

Welcome to this NAST Member Benefit

A promotional banner for a NASTcast event. The background features a laptop keyboard on the left and a wooden surface. The text is arranged in a clean, modern layout. The event title is in large, bold letters, followed by the date and time in a smaller font. A call to action button is prominent. The NASTcast logo is on the left, and the NAST logo is at the bottom right.

**Security Through Simulation:
How to Respond to
a Social Media Hack**

Wednesday, December 9
3pm ET / 2pm CT / 1pm MT / 12pm PT

NAST members are invited to
a real-time table top exercise.

REGISTER NOW

NAST
cast

 NATIONAL ASSOCIATION OF
STATE TREASURERS

Housekeeping

- Recorded to view on demand
- Interactive session
 - Discussion
 - What state are you in? (enter into chat box)
 - Polling
 - Holiday preparations?

Security through Simulation: How to Respond to a Social Media Hack

Adam Bulava | Executive Director, JPMorgan Chase | Global Head of Attack Simulation

Date: December 9, 2020

Disclaimer

This presentation was prepared exclusively for the benefit and use of one or more JPMorgan clients to whom it was directly addressed and delivered. The content is intended for informational purposes and is not intended to be used to evaluate any product or service provided by JPMorgan nor intended to be relied on for any related purpose. The statements made in this presentation are confidential and proprietary to JPMorgan and not intended to be legally binding.

The presentation is incomplete without reference to, and should be viewed solely in conjunction with, the oral briefing provided by JPMorgan. It may not be copied, published or used, in whole or in part, for any purpose other than as expressly authorized by JPMorgan. Neither JPMorgan nor any of its directors, officers, employees, or agents shall incur any responsibility or liability to any recipient(s) of this presentation or any other party with respect to its content.

© 2020 JPMorgan Chase Bank, N.A. All Rights Reserved.

Agenda

15 Mins

Threat Landscape Update

5 Mins

Tabletop Exercise Overview & Guidelines

10 Mins

Day 1 | Scenario Brief & Polling/Discussion

10 Mins

Day 2 | Scenario Brief & Polling/Discussion

10 Mins

Day 3 | Scenario Brief & Polling/Discussion

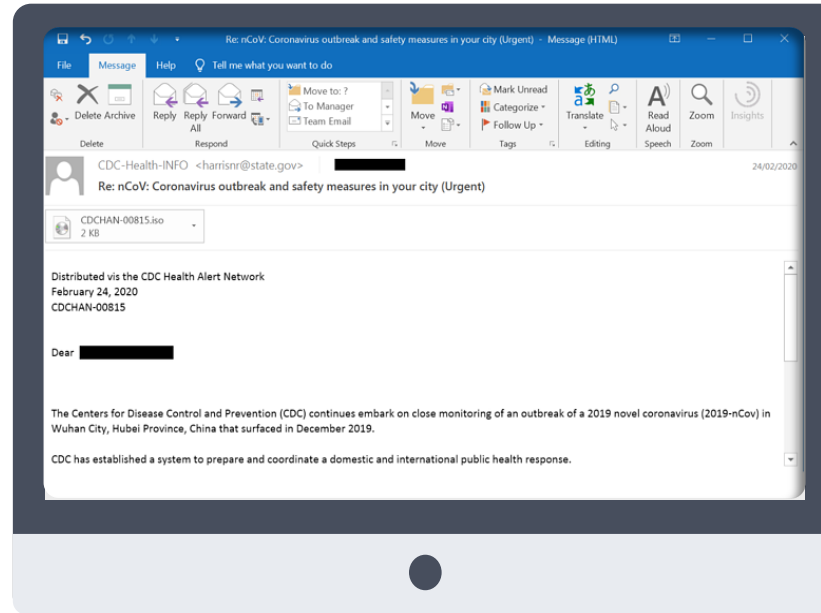
10 Mins

Hot Wash/Lessons Learned/Q&A

Threat Landscape Update

In uncertain times, bad actors will seek opportunities to take advantage of disruptions to normal business operations...

Cyber & fraud actors are leveraging the COVID-19 situation to target individuals and organizations through advanced social engineering (email, phone, text) and the use of fake websites



Example COVID-19 Phishing email



Example fake website that actually downloads a banking Trojan virus

This activity adds to an already growing threat landscape that has seen increased attacks...



