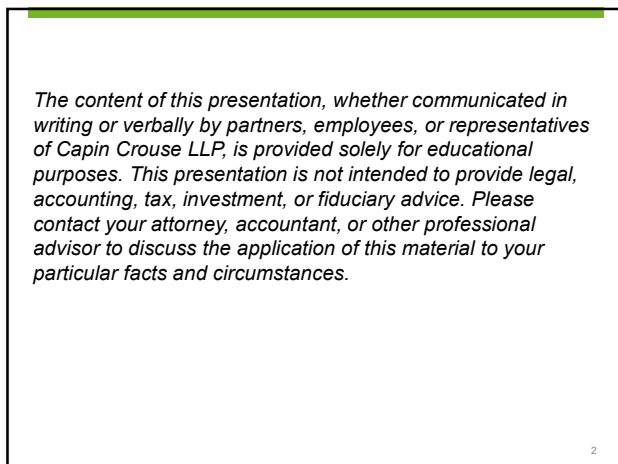
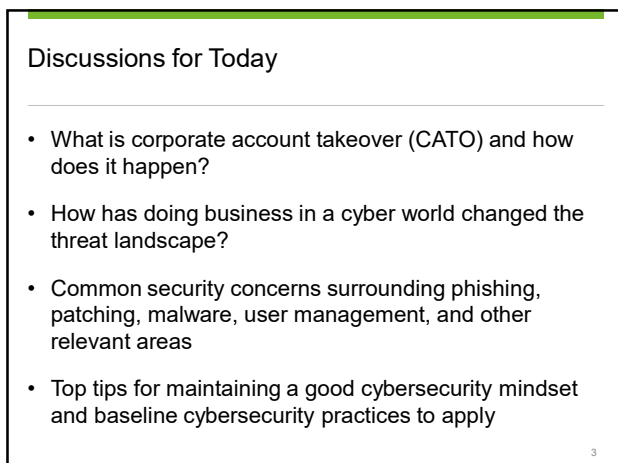




1



2



3



What is CATO?

 CAPINTECH

4

CATO


- Theft of login credentials
- Brute force credential cracking
- Phishing
- Data theft through malware
- Man-in-the-middle attacks

5

5

Account Takeover

- Criminals gain access to customer finances or data
 - Unauthorized transactions or funds transfer
 - Creation of new/fake online banking users
 - Stolen customer information
- Criminals gain access to bank information



6

6

Account Takeover

- How is this accomplished?
 - Lack of security
 - Phishing/malware
 - Credential stuffing
 - Email compromise



7

7

Account Takeover

- Lack of security
 - Logged into Internet banking
 - Password management tool auto-populates passwords
 - Sends code to text or email on device



8

8

Account Takeover

- Phishing and malware
 - Exploited devices allow access
 - Sensitive information obtained
- Credential stuffing



9

9

Account Takeover

- Email compromise
 - Emails appear legitimate
 - Requests seem normal
 - Utilize spoofed/fake email accounts or malware



10

10



11

11



Threat Landscape

 CAPINTECH

12

ChatGPT

March 2023

- Chatbot leaked personal data of customers
- Included active users' first name, last name, email address, payment address, last four digits of credit card number, and card expiration date

13

13

Activision

February 2023

- Breach occurred in December 2022, company revealed in February 2023
- Employee's credentials were compromised in a phishing attack, which was used to compromise the system

14

14

Twitter

December 2022

- More than 200 million Twitter profiles were sold in a data collection sale (compromise a result of previously compromised information)
- Vulnerable application programming interface (API) was compromised

15

15

Dropbox

November 2022

- Unknown attacker gained access to credentials, data containing secrets within the private GitHub repositories
- Secrets (plain text) included API keys and other credentials
- A few thousand names and email addresses belonging to Dropbox employees were also exposed
- Result of a developer falling victim to a phishing attack

