



1


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, tax, 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.

2


Discussions for Today

- What is corporate account takeover (CATO) and how does it happen?
- How has doing business in a cyber world changed the threat landscape?
- Common security concerns surrounding phishing, patching, malware, user management, and other relevant areas
- Top tips for maintaining a good cybersecurity mindset and baseline cybersecurity practices to apply

3



What is CATO?



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
 - Staying 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



11



Threat Landscape



12

FTC Consumer Reports for 2023

- Fraud losses – \$10 billion
- Investment scams – \$4.6 billion
- Imposter scams – \$2.7 billion

Source: [As Nationwide Fraud Losses Top \\$10 Billion in 2023, FTC Steps Up Efforts to Protect the Public](#), Federal Trade Commission

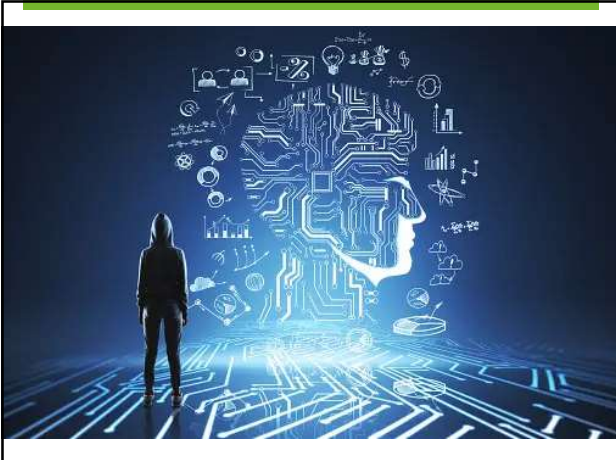
13



14



15



16

Phishing

- Email phishing
- Spear phishing
- Whaling
- Business email compromise
- Voice phishing
- HTTPS phishing
- Clone phishing
- SMS phishing
- Pop-up phishing
- Social media phishing
- Angler phishing
- Evil twin phishing

17

17

Phishing Failure by Industry


- Agriculture and Food Services – 8.2%
- Banking and Financial Institutions – 7.1%
- Legal Sector – 7.1%
- Automotive Part Manufacturers – 7.0%
- Government Organizations – 6.8
- Insurance Sector – 6.7%

Source: PhishingBox, LLC 18

18

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



19

Phishing – How to Detect

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




20



21

Protection and Prevention


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



22

Protection and Prevention

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



23




Baseline Cyber Practices

CAPINTECH

Security Concerns

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



25

25

New Third-Party Vendor Relationships

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



26

26

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



27

27

Existing Vendor Relationships

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



28

28

Organizational Responsibilities

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



29

29




30

30

User Provisioning and Access

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




31

31

Password Security

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



32

32

TIME IT TAKES A HACKER TO BRUTE FORCE YOUR PASSWORD IN 2023

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	1 sec	2 mins	4 mins
8	Instantly	Instantly	78 secs	2 mins	4 mins
9	Instantly	3 secs	24 mins	2 hours	6 hours
10	Instantly	1 min	21 hours	5 days	2 weeks
11	Instantly	32 mins	1 month	10 months	3 years
12	1 sec	14 hours	6 years	63 years	220 years
13	4 secs	2 weeks	142 years	81 years	1k years
14	52 secs	1 year	7k years	202k years	7m years
15	30 mins	22 years	895 years	12m years	77 m years
16	4 hrs	73 years	86 m years	775k years	3m years
17	14 hours	18k years	20m years	48m years	390k years
18	6 days	48k years	115m years	2m years	26m years


[Learn how we made this table at: hivesystems.io/password](https://hivesystems.io/password)
33

33

Password Security

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



34

34

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



35

35

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



36

36

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



37

37

Malware and Patch Management



38

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



39

39

Web Surfing

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



40

40

Social Networking

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



41

41



42

42

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



43

43

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



44

44




45

45

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?



46

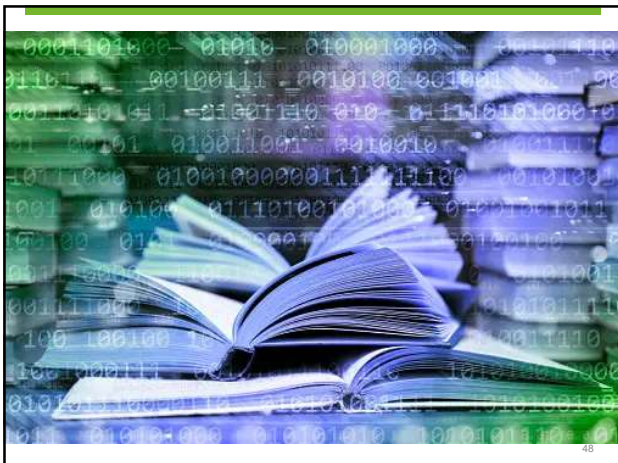
46

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

47

47



48

48

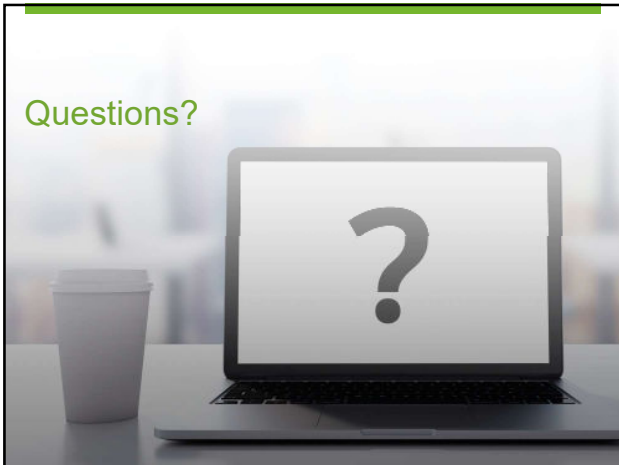
Key Takeaways

- 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

49

49

Questions?




50

Thank you.

Katie Herbert, Senior Manager

✉ kherbert@capincrouse.com

📞 505.50.CAPIN ext. 2007

© 2024 Capin Technology LLC 

51