81% of companies were targets of payment fraud in 2019 – up from a record high 78% in 2017¹

↑ 600%

Increase in cyber crime due to the ongoing COVID-19 pandemic⁴



67% of all payments fraud is first discovered by the treasury services or accounts payable staff at an organization¹

↑ 69%

Increase in the number of “Dark Web” posts selling company network access in Q1 2020 compared to Q4 2019²



Indirect attacks against weak links in the supply chain now account for 40% of security breaches³

Note: ¹ 2020 AFP Payments Fraud and Control Survey Report; ² Positive Technologies – 2020 “Access for Sale” report; ³ Accenture 2020 Annual State of Cyber Resilience report; ⁴ Purple Security 2020 *Cyber Security Statistics*

Key Cyber & Fraud Risks



Business Email Compromise (BEC)

An electronic scam to obtain confidential, personal or financial information through email

BEC scams accounted for **half of all cyber crime losses**, ~\$1.77bn (USD) in 2019¹

Risk Areas

- Email Spoofing/Masking
- Client Email Compromise
- Vendor Email Compromise/Supply Chain
- Lookalike Domain

Best Practice Considerations

- Consider available email security solutions to defend against lookalike domains
- Enable controls to mark outside emails as external and ensure the process for reporting suspicious emails is clear and simple
- Train employees on suspicious email trends



Malware

Malicious software, to include viruses, ransomware, and spyware, designed to cause damage to data and systems, or gain unauthorized

Global ransomware costs are **estimated to reach \$20 billion (USD)** by 2021²

Risk Areas

- Malware modifying legitimate payment instructions to a bad beneficiary
- Encryption of critical files & servers for extortion

Best Practice Considerations

- Block access to suspicious websites
- Scan email attachments upon message receipt
- Ensure all software, antivirus and firmware is patched and updated
- Regularly backup and secure data



Social Engineering

Psychological manipulation of people into performing actions or divulging confidential information

62% of companies experienced **phishing & social engineering** attacks in 2019³

Risk Areas

- Call from someone pretending to be a vendor
- Client received SMS message from a spoofed phone number

Best Practice Considerations

- Train & test all staff regularly against the latest social engineering threats
- Limit the amount of information employees are permitted to disclose on social media
- Consider layered email controls and robust caller authentication processes

Recent Social Media Hacks

April 2013

A news company's social media accounts were hijacked and one fake Tweet resulted in \$136B lost stock market value in three minutes

December 2018

Hackers infiltrated Chile's ATM network after an employee at a Chilean financial firm downloaded malware during a spoofed virtual job interview

February 2020

A US television host was the victim of a BEC scam and sent nearly \$380K to hackers

July 2020

Hackers gained access to multiple high-profile US celebrity Twitter accounts and stole \$120k through a bitcoin scam

November 2016

Russian hackers purchased Facebook ads to infect the US 2016 election season and more than 120 million people viewed the content

April 2019

Mexican social media app developers leaked 146 gigabytes of Facebook user data, which contained over 540 million records

April 2020

Hackers used social media and capitalized on COVID-19 vulnerabilities to launch a viral streaming scam

November 2020

Malicious actors utilized fake Twitter accounts to pose as a news organization and prematurely declare election victories

To combat these risks, employees should be reminded of the following key practices:



Enable safe remote working

Remind employees of cybersecurity **best practices** when working remotely, to include:

- Securing home WiFi networks
- Only using company-approved communications tools
- Never sending work documents to personal email accounts
- Keeping personal device software up-to-date



Follow established procedures

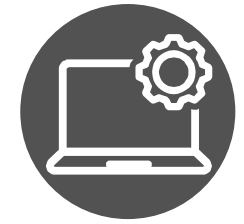
Ensure all staff are aware of **organizational procedures** for:

- Authenticating callers
- Reporting suspicious activity
- Approving changes to account details or transactions
- Escalating potential privacy breaches



Ensure knowledge of response plans

Fully **socialize plans and playbooks** for how to escalate potential incidents and ensure clear channels for staff to alert leadership of any emerging business disruptions



Test business continuity

Conduct **regular resiliency tests and exercises** to build increased preparedness among staff and ensure technology can effectively support contingency situations

Tabletop Exercise

Tabletop Exercise Overview

- This tabletop exercise consists of realistic scenarios based on current threats and historic examples of actual cyber crises – it is not based upon any intelligence indicating a specific threat to your organization
- This type of incident has resulted in legal & regulatory action, media attention, and financial loss
- The exercise is designed to emphasize and examine roles & responsibilities as well as key decisions that organizations must make during a cyber event



Key Objectives

- Highlight and develop the skills to lead and work through a cyber incident
- Understand all relevant stakeholders required to respond to a significant breach
- Learn how to conduct an exercise that could be used to test your agency's breach preparedness
- Take away ideas for how your company could improve its incident response plan