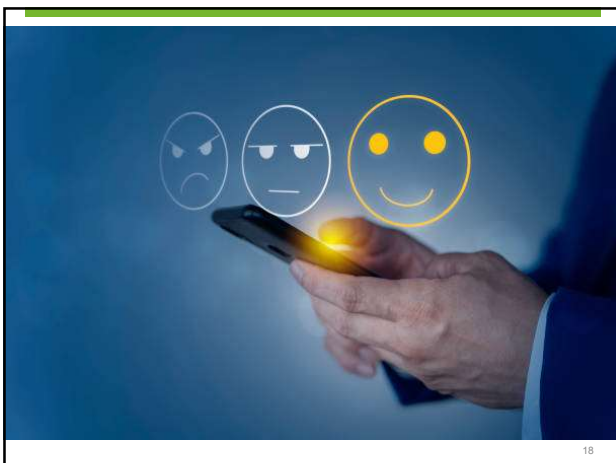
16

16



17

17



18

18



19

19

Phishing

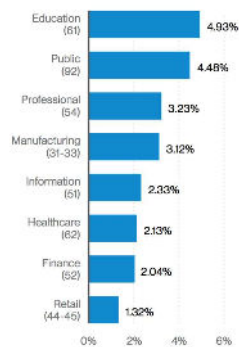
- Malware installation
- Credential capturing
- Compromise of information
- Unauthorized changes or tasks



20

20

Phishing Failure by Industry




© 2023 PhishingBox, LLC

21

21

Examples

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

****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]

22

22

Examples

From: Susan Fry [mailto:sfry@yourcompany.com]
Sent: Tuesday, January 9, 2018 9:25 AM
To: Hamil, James <james.hamil@yourcompany.com>
Subject: Please handle ASAP

– External email. Forward any suspicious emails to bad@yourcompany.com –

Hi James,

I'm currently tied up in a meeting for the next six hours, but we have a vendor saying we're late on paying an invoice. Can you handle the attached ASAP? I can't take calls, so just email me if you have questions.

Susan Fry
Chief Operating Officer
sfry@yourcompany.com

Sent from my iPhone, please excuse typos

23

23

Examples

Microsoft account unusual sign-in activity

 Microsoft Team <outlook@microsoft.com>
View signature

****EXTERNAL****

Email account

Unusual sign-in activity

We detected something unusual about a recent sign-in to the email account **[REDACTED]** to help keep you safe, we required an extra security challenge.

Sign-in details:

Country/region: Krasnodarskiy kray, Russia

IP Address: 31.181.250.117

If this was you, then you can safely ignore this email.

If you are not sure this was you, a malicious user might have your password. It is strongly advised that you change your password immediately.

[Reset Password](#)

Thanks,

Mail support team

24

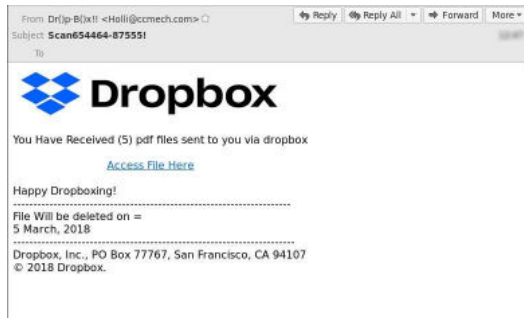
24

Examples

25

25

Examples



26

26

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



27

27

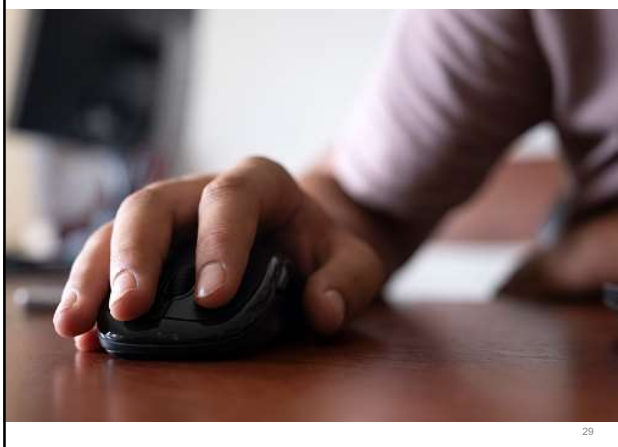
Phishing – How to Detect

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



28

28



29

29

Protection and Prevention

- Banking controls
 - Multi-factor authentication
 - New user alerts
- Device authentication and restrictions
- Enhanced controls for high-risk transactions
- User training



