AN ALFN WEBINAR PRESENTATION

ALFN

Representing, defending and educating America's mortgage servicing industry.

AMERICAN LEGAL & FINANCIAL NETWORK

ARCHIVES AVAILABLE ON ALFN.ORG

ALFN ANSWERS WEBINAR

Cybersecurity and Financial Privacy

Thursday, August 13, 2020
1:00-2:15 PM Central Time

Sponsored By

Associate Member Partner

ā360inc™
Technology | Outsourcing | Consulting

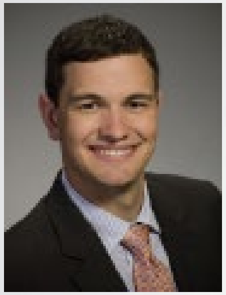
Attorney-Trustee Member Partner

PADGETT
LAW GROUP

Contact information for today's presenters

PRACTITIONERS. EXPERTS. ALFN WEBINAR PRESENTERS.

MODERATOR

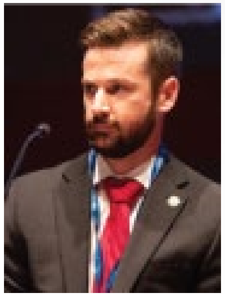


Matt White, Esq.
CIPP/US, CIPP/E, CIPM
Shareholder
Baker Donelson
mwhite@bakerdonelson.com

SPEAKER

Alex Koskey, Esq.
CIPP/US, CIPP/E
Associate
Baker Donelson
akoskey@bakerdonelson.com

SPEAKER



James McDowell
Chief of Cyber Operations
Alabama Securities Commission
james.mcdowell@asc.alabama.gov

SPEAKER

Jamie Stewart
Western Region Operations Manager
Janeway Law Firm
jamiestewart@janewaylaw.com

Agenda

- Introductions
- Cybersecurity 101
- New & Evolving Cyber Threats
- Table-Top Exercise

Payment will be raised on

5/15/2017 16:32:52

Time Left

02:23:59:49

Your files will be lost on

5/19/2017 16:32:52

Time Left

06:23:59:49

What Happened to My Computer?

Your important files are encrypted.

Many of your documents, photos, videos, databases and other files are no longer accessible because they have been encrypted. Maybe you are busy looking for a way to recover your files, but do not waste your time. Nobody can recover your files without our decryption service.

Can I Recover My Files?

Sure. We guarantee that you can recover all your files safely and easily. But you have not so enough time.

You can decrypt some of your files for free. Try now by clicking <Decrypt>.

But if you want to decrypt all your files, you need to pay.

You only have 3 days to submit the payment. After that the price will be doubled.

Also, if you don't pay in 7 days, you won't be able to recover your files forever.

We will have free events for users who are so poor that they couldn't pay in 6 months.

How Do I Pay?

Payment is accepted in Bitcoin only. For more information, click <About bitcoin>.

Please check the current price of Bitcoin and buy some bitcoins. For more information, click <How to buy bitcoins>.

And send the correct amount to the address specified in this window.

After your payment, click <Check Payment>. Best time to check: 9:00am - 11:00am

Send $300 worth of bitcoin to this address:

12t9YDPgwueZ9NyMgw519p7AA8isjr6SMw

What is hacking?

Hacking is creatively breaking things…

Top Cybersecurity Threats

Social Engineering/Phishing/Spear Phishing

Web security risks (OWASP’s Top Ten)

