

[illegible]

1

The content of this presentation, whether communicated in writing or verbally by partners, employees, or representatives of CapinTech, 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



What is Corporate Account Takeover (CATO)?

 **CAPINCROUSE**
A Division of the Davis, Phipps & Hargrave

3

CATO

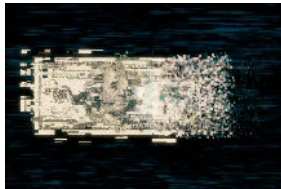
- Theft of login credentials
- Brute force credential cracking
- Phishing
- Data theft through malware
- Man-in-the-middle attacks



4

Account Takeover

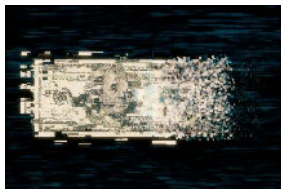
- Criminals gain access to customer finances or data
 - Unauthorized transactions or funds transfer
 - Creation of new/fake online banking users
- Stolen customer information
- Criminals gain access to bank information



5

Account Takeover

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



6

Account Takeover

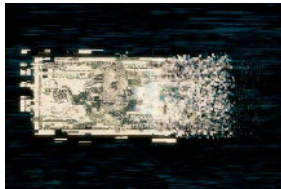
- Lack of security
 - Staying logged into Internet banking
 - Password management tool auto-populates passwords
 - Sends code to text or email on device



7

Account Takeover

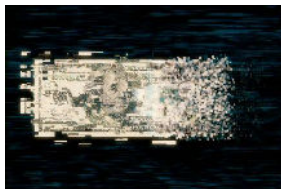
- Phishing and malware
 - Exploited devices allow access
 - Sensitive information obtained
- Credential stuffing



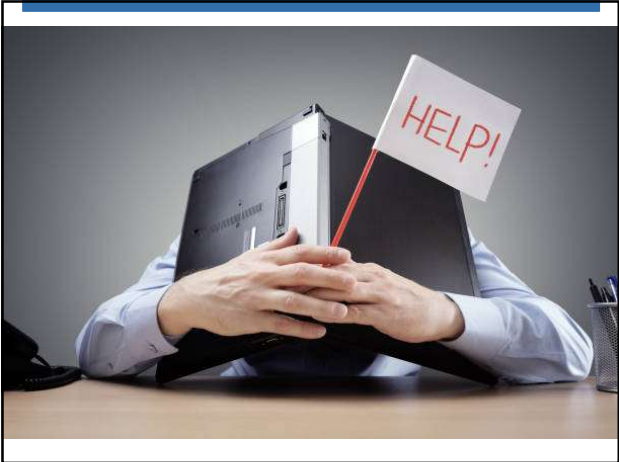
8

Account Takeover

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



9



10

Threat Landscape

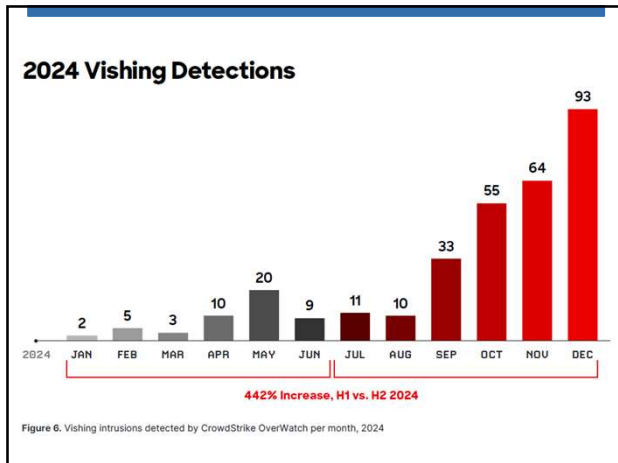
11

FTC Consumer Reports for 2024

- Fraud losses – \$12.5 billion
- Investment scams – \$5.7 billion
- Imposter scams – \$2.95 billion

Source: Federal Trade Commission

12



13

Social Engineering

- FAMOUS CHOLLIMA employed fictitious LinkedIn profiles with genAI-created text and fake profile images
- Deepfake video and voice clones enabled business email compromise (BEC) schemes
- Studies validated effectiveness of genAI in phishing
- China-aligned, LLM-powered Green Cicada network posted coordinated inauthentic behavior on social media
- Russia-aligned operators used LLMs to spread disinformation on social media
- GenAI was used during Indian election season to create videos and images

Source: CrowdStrike 2025 Global Threat Report

14

Where do cyber threats come from?

