

2024 Cybersecurity and Corporate Account Takeover Training Board of Directors



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.

- ### Discussions for Today
- Current threat landscape and lessons learned
 - Common security concerns surrounding phishing, patching, malware, user management, and other relevant areas
 - Corporate Account Takeover (CATO)
 - Best practices for mitigating these threats and steps for applying these practices within your organization



Threat Landscape



Cloudflare February 2024

- Hacked using authentication tokens stolen in Okta breach
- Internal Atlassian server was breached
- Did not impact Cloudflare customer data or systems

5

AnyDesk February 2024

- Breach of production servers
- Hackers reset passwords
- AnyDesk revoked security-related certificates and remediated or replaced systems as necessary

6

Bank of America

February 2024

- Result of a service provider hack in late 2023
- Customer personally identifiable information (PII) exposed (names, addresses, Social Security numbers, dates of birth, and financial information, including account and credit card numbers)
- 57,028 people were directly impacted

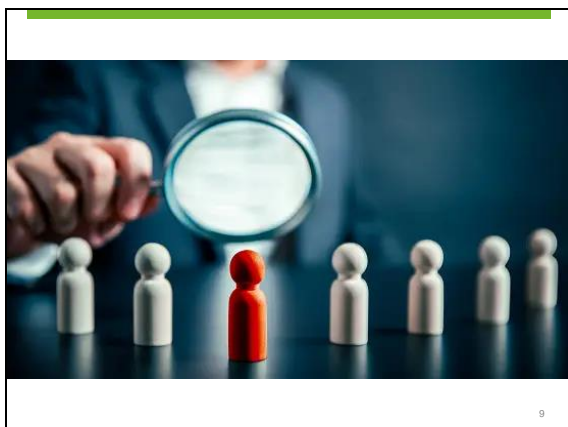
7

Facebook Marketplace

February 2024

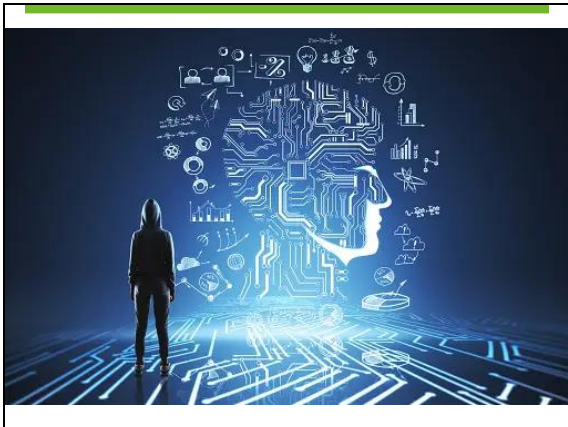
- Partial Facebook Marketplace database stolen after a Meta contractor's system was hacked
- PII exposed (names, phone numbers, email addresses, Facebook IDs, and Facebook profile information)
- Not the first incident of this kind that Meta has experienced in recent years

8



9





Phishing

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

12

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

13

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



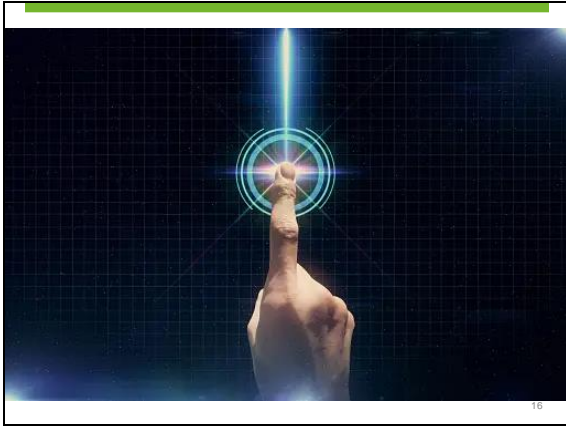
14


Phishing – How to Detect

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




15






Verification Procedures



Customer & Vendor Verification



In-Person Requests

- Beware of forged identification documents
- Secret PIN
- Proper documentation



19

Requests Via Phone

- Verify caller ID
- Call back with known phone number
- Secret PIN
- Knowledge-based questions
 - What is your bank's policy?