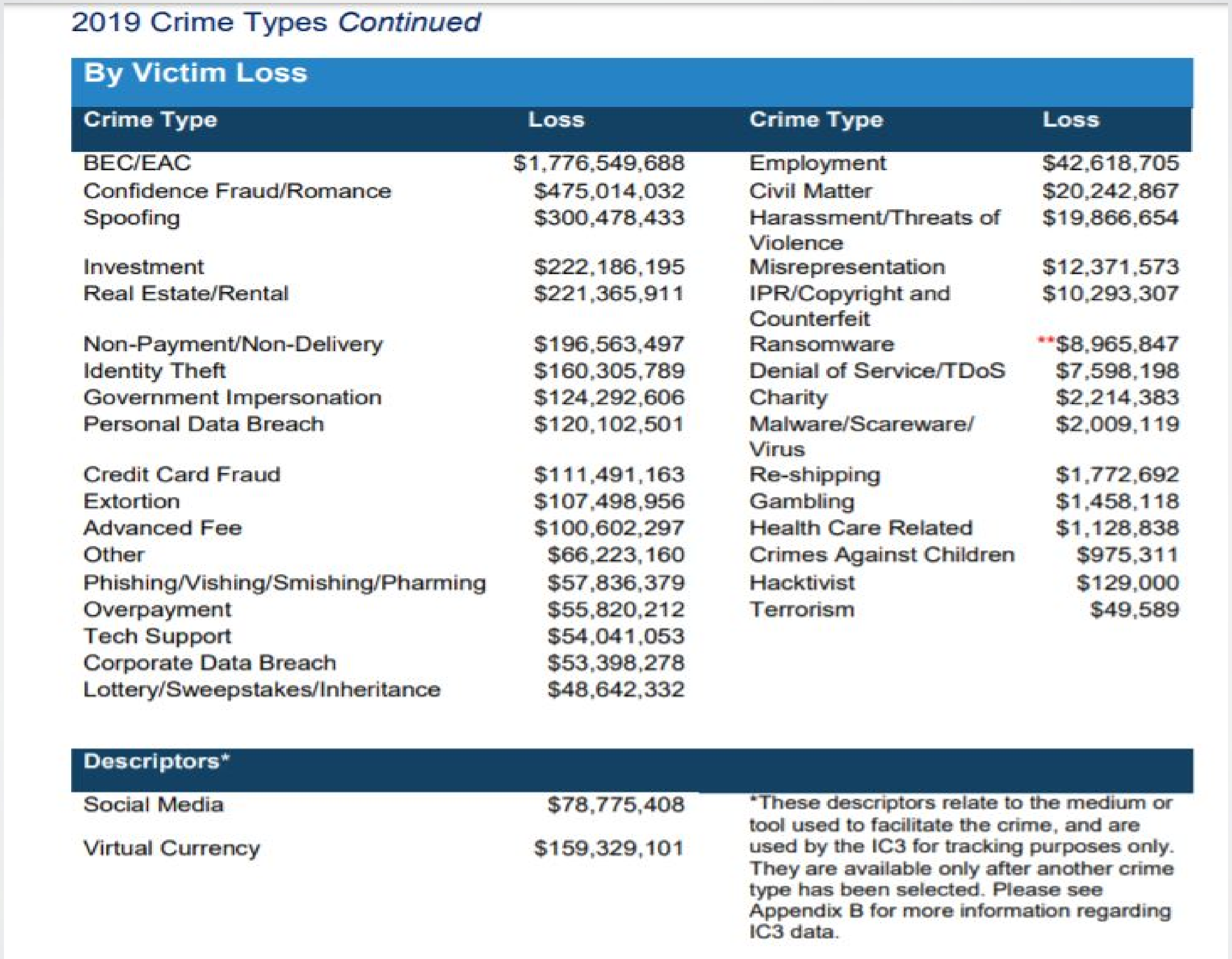
Bad passwords and/or reusing them

Cybersecurity 101

Why it matters?

