Corporate Customer Training
Cybersecurity & Account Takeover

Katie Kane, Senior Manager
4.12.23

CAPINTECH

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

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
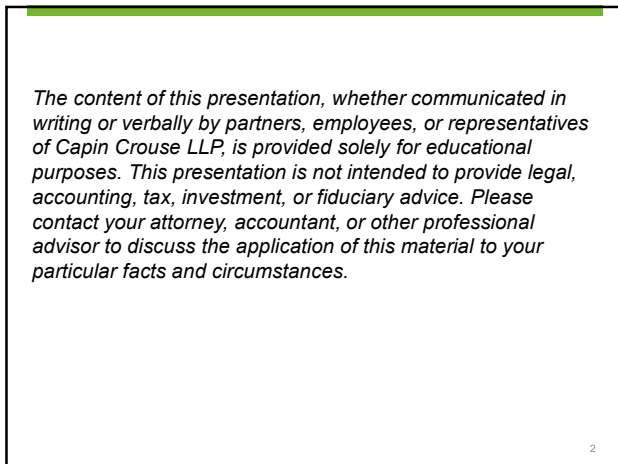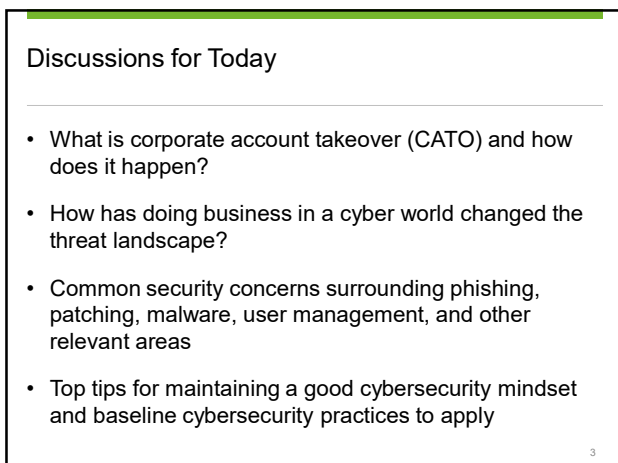
3

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
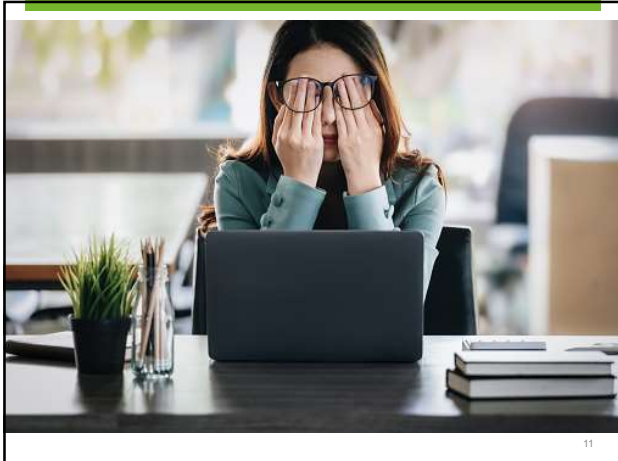 - Sensitive information obtained
- Credential stuffing

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

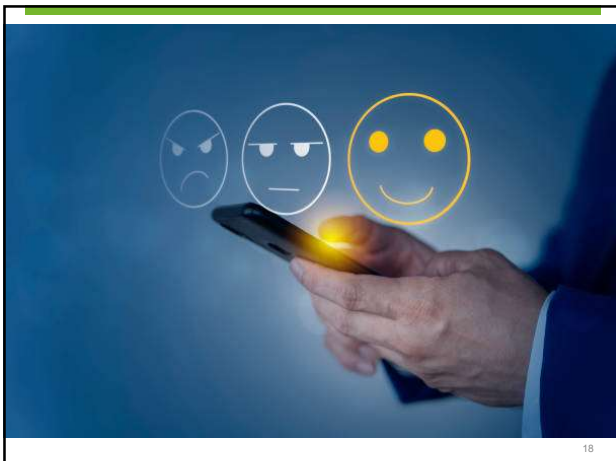- Result of a developer falling victim to a phishing attack