Exercise Conduct



- 45-minute, virtual, discussion-based exercise



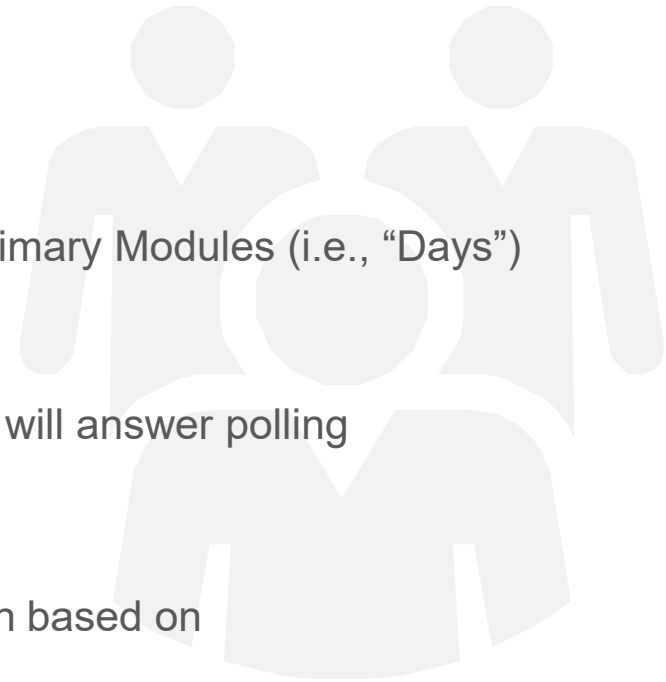
- The scenario will be presented across three primary Modules (i.e., “Days”)



- At the conclusion of each Module, participants will answer polling questions based upon the evolving scenario



- Facilitator will then moderate a brief discussion based on polling results and participant insights



Exercise Conduct (cont.)



- You work for the Treasurer's Office in the fictional state of Winnemac, responsible for a wide range of duties including receiving and depositing state funds, managing investments, and tracking budget surpluses/deficits. Your State Treasurer is running for re-election in November and it's looking like a tight race



- This exercise will take place over five days (notionally)



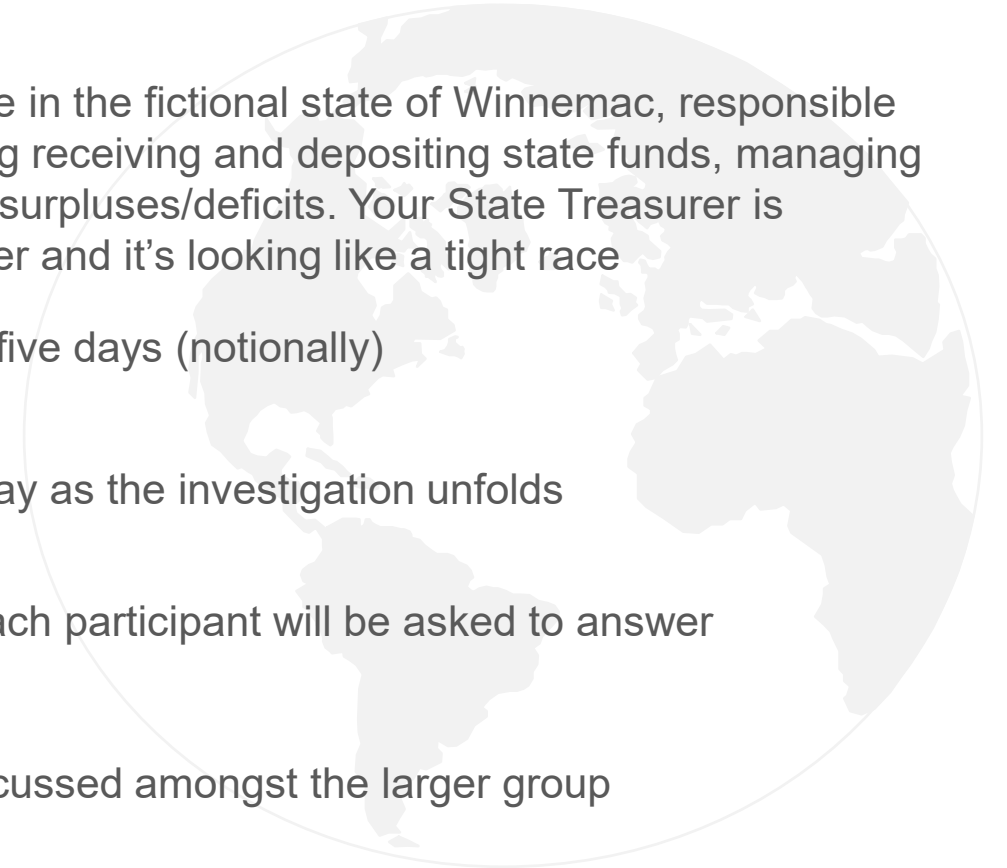
- New facts will be provided each day as the investigation unfolds



- At the end of each module/day, each participant will be asked to answer polling questions