$3.5 Billion in USD
(Losses)
2019 IC3 Report

Cybersecurity 101



2019 Crime Types *Continued*

By Victim Loss

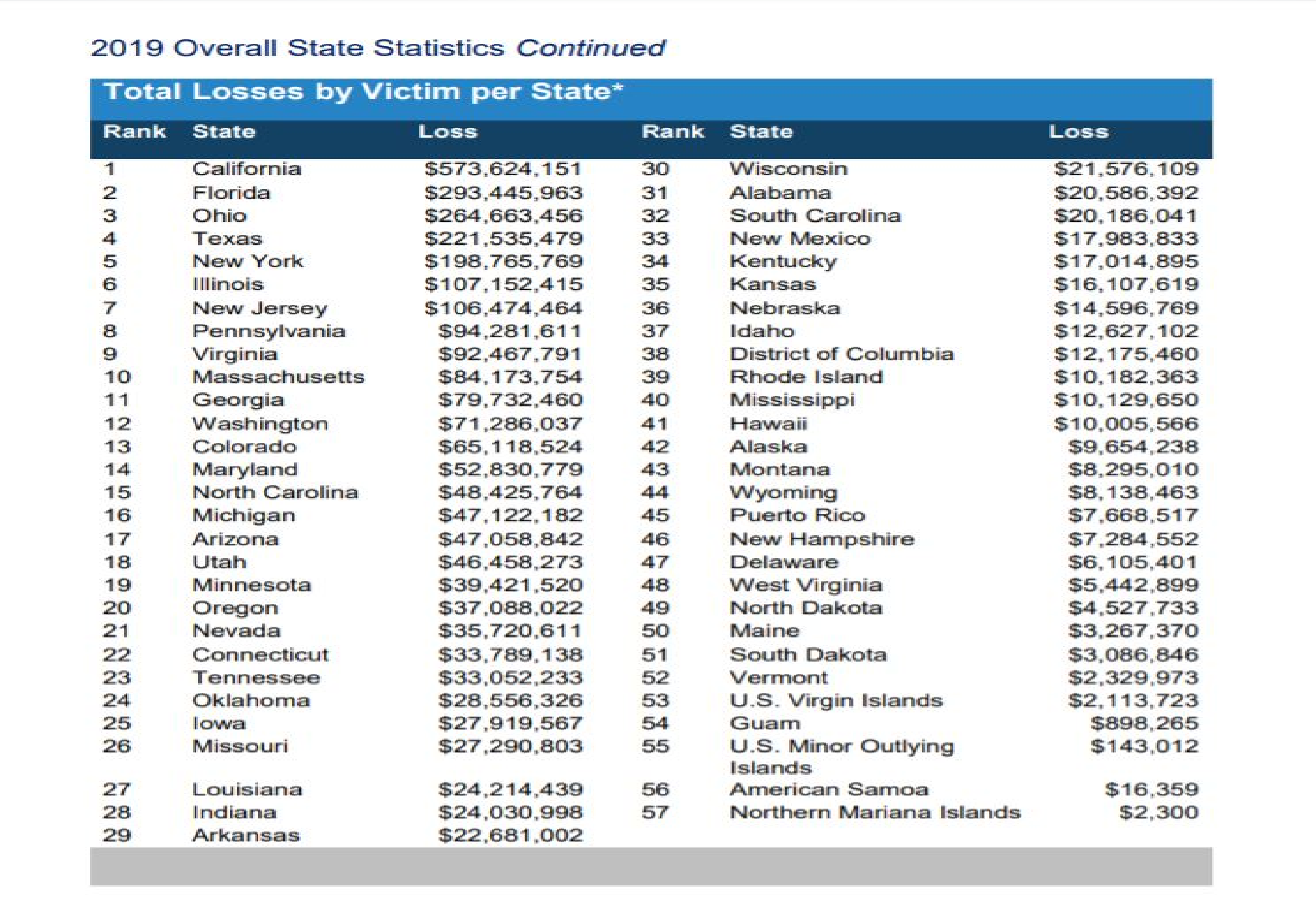
Crime Type	Loss	Crime Type	Loss
BEC/EAC	$1,776,549,688	Employment	$42,618,705
Confidence Fraud/Romance	$475,014,032	Civil Matter	$20,242,867
Spoofing	$300,478,433	Harassment/Threats of Violence	$19,866,654
Investment	$222,186,195	Misrepresentation	$12,371,573
Real Estate/Rental	$221,365,911	IPR/Copyright and Counterfeit	$10,293,307
Non-Payment/Non-Delivery	$196,563,497	Ransomware	**$8,965,847
Identity Theft	$160,305,789	Denial of Service/TDoS	$7,598,198
Government Impersonation	$124,292,606	Charity	$2,214,383
Personal Data Breach	$120,102,501	Malware/Scareware/ Virus	$2,009,119
Credit Card Fraud	$111,491,163	Re-shipping	$1,772,692
Extortion	$107,498,956	Gambling	$1,458,118
Advanced Fee	$100,602,297	Health Care Related	$1,128,838
Other	$66,223,160	Crimes Against Children	$975,311
Phishing/Vishing/Smishing/Pharming	$57,836,379	Hacktivist	$129,000
Overpayment	$55,820,212	Terrorism	$49,589
Tech Support	$54,041,053		
Corporate Data Breach	$53,398,278		
Lottery/Sweepstakes/Inheritance	$48,642,332		

Descriptors*	
Social Media	$78,775,408
Virtual Currency	$159,329,101

*These descriptors relate to the medium or tool used to facilitate the crime, and are used by the IC3 for tracking purposes only. They are available only after another crime type has been selected. Please see Appendix B for more information regarding IC3 data.

