



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, 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.





Colonial Pipeline Company **May 2021**

- Result of a single compromised VPN password that granted access on April 29, 2021
 - Account was enabled but not active
- Password since discovered inside a batch of leaked passwords on the dark web
 - Colonial employee may have used the same password on another account that was previously hacked

Microsoft Power Apps **August 2021**

- Approximately 38 million records across 47+ organizations
- Various types of records exposed
 - Employee records; COVID testing, tracing, and vaccinations; names, dates of birth, Social Security numbers, addresses, and demographic details
- Misconfiguration was by third party, not Microsoft directly

Neiman Marcus

September 2021

- Result of a May 2020 data breach
- Approximately 3.1 million online customer accounts compromised, exposing personal data
 - Payment card data, including expiration dates and other personal information
 - Usernames, passwords, security questions, and answers for online accounts

Robinhood

November 2021

- A social engineering attack used to gain access to internal systems
- Accessed a list that contained email addresses of 5 million users, full names of 2 million users, and personal information of approximately 310 users
- Approximately 10 customers may have had a large amount of information compromised

Apache Log4j

December 2021

- What is Log4j?
- Many don't know how they were affected
- Extensive efforts to pinpoint vulnerable devices
- Thousands of attempts to exploit the vulnerability

Apache Log4j December 2021

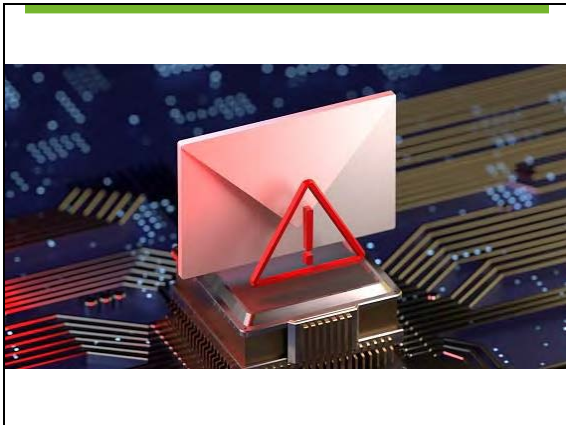
- Organizations "have a duty" to take "reasonable steps" to mitigate known software vulnerabilities
- FTC threatening action against those failing to mitigate
- Incident response component
 - You patched and resolved the issue.
 - But were you already affected?

Crypto.com January 2022

- Took advantage of a vulnerability and hacked the exchange
- Over \$34 million in cryptocurrency stolen from the wallets of 483 users
- Multi-factor authentication controls were bypassed
- All withdrawals were halted for approximately 14 hours while investigation took place








Phishing

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

A small illustration of a red diamond-shaped icon hanging from a laptop screen, symbolizing a phishing attempt or a security warning.

Phishing Failure

- 11% failure rate
 - Attachments – 20%
 - Data entry/credential – 4%
 - Link – 12%



Examples



Examples

From: Susan Fry [\[mailto:sfry@yourcompany.com\]](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 baib@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

Examples

Microsoft account unusual sign-in activity

Microsoft Team - csulbook@microsoft.com

SECURITY

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: Kazakhstan/Almaty, 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

Examples

Reset your password

Current Password

New Password

Confirm Password

Examples

Dropbox

You Have Received (5) pdf files sent to you via dropbox

[Access File Here](#)

Happy Dropboxing!

File Will be deleted on = 5 March, 2018

Dropbox, Inc., PO Box 77767, San Francisco, CA 94107
© 2018 Dropbox.

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



Phishing – How to Detect

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







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



Account Takeover

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



Account Takeover

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



Account Takeover

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



Account Takeover


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






Protection and Prevention

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



Protection and Prevention


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





Security Concerns

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



New Third-Party Vendor Relationships

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



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



Existing Vendor Relationships

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



Organizational Responsibilities

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





User Provisioning and Access

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



Password Security

- Numbers, characters, symbols
- Avoid common words
- Change often and when compromised
- Length – 8...12...??




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	Instantly	Instantly	Instantly
8	Instantly	Instantly	2 secs	7 secs	31 secs
9	Instantly	Instantly	2 mins	7 mins	39 mins
10	Instantly	10 secs	1 hour	7 hours	2 days
11	Instantly	4 mins	3 days	3 weeks	5 months
12	Instantly	2 hours	5 months	3 years	34 years
13	2 secs	2 days	34 years	300 years	3k years
14	19 secs	2 months	1k years	12k years	102k years
15	3 mins	4 years	54k years	750k years	10m years
16	32 mins	100 years	3m years	48m years	1.8e years
17	5 hours	3k years	1.75m years	301m years	92bn years
18	2 days	69k years	90m years	1.75bn years	77m years
19	3 weeks	2m years	46.7bn years	117n years	438m years

[Learn about our methodology at hivesystems.io/password](https://hivesystems.io/password)


Password Security

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



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



Email

- Easily spoofed or hacked
- Not all services are encrypted
- Confidential email **MUST** be secured
 - Sending and receiving
- If not needed, limit or restrict web mail

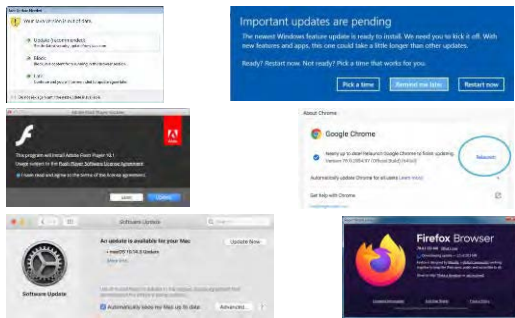


Wi-Fi Networks

- 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



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



Web Surfing

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



Social Networking

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






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



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





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?



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





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

Questions?
