know what I mean).

While you were watching video clips,
my trojan started working as a RDP (remote desktop) with a keylogger that gave me access to your screen as well as a webcam.

Immediately after this, my program gathered all your contacts from messenger, social networks, and also by e-mail.

What I've done?
I made a double screen video.
The first part shows the video you watched (you have good taste, yes ... but strange for me and other normal people),
and the second part shows the recording of your webcam.

What should you do?

Well, I think $670 (USD dollars) is a fair price for our little secret.
You will make a bitcoin payment (if you don't know, look for "how to buy bitcoins" on Google).

BTC Address: 1GjZSJnpU4AfTS8vmre6rx7eQgeMUq8VYr
(This is CASE sensitive, please copy and paste it)

Remarks:
You have 2 days (48 hours) to pay. (I have a special code, and at the moment I know that you have read this email).

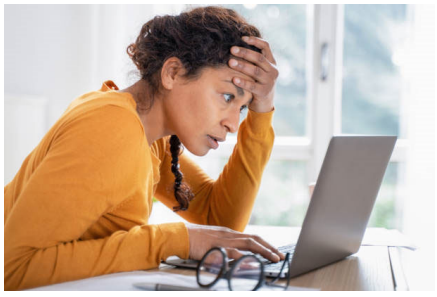
If I don't get bitcoins, I will send your video to all your contacts, including family members, colleagues, etc.
However, if I am paid, I will immediately destroy the video, and my trojan will be destruct someself.

If you want to get proof, answer "Yes!" and resend this letter to youself.
And I will definitely send your video to your any 11 contacts.

This is a non-negotiable offer, so please do not waste my personal and other people's time by replying to this email.

Other Examples

- Posing as vendor to change bank account information
- Use similar domain name
  - joe@alliedconsulting.com
  - joe@alliedconsulting.com
  - aliiedconsulting.com



Warning Message

The below message in red has been added to all messages received from an outside party.

- Helps to identify fraudulent emails (email from a director, etc.)

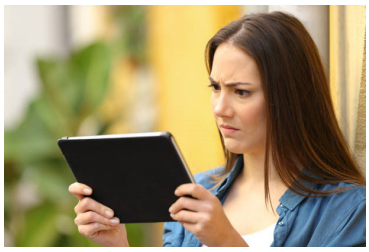
CAUTION: This email originated from outside of the organization. Do not click links or open attachments unless you recognize the sender and know the content is safe.

Phishing – How to Detect

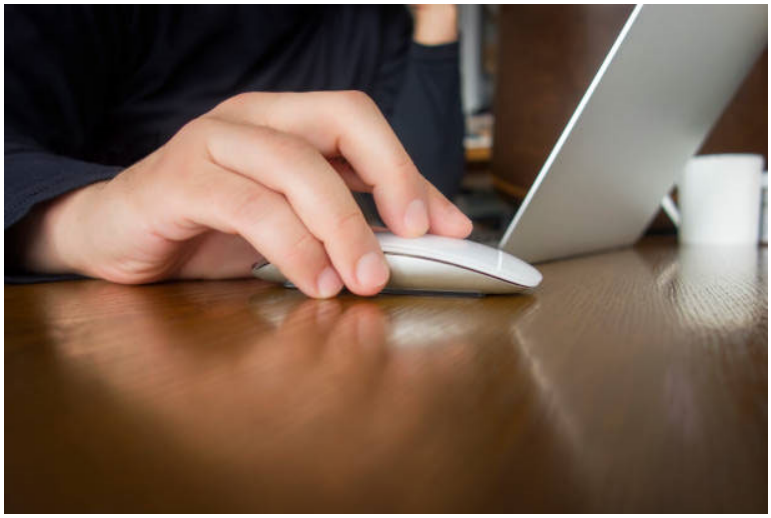
- Inspect for typos
- Check email address and domain name
- Click correctly
  - Hover over link
  - Right click and copy
  - Visit website manually

Phishing – How to Detect

- It doesn't feel right
- Tone is off
- Urgent/threatening
- Unfamiliar or unexpected



One click… that's all it takes!