IC3 2019 Internet Crime Report - https://pdf.ic3.gov/2019_IC3Report.pdf

Cybersecurity 101



2019 Overall State Statistics *Continued*

Total Losses by Victim per State*

Rank	State	Loss	Rank	State	Loss
1	California	$573,624,151	30	Wisconsin	$21,576,109
2	Florida	$293,445,963	31	Alabama	$20,586,392
3	Ohio	$264,663,456	32	South Carolina	$20,186,041
4	Texas	$221,535,479	33	New Mexico	$17,983,833
5	New York	$198,765,769	34	Kentucky	$17,014,895
6	Illinois	$107,152,415	35	Kansas	$16,107,619
7	New Jersey	$106,474,464	36	Nebraska	$14,596,769
8	Pennsylvania	$94,281,611	37	Idaho	$12,627,102
9	Virginia	$92,467,791	38	District of Columbia	$12,175,460
10	Massachusetts	$84,173,754	39	Rhode Island	$10,182,363
11	Georgia	$79,732,460	40	Mississippi	$10,129,650
12	Washington	$71,286,037	41	Hawaii	$10,005,566
13	Colorado	$65,118,524	42	Alaska	$9,654,238
14	Maryland	$52,830,779	43	Montana	$8,295,010
15	North Carolina	$48,425,764	44	Wyoming	$8,138,463
16	Michigan	$47,122,182	45	Puerto Rico	$7,668,517
17	Arizona	$47,058,842	46	New Hampshire	$7,284,552
18	Utah	$46,458,273	47	Delaware	$6,105,401
19	Minnesota	$39,421,520	48	West Virginia	$5,442,899
20	Oregon	$37,088,022	49	North Dakota	$4,527,733
21	Nevada	$35,720,611	50	Maine	$3,267,370
22	Connecticut	$33,789,138	51	South Dakota	$3,086,846
23	Tennessee	$33,052,233	52	Vermont	$2,329,973
24	Oklahoma	$28,556,326	53	U.S. Virgin Islands	$2,113,723
25	Iowa	$27,919,567	54	Guam	$898,265
26	Missouri	$27,290,803	55	U.S. Minor Outlying Islands	$143,012
27	Louisiana	$24,214,439	56	American Samoa	$16,359
28	Indiana	$24,030,998	57	Northern Mariana Islands	$2,300
29	Arkansas	$22,681,002			

IC3 2019 Internet Crime Report -
https://pdf.ic3.gov/2019_IC3Report.pdf

Questions to ask clients

- Do they force patches out?
- How are employee terminations handled?
- Do they conduct third-party due diligence?
- Do they offer free Wi-Fi and conduct business on the same network?
- Do they train employees on cyber-risks?

Next Steps (Do)