- Polling responses will then be discussed amongst the larger group





Day One

October 2020

State of the World – Monday, October 5

- Based on recent credible threat intelligence, the FBI, DHS United States Computer Emergency Readiness Team (US-CERT), and the Multi-State Information Sharing and Analysis Center (MS-ISAC) release the following *Cyber Alert* to all State and Local Government Departments & Agencies:

9:00AM

Cyber Alert: Email Phishing Campaigns Targeting MS-ISAC Members

Date: Monday, October 5, 2020

On September 2, 2020, DHS US-CERT, FBI, and MS-ISAC release a joint indicator bulletin (JIB) detailing an evolved form of malware, known as Kooberface, that is being used in spear phishing campaigns targeting State, Local, Territorial, and Tribal (SLTT) officials during the 2020 election season. The malware is polymorphic in nature and circumvents normal signature-based detection mechanisms.

The campaigns vary from target to target, but generally utilize social media platforms and urge users to click on malicious links or download malicious files. The malware, when executed, attempts to gain control of the user's social media account and can record keystrokes, take screenshots, and access locally installed applications.

Recommendations: The JIB recommends the following general best practices to limit the effect of spear phishing and social media scams to your organization:

1. Remind users to not click suspicious links or download suspicious applications, as they may contain malware
2. Implement a social media policy and establish regular social media trainings to enforce the policy

Monday, October 5, 2020

1:00PM

- Bradley Shaw is an intern in the Winnemac State Treasury Department who supports the monitoring and creation of content for state elected officials' social media accounts
- Chloe Smith, a recruiter at Belle Staffing Solutions, contacts Bradley through *Connect-In* and requests his résumé

From: Recruiting <recruiter@connect-in.com> Sent: Monday 10/5/2020 1:00 PM
To: Bradley Shaw <shaw007@gmail.com>
Cc:
Subject: Connect-In: Direct Message from a recruiter!

Connect-In A recruiter sent you a direct message!

Hi Bradley,

I just looked at your profile and am very impressed with your government experience. You would be a great fit for one of our government agency Executive Staff Assistant positions. Please send me your resume at chloe.smith@bssolutions.net.