30

30

Protection and Prevention

- Company controls
 - Employee education
 - Proper security
 - Monitor for suspicious activity
 - Understand responsibilities



31

31



Baseline Cyber Practices



32

32

Security Concerns

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



33

33

New Third-Party Vendor Relationships

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



34

34

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



35

35

Existing Vendor Relationships

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



36

36

Organizational Responsibilities

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



37

37

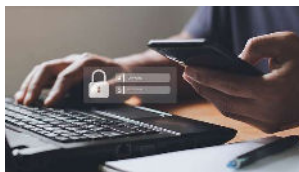


38

38

User Provisioning and Access

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



39

39

Password Security

- Numbers, characters, symbols
- Avoid common words
- Change often and when compromised
- Length – 12, 14, ???



40

40

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	172m 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



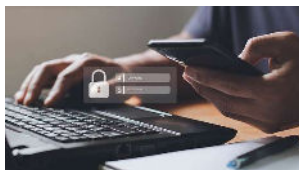
> Learn about our methodology at hivesystems.io/password

41

41

Password Security

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



42

42

Multi-Factor Authentication

- Critical for all cloud applications
 - Remote access, email, AWS/Azure
- Mobile devices, email message, tokens
- Consider IP address, time and day restrictions



43

43

Email Security

- Encryption for confidential/sensitive information
 - Sending and receiving
- Auto-forwarding disabled
- If not needed, limit or restrict web mail
- Strip links within incoming email



44

44

Wi-Fi Networks

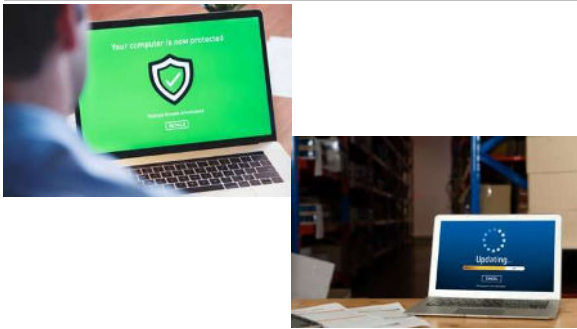
- Ensure properly secured Wi-Fi, including those at home offices (WPA2 encryption or better)
 - Avoid use of public Wi-Fi; if necessary, use a VPN!
- Secure password for access
- Guest network for non-business systems (segregate)
- Keep personal and business devices up to date
- Consider the use of mobile hotspots



45

45

Malware and Patch Management



46

46

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



47

47

Web Surfing

- Avoid questionable websites
- Be cautious when downloading
- Use updated browsers
- Inspect URLs
- Be wary of malvertising



48

48

Social Networking

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



49

49



50

50

Data Storage

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



51

51

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



52

52



53

53

Remote Access Tools

- VPNs, LogMeIn, GoToMyPC
- Increase in end users
- Require proper security measures
 - Quick fixes vs. long-term solution
- Does this affect strategic planning?



54

54

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

55

55



56

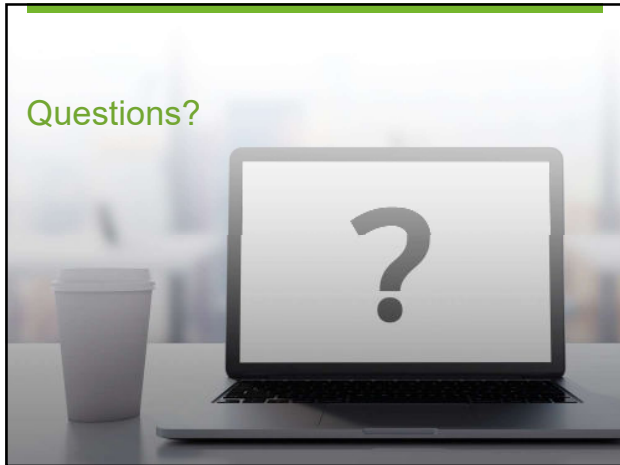
56

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

57

57



58




Thank you.

Katie Kane, Senior Manager

✉ kkane@capincrouse.com

📞 505.50.CAPIN ext. 2007

© 2023 Capin Technology LLC



59