1. Do remember you are a target

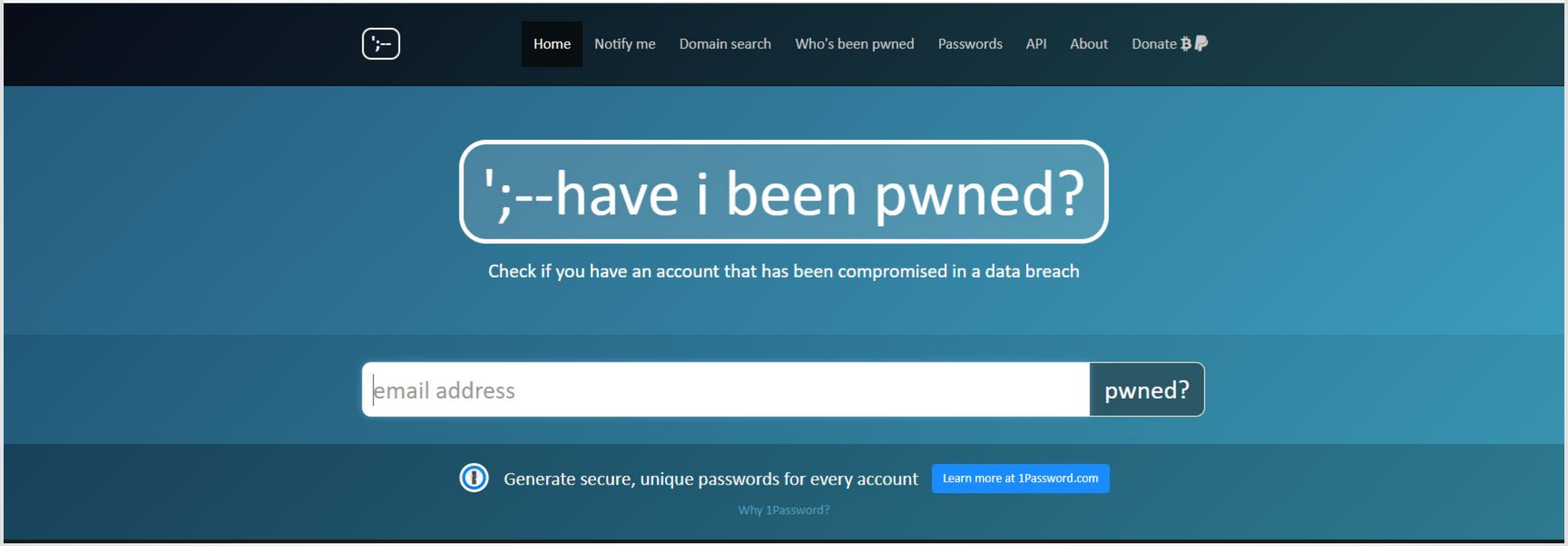
2. Do verify all information requests that you weren't expecting

3. Do have a password that is at least 12 characters long

4. Do use multi-factor authentication wherever possible

5. Do change default passwords

Cybersecurity 101



';--have i been pwned?

Check if you have an account that has been compromised in a data breach

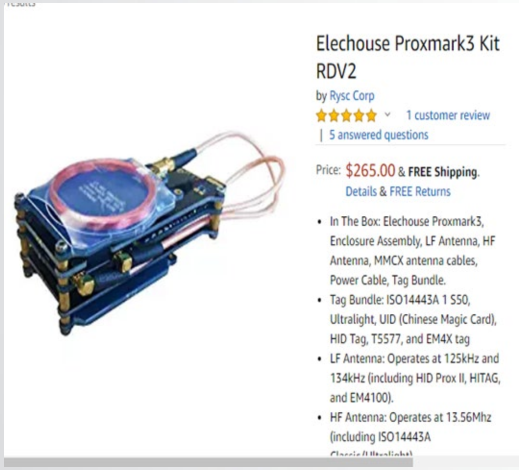
Generate secure, unique passwords for every account

Cybersecurity 101

Next Steps (Don't)

1. Don't Connect to "Free Wi-Fi"
2. Don't use the same password for everything
3. Don't create a document called "Passwords"…
4. Don't click on links that look strange
5. Don't allow strangers access to your devices