16

16

17
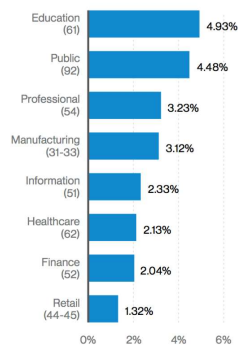
17

18

18

19

Phishing

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

20

Phishing Failure by Industry

Industry	Percentage
Education (61)	4.93%
Public (92)	4.48%
Professional (54)	3.23%
Manufacturing (31-33)	3.12%
Information (51)	2.33%
Healthcare (62)	2.13%
Finance (52)	2.04%
Retail (44-45)	1.32%

© 2023 PhishingBox, LLC

21

Examples

EXTERNAL

Morning ▮▮▮▮

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
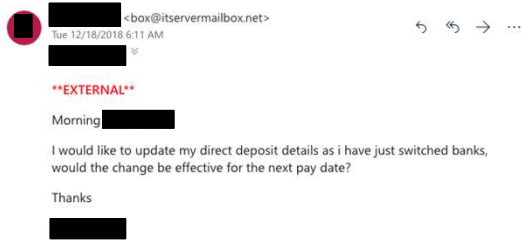
22

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

Examples

Microsoft account unusual sign-in activity

Microsoft Team <outlook@microsoft.com>
Today 4:56 PM

EXTERNAL
Email account
Unusual sign-in activity

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

Sign-in details:
Country/region: Krasnodarskiy Kray, Russia
IP Adddress: 31.181.250.117

If this was you, then you can safely ignore this email.
If you are not sure this was you, a malicous user might have your password. It is strongly advised that you change your password immediately.
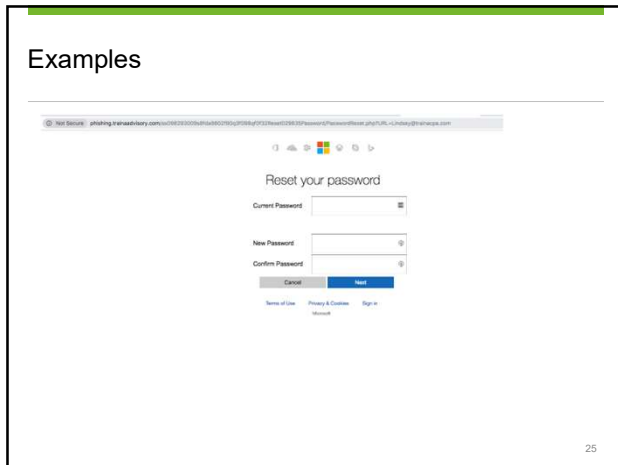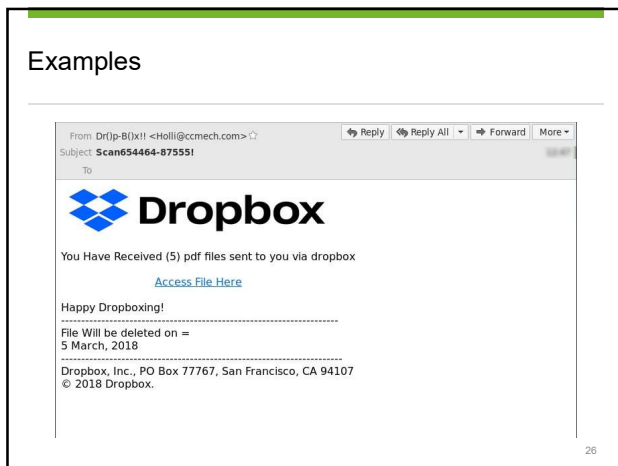
Reset Password