- Hostile nation-states
- Terrorist groups
- Natural disasters
- Organized crime
- Hacktivists
- Disgruntled insiders
- Hackers
- Accidental actions of authorized insiders

Source: UpGuard Critical Cybersecurity Threats and KPIs for Every Business

15

Top 17 Common Cyber Threats

- Malware
- Spyware
- Phishing attacks
- DDoS attacks
- Ransomware
- Zero-day exploits
- Advanced persistent threats
- Trojans
- Wiper attacks
- Intellectual property theft
- Data manipulation and destruction
- Man-in-the-middle attacks

Source: UpGuard Critical Cybersecurity Threats and KPIs for Every Business

16

Top 17 Common Cyber Threats, continued

- Drive-by downloads
- Malvertising
- Rogue software



Source: UpGuard Critical Cybersecurity Threats and KPIs for Every Business

17



18



19



20

Top 12 Types of Social Engineering

- Phishing
- Spear phishing
- Vishing
- Smishing
- Pretexting
- Baiting

- Quid Pro Quo
- Tailgating/Piggybacking
- Dumpster Diving
- Watering Hold Attack
- Business Email Compromise
- Honeytrap

21

Phishing – How to Detect

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



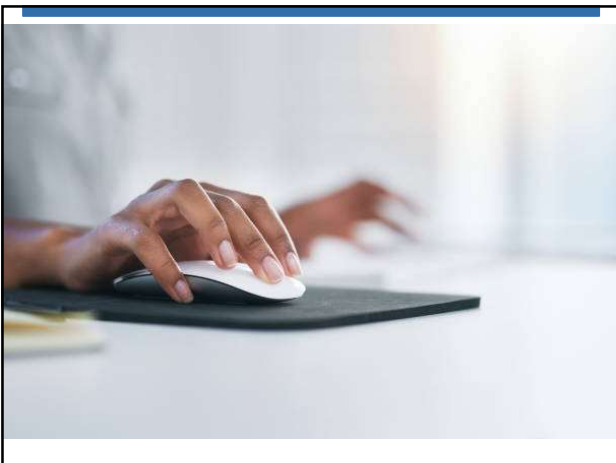
22

Phishing – How to Detect

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



23



24

Vishing – How to Detect

- Proper verification procedures
 - Out-of-wallet questions
- Out of the ordinary request
- Never just rely on voice



25

Protection and Prevention

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



26

Protection and Prevention

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



27




Baseline Cyber Practices



28

Security Concerns


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



29

New Third-Party Vendor Relationships

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



30

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



31

Existing Vendor Relationships

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



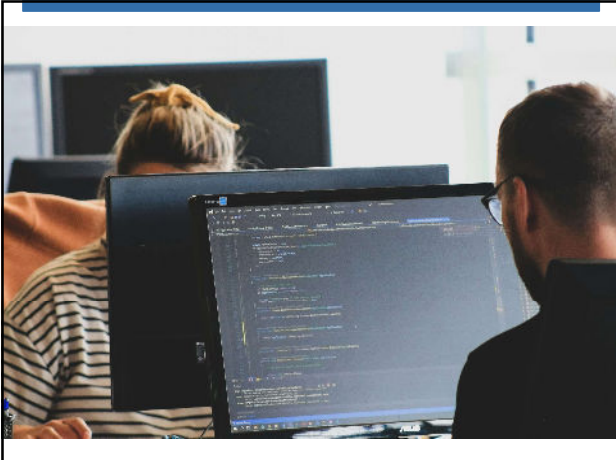
32

Organizational Responsibilities

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



33



34

End-User Assistance

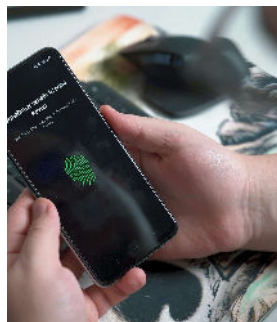
If you see something, say something!