HACKING TOOLS AVAILABLE ON AMAZON…



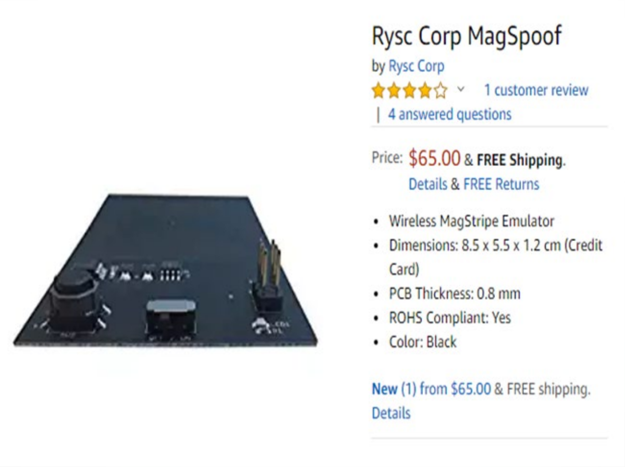
Elechouse Proxmark3 Kit RDV2

by Rysc Corp

★★★★★ 1 customer review | 5 answered questions

Price: $265.00 & **FREE Shipping**. Details & FREE Returns

- In The Box: Elechouse Proxmark3, Enclosure Assembly, LF Antenna, HF Antenna, MMCX antenna cables, Power Cable, Tag Bundle.
- Tag Bundle: ISO14443A 1 S50, Ultralight, UID (Chinese Magic Card), HID Tag, T5577, and EM4X tag
- LF Antenna: Operates at 125kHz and 134kHz (including HID Prox II, HITAG, and EM4100).
- HF Antenna: Operates at 13.56Mhz (including ISO14443A Classic/Ultralight)



Rysc Corp MagSpoof

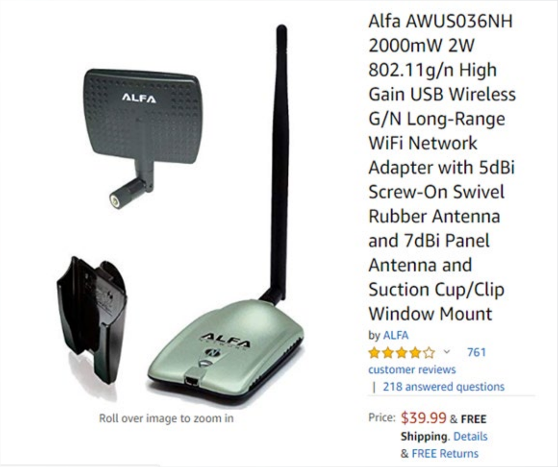
by Rysc Corp

★★★★☆ 1 customer review | 4 answered questions

Price: $65.00 & **FREE Shipping**. Details & FREE Returns

- Wireless MagStripe Emulator
- Dimensions: 8.5 x 5.5 x 1.2 cm (Credit Card)
- PCB Thickness: 0.8 mm
- ROHS Compliant: Yes
- Color: Black

New (1) from $65.00 & FREE shipping. Details



Alfa AWUS036NH 2000mW 2W 802.11g/n High Gain USB Wireless G/N Long-Range WiFi Network Adapter with 5dBi Screw-On Swivel Rubber Antenna and 7dBi Panel Antenna and Suction Cup/Clip Window Mount

by ALFA

★★★★☆ 761 customer reviews | 218 answered questions

Price: $39.99 & **FREE Shipping**. Details & FREE Returns

Roll over image to zoom in

New and Evolving Cyber Threats

- **Cyberattacks on Internet of Things (IoT)**
  - As more and more devices connect to the internet, including cameras, watches, activity trackers, cars, and more, there is an increased risk that these devices can be compromised. Some are concerned that these threats may be increased as 5G technology is rolled out.
- **Cloud Jacking**
  - An attack where hackers infiltrate the information, programs, and systems of businesses, stored in the cloud.
- **Remote Worker Endpoint Security**
  - Remote workers can be without network perimeter security, meaning a critical layer of cybersecurity defense is missing. Additionally, mobile devices can conceal warning signs of a phishing or other cybersecurity attack.

AI Cyberattacks and Deepfakes

- **Cyberattacks powered by AI**
  - Bad actors create programs using AI that mimic human behaviors, and then use these programs to trick people into giving up their sensitive information. Examples include "Deepfakes" – AI created fake images and sounds that appear real.
- **Deep Dive on Deepfakes**
  - Deepfakes leverage generative artificial intelligence to allow one individual to impersonate another individual in video and/or audio with remarkably realistic results.
  - Can you spot which video clip is fake or authentic? Try to guess while we walk through this deepfake quiz. https://www.cnn.com/interactive/2019/01/business/pentagons-race-against-deepfakes/
  - The first recorded deepfake hack, in 2019, involved an executive giving up $240,000 because of an urgent call from someone pretending to be the executive's boss.
  - Could deepfakes impact our industry?

Table-Top Exercise

Day 1: Thursday, September 3, 2020 – 9:00 a.m.

- A loan servicing specialist at First Place Lending contacts the IT Help Desk reporting that he has been locked out of his computer. He reports seeing a pop-up screen stating that the data on his computer has been encrypted and demanding payment to get the data back.