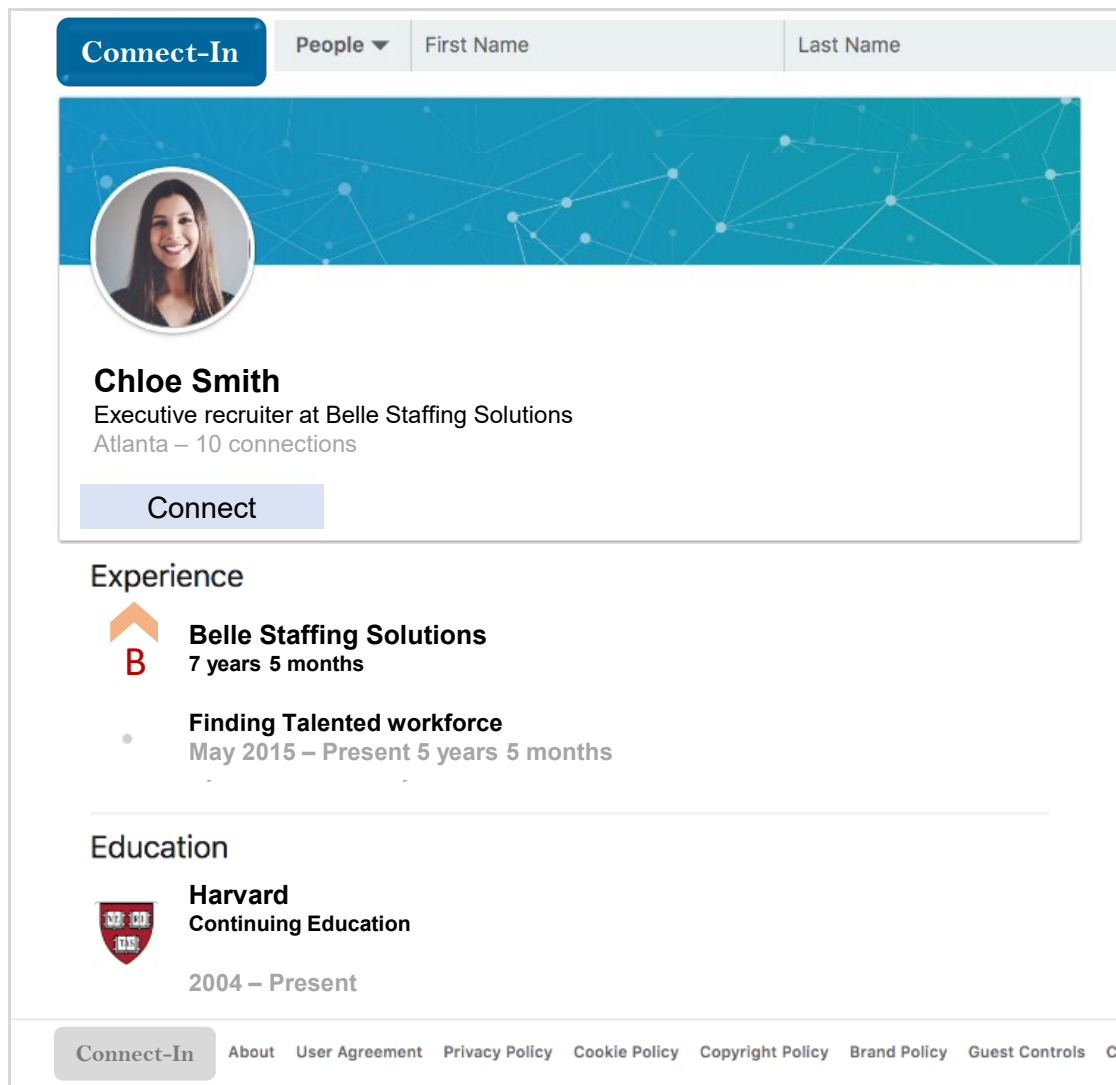
Chloe Smith
Belle Staffing Solutions

You are receiving Messages from Connect-In Recruiters.
This email was intended for Bradley Shaw (Intern at Winnemac State Government). [Learn why we included this.](#)

Monday, October 5, 2020

1:15PM

- Before he sends his résumé, Bradley looks up Chloe on *Connect-In* and reviews her profile



The screenshot shows a user profile on the Connect-In platform. At the top, there is a navigation bar with 'Connect-In' on the left and 'People', 'First Name', and 'Last Name' on the right. The profile header features a blue background with a network diagram and a circular profile picture of a woman. Below the picture, the name 'Chloe Smith' is displayed, followed by her title 'Executive recruiter at Belle Staffing Solutions' and location 'Atlanta - 10 connections'. A 'Connect' button is visible below the profile information. The 'Experience' section lists 'Belle Staffing Solutions' with a logo and '7 years 5 months', and 'Finding Talented workforce' with 'May 2015 - Present 5 years 5 months'. The 'Education' section lists 'Harvard Continuing Education' with the Harvard logo and '2004 - Present'. At the bottom, there is a footer with 'Connect-In' and various policy links: 'About', 'User Agreement', 'Privacy Policy', 'Cookie Policy', 'Copyright Policy', 'Brand Policy', 'Guest Controls', and 'Cor'.

How to Spot a Fake Social Media Profile

Tips to Spot a Fake Profile

1. Incomplete profile
2. Fake photo/name
3. Generic job title
4. Limited connections
5. Little recent activity
6. Suspicious work history

Actions to Take

1. Research people further on the internet
2. Report fake profiles to the social media company
3. Don't accept the "friend request"

The screenshot shows a LinkedIn profile for Chloe Smith. Red callout boxes with numbers 1 through 6 point to specific areas of the profile:

- 1. The profile header area, including the 'Connect-In' button and search filters.
- 2. The profile picture of a woman.
- 3. The name 'Chloe Smith'.
- 4. The job title 'Executive recruiter at Belle Staffing Solutions'.
- 5. The 'Connect' button.
- 6. The 'Experience' section, specifically the entry for 'Belle Staffing Solutions'.

The profile details shown are:

- Name:** Chloe Smith
- Job Title:** Executive recruiter at Belle Staffing Solutions
- Location:** Atlanta – 10 connections
- Experience:**
 - Belle Staffing Solutions** (7 years 5 months)
 - Finding Talented workforce** (May 2015 – Present 5 years 5 months)
- Education:**
 - Harvard** Continuing Education (2004 – Present)

The footer of the page includes: Connect-In, About, User Agreement, Privacy Policy, Cookie Policy, Copyright Policy, Brand Policy, Guest Controls, Cor

Monday, October 5, 2020

3:00PM

- After receiving the résumé, Chloe follows up with Bradley on *Connect-In* and mentions that she was unable to reach him on his personal email. She asks that Bradley provide an alternate email and he gives his government email address
- Shortly after, Chloe sends Bradley a link at his work email to schedule an interview

From: Chloe Smith <lewfrtg87y@bssolutions.net> Sent: Monday 10/5/2020 3:00 PM
To: Bradley Shaw <bradleyt.shaw01@winnemacstate.gov>
Cc:
Subject: Belle Staffing Solutions Follow-up

Hi Bradley,

Thank you for sending me your resume. We are ready for the next step.

Please schedule interview through are [scheduling portal](#). You're access to this link will be available for 24 hours.