20

Requests Via Email

- Do not exchange confidential information
- Beware of spoofed email addresses
- Email customers with verified email address
- Utilize alternative methods of communication (e.g., phone, in-person, secure message system)



21

Requests Via Text

- Never send sensitive information via text
- Not secure form of communication
- Who is authorized?
- What is appropriate?



22



What is CATO?



CATO

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

24

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



25

Account Takeover

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



26

Account Takeover

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



27

Account Takeover

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



28

Account Takeover

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



29



Protection and Prevention

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



31



Baseline Cyber Practices



Security Concerns

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



33

New Third-Party Vendor Relationships

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



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

Existing Vendor Relationships

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



36

Organizational Responsibilities

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



37



38

End-User Assistance

If you see something, say something!



39

User Provisioning and Access

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



40

Password Security

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



41

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 secs	4 secs
8	Instantly	Instantly	28 secs	2 mins	5 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	4 months	10 months	3 years
12	1 sec	14 hours	6 years	53 years	226 years
13	5 secs	2 weeks	332 years	3k years	15k years
14	52 secs	1 year	17k years	202k years	1m years
15	9 mins	27 years	896k years	12m years	77m years
16	1 hour	713 years	46m years	779m years	58m years
17	14 hours	18k years	26m years	48bn years	380bn years
18	6 days	481k years	126bn years	2tn years	26tn years



> Learn how we made this table at hivesystems.io/password

42

Password Security

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



43

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



44

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



45

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



46

Malware and 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



48

Web Surfing

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



49

Social Networking

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



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



52

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



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?



55

Shadow IT

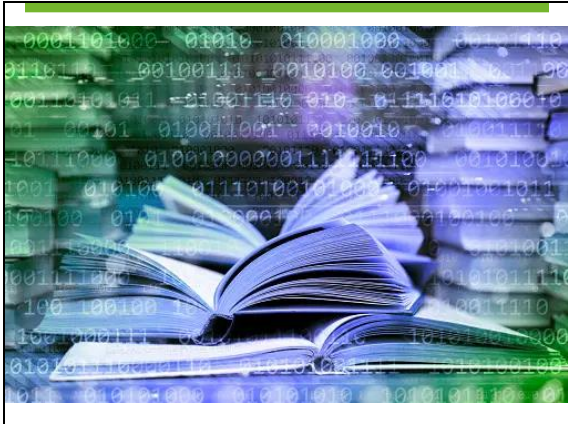
- Apps or devices that are utilized without IT knowledge
 - Personal or mobile devices
- Rogue cloud services
 - Personal email, document scanning, cloud storage
- Appropriate authorization procedures

56

Evolving Technologies



57

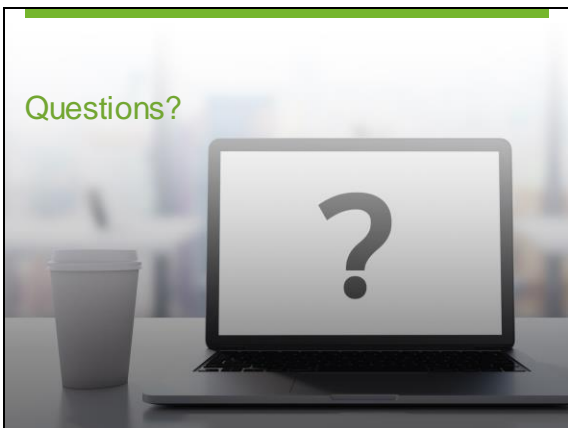


Key Takeaways

- 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

59

Questions?



Thank you.

Katie Herbert, Senior Manager

✉ kherbert@capincrouse.com

☎ 505.50.CAPIN ext. 2007

© 2024 CapinTech LLC