Thanks,
Mail support team

24

Examples

25

Examples

26

Phishing – How to Detect

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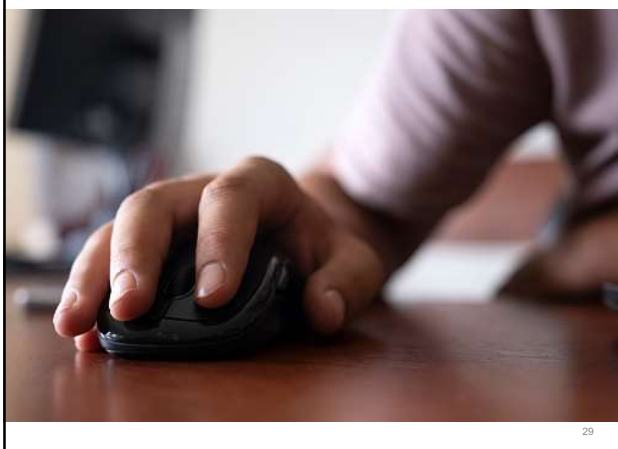 - Visit website manually

27

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

4/12/2023

Protection and Prevention

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

31

Baseline Cyber Practices

CAPINTECH

32

Security Concerns

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

33

11

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
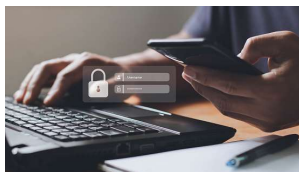
39

39

Password Security

- Numbers, characters, symbols

- Avoid common words

- Change often and when compromised

- Length – 12, 14, ???

40

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

41

Password Security

- Unique and private passwords

  - Password manager?

- Business ≠ personal

- Account lockout and inactivity threshold

- Biometrics

- Layered security
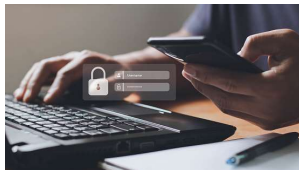
42

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
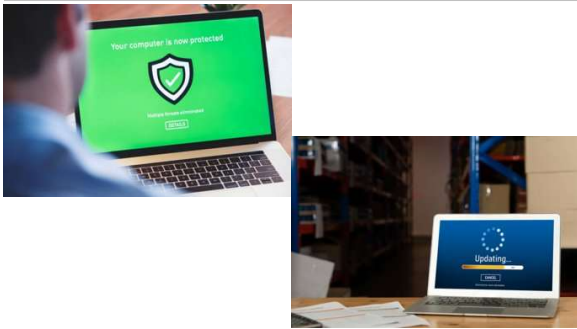
46

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

Web Surfing

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

48

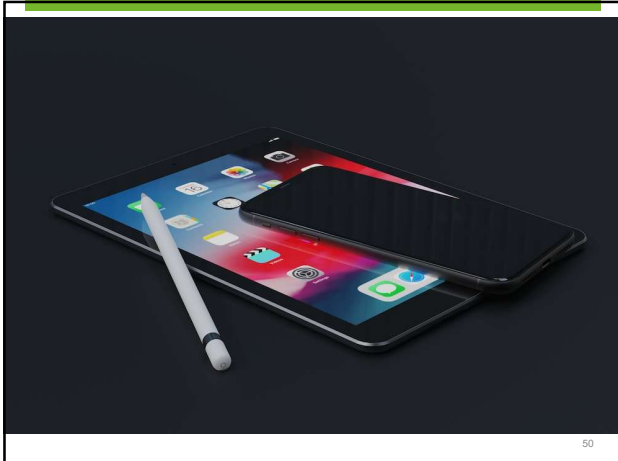## Social Networking

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

49

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

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
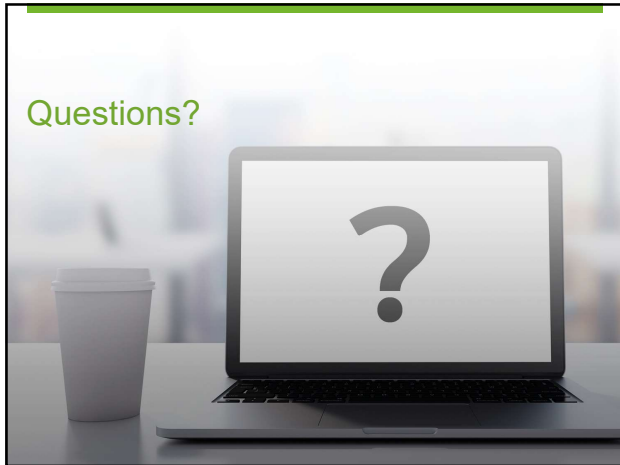- Appropriate authorization procedures

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

CAPINTECH

59