Chloe Smith
Belle Staffing Solutions

Monday, October 5, 2020

4:00PM

- Bradley clicks on the link from his work computer and attempts to schedule an interview, but he receives a *404 Error* message. Next, Bradley tries to email Chloe about the issue, but his email bounces back
- The malicious code embedded on the webpage detonates on Bradley's system and sends the passwords stored in memory, including those used for social media accounts, back to the hacker
- Thinking the email is suspicious, the intern reports it to the IT Department



IT can see suspicious traffic coming from Bradley's internal company machine communicating with an unknown, external Eastern European IP address. Further investigation is required to determine additional details

Discussion Question

From the perspective of your own organization....

1 | Do you receive regular threat intelligence/alerts – such as the example in this scenario?

- A Yes
- B No
- C I don't know

Enter your response and comments in the Question box.

Polling Questions

From the perspective of your own organization....

- 2 | If you were Bradley in this scenario and a recruiter contacted you in this manner, what immediate actions would you take? Select all that apply:
- A Research the recruiter
 - B Research the staffing agency
 - C Ask the recruiter for the URL to the Executive Staff Assistant job posting
 - D Send your résumé right away to the recruiter because you definitely need a full time job!

Discussion Question

From the perspective of your own organization....

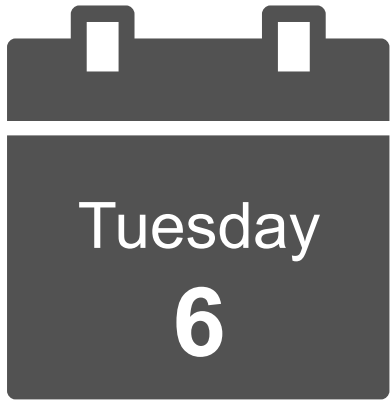
3 | Does your organization have a formal policy or process to guide employees on how to responsibly use social media?

- A Yes
- B No
- C I don't know

Discussion Question

From the perspective of your own organization....

- 4 | If you answered “yes” to the previous question, are all personnel, regardless of employment status, regularly trained on this social media policy/process at your office?
- A Yes
 - B No
 - C I don't know
 - D Does not apply/Selected “no” to the previous question



Day Two

October 2020

Tuesday, October 6, 2020

1:00PM

- Winnemac constituents call the Treasurer's Office inquiring about the content that was recently posted on the State Treasurer's official Twitter account and on a public, Winnemac Treasury Department Facebook group
- Furthermore, the Office's Social Media Manager notices that she is locked out of all social media accounts



Winnemac State Treasurer 
@WM_Treasurer

Help support my reelection! A generous benefactor will DOUBLE all bitcoin contributions made to my campaign over the next hour <http://stategov/y9vcr.goog.gl>.
#LimitedTime #Hurry

1:00 PM | Oct 6, 2020 · [Twitter for iPhone](#)

11 Retweets 16 Likes



 **Winnemac Treasury Department**
9 minutes ago · 

DOUBLE YOUR DONATION!!! As part of our state's relief efforts we have been authorized to donate unclaimed funds. We will match 100% all bitcoin donations to state relief efforts <http://stategov/y9vcr.goog.gl>

[Like](#) · [Comment](#) · [Share](#)

 5 people Jon Jacobs and 4 others like this.

 2 shares

Tuesday, October 6, 2020

2:00PM

- The Social Media Manager is reporting the team is still locked out of all social media accounts. The Office contacts Twitter & Facebook notifying them of the apparent account takeovers
- In the interim, a subsequent tweet is sent from the State Treasurer's Twitter account, polling Winnemacians on local foods
- More than 50 social media users begin complaining that the link directs them to what appears to be a Deepfake video where the State Treasurer makes derogatory comments about the voters' intellect



Tuesday, October 6, 2020

4:00PM

- While awaiting responses from Twitter and Facebook, the IT Department continues its investigation of the State Treasury systems
- A local media outlet reaches out to the Chief of Staff at the State Treasurer's Office claiming to have received details of a serious cyber attack from an anonymous source
- The reporter is asking about the incident and wants to know how the Office is responding. The news outlet also wants a comment about the Deepfake video that was shared on Twitter because they are planning to release a story shortly

Polling Questions

From the perspective of Winnemac....

- 1 | At this point, what are the top immediate actions you would take in response to the current situation? Select the top two actions:
 - A | Make a public statement and notify constituents
 - B | Respond directly to the reporter and provide additional information
 - C | Contact law enforcement to assist in the investigation
 - D | Notify the State Governor's Office of the unfolding situation
 - E | Contact your Cyber Insurance Provider to alert them of the incident and begin a claim
 - F | Wait to take any further action until you know more information about what happened

Polling Questions

From the perspective of your own organization....