- The Help Desk asks the loan officer if he saw any previous anomalies on his computer. The employee says he does not recall anything out of the ordinary.

POLLING QUESTION 1

What Actions Should Be Taken After Learning of the Incident?

1 – Notify the FBI and local authorities to report the incident and submit a claim under the company’s cyber insurance policy.

2 – The IT Manager should notify the CISO to activate the company’s Incident Response Plan and work to preserve all available logs and other forensic evidence for an investigation.

3 – The IT team should send an email to all employees notifying them of the incident and ask if anybody else is having computer issues.

Day 1: Thursday, September 3, 2020 – 10:45 a.m.

- The IT Help Desk has now received calls from at least 30 users reporting that they are locked out of their computers.
- By 1:00 p.m., it is believed that more than 75 systems (workstations and servers) have been locked out.
- Employees and staff are asking questions as business operations have been severely disrupted.
- With the approaching holiday weekend, the team is short-staffed.

POLLING QUESTION 2

Based upon the current information, who else should be notified?

1 – Only members of the company’s Incident Response Team should be notified at this time.

2 – The company’s Incident Response Team and any applicable federal and state regulators.

3 – The company’s Incident Response Team, all employees, and all third party service providers.

Day 1: Thursday, September 3, 2020 – 5:00 p.m.

- Throughout the day, the IT team is able to analyze the pop-up screen seen on the loan servicing specialist’s computer, which has instructions for contacting the attackers.

- The pop-up screen states that First Place Lending has 96 hours to make the payment, but has no other information.

- First Place Lending determines that you have to contact the attackers to learn the amount of the demand and instructions for payment.

POLLING QUESTION 3

Given the current information, what are the company’s next steps?

1 – Retain outside counsel and a computer forensics company to assist with the investigation and reach out to the attacker to determine the ransom demand.

2 – Continue with investigating the matter internally since the initial findings are not serious and you’d prefer to avoid the expense of engaging third parties.

3 – Gather your communications team, considering retaining a public relations firm, and begin preparing a statement to your employees, customers, and third party business partners regarding the incident.

Considerations at the End of “Day 1”

- Based on the facts provided, what actions would you take?
- Who internally should be involved in the decision-making process at this point?
- Should the IT team contact the attacker? If so, how?
- What is the severity of this incident?
- Are there any persistent threats/risks known at this time?
- Should First Place Lending engage any third parties?
  - External counsel?
  - External PR firm?

Day 2: Friday, September 4, 2020 – 10:00 a.m.

- First Place Lending notifies its insurance carrier of the incident.

- The company also brings in outside counsel, who retained a third party forensics company to assist IT with the investigation.

- The forensics company anonymously reaches out to the attacker and reports back that the ransom demand is 110 bitcoin (approximately $1.2M) in exchange for the decryption keys to all impacted computers and servers.

- The deadline to pay the ransom is September 7, 2020 at 5:00 PM (Labor Day)

- Due to systems being encrypted, most business operations are suspended for the day.

POLLING QUESTION 4

Should the company pay the ransom?

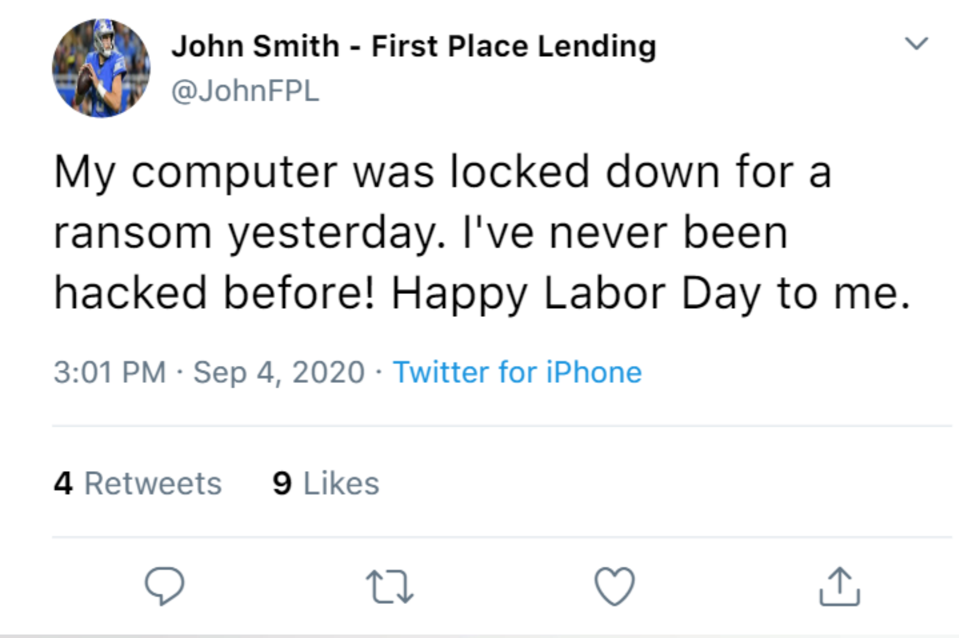
1 – Yes. The company needs to restore business operations ASAP.