35

User Provisioning and Access

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



36

Password Security

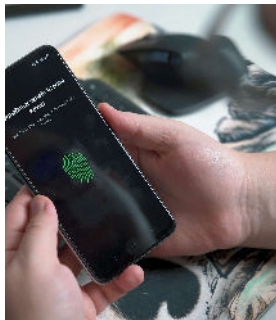
- Numbers, characters, symbols
- Avoid common words
- Change often and when compromised
- Length – 12, 14
 - Standards should be documented in your policy



37

Password Security

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



38

Multi-Factor Authentication

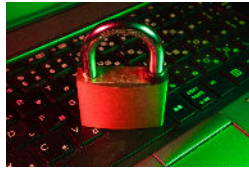
- Critical for all cloud applications
 - Remote access, email, AWS/Azure
- Mobile devices, email message, tokens
- Consider IP address, time, and day restrictions



39

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



40

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



41

Malware and Patch Management



42

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



43

Web Surfing

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



44

Social Networking



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

45



46

Data Storage



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

47

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



48



49

Remote Access Tools

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



50

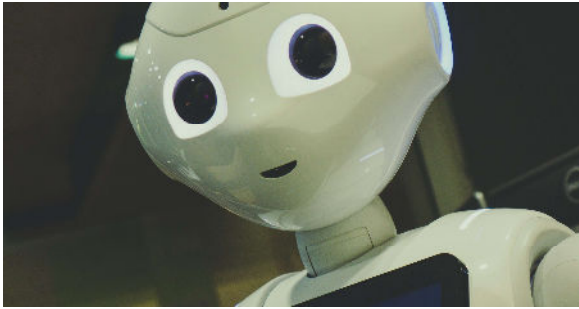
Shadow IT



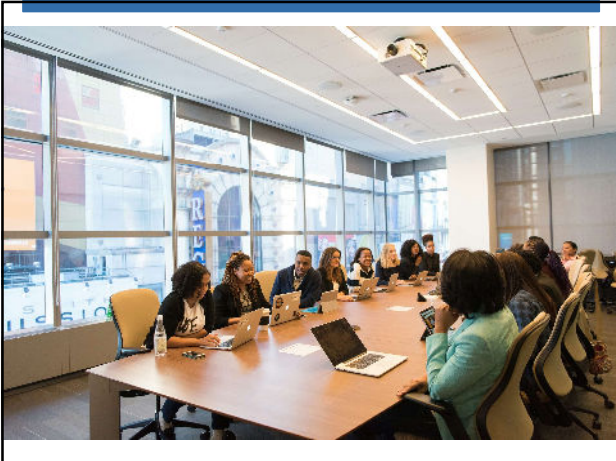
- Apps or devices that are used without IT's knowledge
 - Personal or mobile devices
- Rogue cloud services
 - Personal email, document scanning, cloud storage
- Improper authorization

51

Evolving Technologies

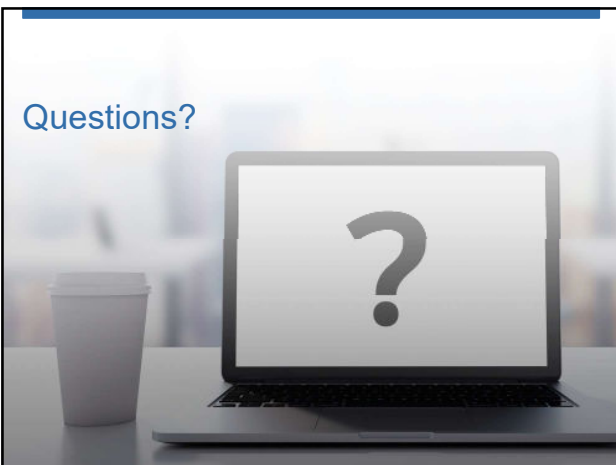


52



53


Questions?





54

Thank you.

Katie Herbert, Senior Manager
CapinTech

 kherbert@capincrouse.com

 505.50.CAPIN ext. 2007



© Copyright CapinCrouse 2025