2 | What additional steps would you take to specifically secure your own Office's official social media accounts to avoid this situation from occurring? Select the top two steps:

- A Audit what applications/tools might have access to your social media credentials
- B Develop strong passwords for your accounts
- C Limit access to your social media accounts based on a "need to know" policy
- D Continue to educate yourself and your staff regarding the Social Media Threats
- E Frequently update your devices to ensure you are using the most recent software

Discussion Question

From the perspective of your own organization....

4 | Does your organization have a formal playbook/plan that addresses how to respond to potential cyber or fraud incidents?

- A Yes
- B No
- C I don't know

Discussion Question

From the perspective of your own organization....

5 | If you answered “yes” to the previous question, do you provide annual employee training based on that playbook/plan?

- A Yes
- B No
- C I don't know
- D Does not apply/Selected “no” to the previous question



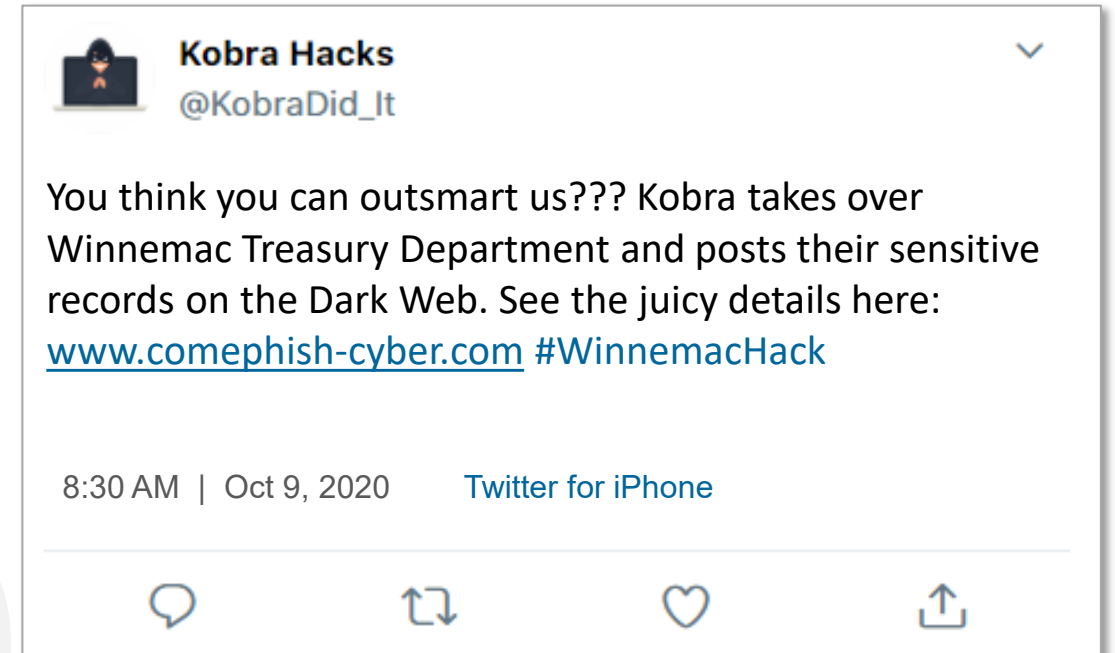
Day Three

October 2020

Friday, October 9, 2020

8:30AM

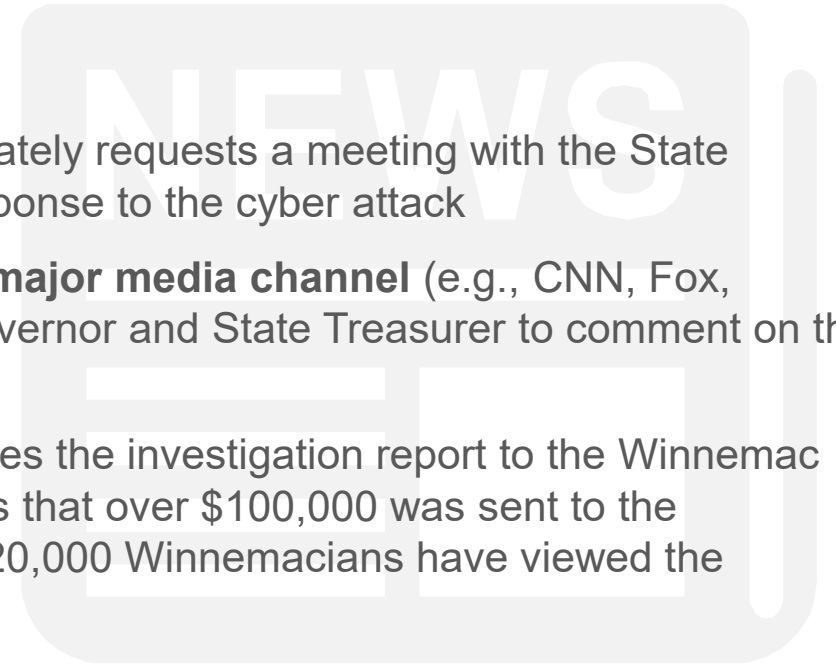
- A few days later, an anti-western cyber criminal group called **Kobra**, takes responsibility for the **cyber attack** and claims that sensitive records from the State of Winnemac have been posted to the “Dark Web”
- Kobra broadcasts their hack on Twitter