Security Concerns

- Third-party vendors
  - New relationships
  - Existing vendors
- Organization responsibilities
- End-user assistance

New Third-Party Vendor Relationships

- General inquiry
- Workforce
- Information security
  - Cloud storage
- Policy documentation

New Third-Party Vendor Relationships

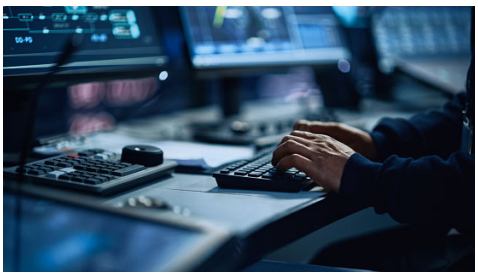
- Review System and Organization Controls (SOC) reports
- Review any contracts
- Research what others have implemented
  - Hardening controls
  - Proper implementation procedures
  - Possible mistakes

Existing Vendor Relationships

- Periodic oversight procedures
  - Review of audit reports
  - Backup or disaster recovery testing
  - Financial condition
  - Existing contracts
  - Vendor oversight

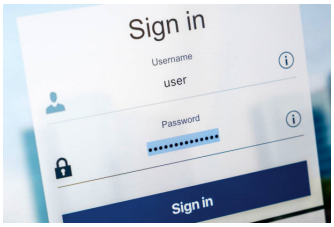
Organizational Responsibilities

- Ongoing monitoring of critical vendor services
  - Patch management reporting
  - Malware management reporting
  - Backup process



User Provisioning and Access

- Minimum rights for users
- Review regularly
  - Job transfers
  - No longer needed
  - Vendors
  - Service accounts



Password Security

- Numbers, characters, symbols
- Avoid common words
- Change often and when compromised
- Length – 8…12…??

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2022

Number of Characters	Numbers Only	Lowercase Letters	Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters	Numbers, Upper and Lowercase Letters, Symbols
4	Instantly	Instantly	Instantly	Instantly	Instantly
5	Instantly	Instantly	Instantly	Instantly	Instantly
6	Instantly	Instantly	Instantly	Instantly	Instantly
7	Instantly	Instantly	2 secs	7 secs	31 secs
8	Instantly	Instantly	2 mins	7 mins	39 mins
9	Instantly	10 secs	1 hour	7 hours	2 days
10	Instantly	4 mins	3 days	3 weeks	5 months
11	Instantly	2 hours	5 months	3 years	34 years
12	2 secs	2 days	24 years	200 years	3k years
13	19 secs	2 months	1k years	12k years	202k years
14	3 mins	4 years	64k years	750k years	16m years
15	32 mins	100 years	3m years	46m years	1bn years
16	5 hours	3k years	173m years	3bn years	92bn years
17	2 days	69k years	9bn years	179bn years	7tn years
18	3 weeks	2m years	467bn years	11tn years	438tn years

HIVE SYSTEMS

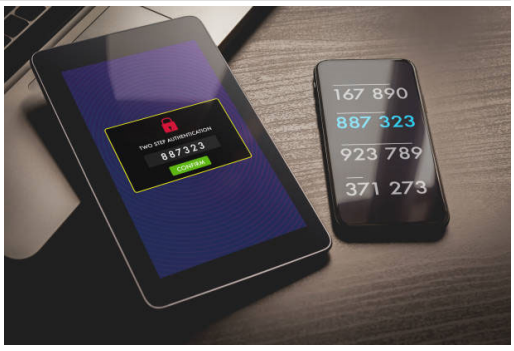
› Learn about our methodology at hivesystems.io/password

Password Security

- Unique and private passwords
  - Password manager?
- Business ≠ personal
- Account lockout and inactivity threshold
- Biometrics
- Layered security

Multi-Factor Authentication

- Critical for all cloud applications
  - Remote access
  - Email
  - AWS/Azure



- Consider IP address, time and day restrictions
- Mobile devices, email message, tokens