Friday, October 9, 2020

9:15AM

- The Governor of Winnemac immediately requests a meeting with the State Treasurer to discuss the State's response to the cyber attack
- News of the hack is **now on every major media channel** (e.g., CNN, Fox, MSNBC). Outlets are asking the Governor and State Treasurer to comment on the situation
- Additionally, law enforcement provides the investigation report to the Winnemac Treasurer's Office. The report shows that over \$100,000 was sent to the adversary's bitcoin wallet and over 20,000 Winnemacians have viewed the Deepfake video



Friday, October 9, 2020

10:30AM

- Constituents are complaining to the State Treasurer's Office and on social media that the Office has not responded in a timely matter to their concerns and has not taken appropriate steps to protect their personal data
- Twitter finally replies back to the Office's complaint and says, "Thank you. We will look further into this issue and get back to you."
- During the morning crisis management call, the Office employees discuss the incident and the extent of the attack. Morale is low and staff seem demotivated and fearful due to the public outcry against the Treasurer's Office. Additionally, the Communications Team begins developing further talking points after consulting with the IT Department

Discussion Questions

From the perspective of Winnemac....

- 1 | Based off of the law enforcement analysis, would you return the \$100K to constituents? Y N
- 2 | Now that news of the incident is on the major networks, would you make a more detailed statement about the incident and accept responsibility? Y N
- 3 | Do you think this situation will have a negative impact on the November election? Y N

Exercise Wrap Up



Final Forensics Report

- The forensics report is finalized and the source of the attack was identified as a phishing email **from someone posing as a Job Recruiter** that led to unauthorized system access via valid user credentials. After the intern clicked the link from the Recruiter, the adversary exfiltrated (i.e., stole) data from Winnemac's servers and spread ransomware throughout the network
- After analyzing its systems, the IT Department saw suspicious traffic coming from an internal company machine communicating with an unknown, external Eastern European IP address
- Additionally, forensics determine that Winnemac's network was **infected by a modified strain of the Kooberface virus**

Exercise Wrap Up (cont.)

Financial Loss & Reputational Damage



- The State of Winnemac is sued in a number of class action lawsuits alleging it **did not protect data and failed to notify its constituents in a timely manner**
- The State also reimbursed the \$100,000 back to its impacted citizens, which negatively impacted the following year's budget projections
- The State Treasurer barely managed to be re-elected despite significant reputational fallout from the erroneous tweets which required a steadfast public relations effort to convince constituents the Deepfake video was not genuine

Social Media Best Practices

DOs	DON'Ts
✓ Create strong, unique passwords	✗ Overshare personal & business information
✓ Enable Multi-Factor Authentication (MFA)	✗ Excessive hashtags and tagging
✓ Review current privacy settings	✗ Share false information
✓ Review application permissions	✗ Misuse location tags
✓ Keep a pulse on trends	✗ Spam followers & post irrelevant news
✓ Interact with your audience	✗ Share your travel itinerary

“Top 10 List” of Effective Programs/Practices



1. Conduct an Independent Assessment



2. Engage government and law enforcement



3. Join an industry forum



4. Simulate an internal attack



5. Deploy mandatory employee training and testing



6. Know your third party vendors



7. Conduct Exercises & Drills



8. Understand how money leaves your organization



9. Implement controls for maximum effect



10. Plan for Payment Contingencies

Helpful Links

Social Engineering Attacks & Techniques in recent times

- [The State of Ransomware in the US: Report and Statistics 2019](#)
- [How Hackers Profile Victims For Social Media Engineering Attacks](#)
- [7 Key Points From Verizon's 2020 Data Breach Investigations Report \(DBIR\)](#)
- [How To Protect Your Employees From Phishing Attacks](#)

Social Media & Fraud

- [What to Do When Your Social Media Account Gets Hacked](#)
- [Twitter Hack Exposes Broader Threat to Democracy and Society](#)

Best Practices in Cybersecurity

- [Cybersecurity: Protecting Local Government Digital Resources](#)
- [Cybersecurity Resources for Local Governments](#)
- [Cybersecurity Must Be Embedded in Every Aspect of Government Technology](#)

Exit Poll

Q&A