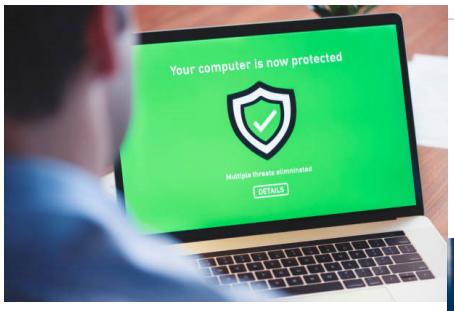
Email

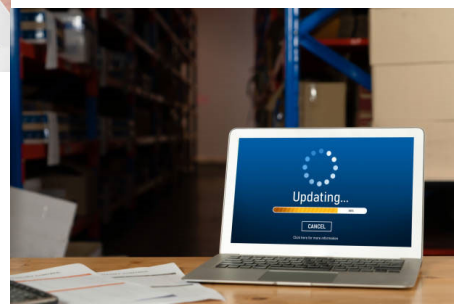
- Easily spoofed or hacked
- Not all services are encrypted
- Confidential email MUST be secured
  - Sending and receiving
- Limit or restrict web mail
- Implement response procedures to constituent requests via email

Wi-Fi Networks

- Ensure properly secured home Wi-Fi
  - Be wary of public Wi-Fi; use a VPN!
- Secure password for access
- Guest network for non-business systems
- Keep personal and business devices up to date

Malware & Patch Management





Device Management

- Centralized system
  - All devices present
  - Receive latest updates or definition files
  - Remediate issues
- Limited user rights
  - Downloaded apps from Internet
  - Browser add-ons

Web Surfing

- Avoid questionable websites
- Be cautious when downloading
- Use updated browsers
- Inspect URLs
- Be wary of malvertising
- Don’t save credentials in browser

Social Networking

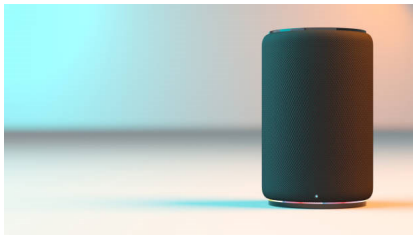
- Impersonation
  - Phishing and vishing
- Identity theft
- Pretexting
- Security questions and answers
- Data not always private

Data Storage

- Cloud apps can be accessed from any location on any device
- Risk of apps being accessible on unauthorized devices, resulting in data management concerns

Internet of Things (IoT) Devices

- Inventory devices in use
- Layered security controls
  - Strong passwords
  - Evaluate data and analytics sharing
  - Patching procedures
  - Disable features
  - Segmented network
- Consider listening capability



Shadow IT

- Apps or devices that are utilized without IT knowledge
  - Personal or mobile devices
- Rogue cloud services
  - Personal email, document scanning, cloud storage
- Appropriate authorization procedures

Polling Question 4

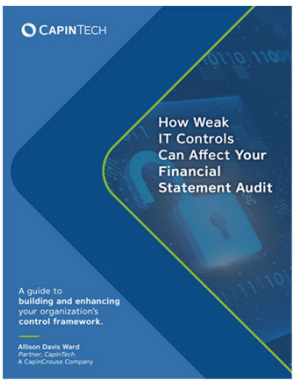
Do you feel that this presentation was helpful?

- I feel much more knowledgeable about the topic.
- I learned a little, but it is still overwhelming.
- I have a lot more to learn when it comes to information security management.

Key Takeaways

- New threats happening every day — no one is immune!
- Loss of reputation can be significant
- Manage vendor relationships appropriately
- Maintain adequate security controls
  - Provide necessary tools for users
  - Doesn't have to be expensive!
  - Train to build culture of awareness

New E-book Now Available!



Download your free copy!
Scan this QR code or visit
capincrouse.com/it-controls

Questions?

Thanks!

Katie Kane, Senior Manager

kkane@capincrouse.com

505.50.CAPIN ext. 2007

CAPINTECH