2 – No. The company should not set a precedent of negotiating with attackers as it will lead to future attacks.

3 – Unsure. I need more information about the forensic investigation and whether data can be restored from backups.

Day 2: Friday, September 4, 2020 – Afternoon

- At 3:01 p.m., an employee of the company tweets about the incident from his personal account.
- At 3:29 p.m., a bank representative notes that she is having trouble accessing reports from First Place Lending and asks for help.
- By 5:00 p.m., First Place Lending's social media team has received multiple inquiries on Facebook and Twitter.

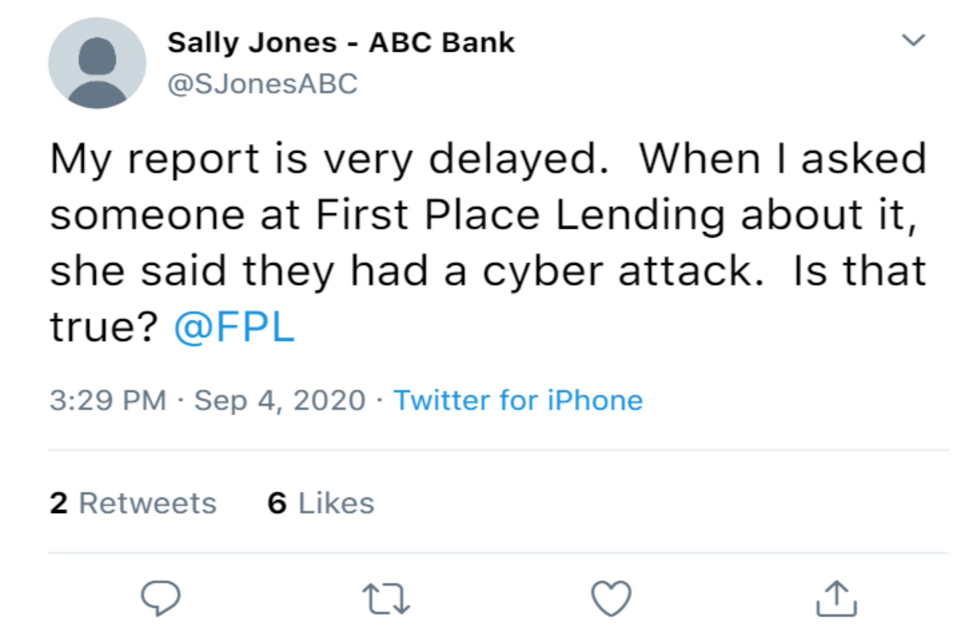


John Smith - First Place Lending
@JohnFPL

My computer was locked down for a ransom yesterday. I've never been hacked before! Happy Labor Day to me.

3:01 PM · Sep 4, 2020 · Twitter for iPhone

4 Retweets **9** Likes



Sally Jones - ABC Bank
@SJonesABC

My report is very delayed. When I asked someone at First Place Lending about it, she said they had a cyber attack. Is that true? @FPL

3:29 PM · Sep 4, 2020 · Twitter for iPhone

2 Retweets **6** Likes

POLLING QUESTION 5

How Should the Company Craft Its Media Message in Response to Social Media Posts and Concerned Customers?

1 – Release a holding statement that the company is investigating and will report back when there is additional information, but reassure the public that the company takes its customer’s data security seriously.

2 – Have a C-Suite member do an interview on TV stating that the investigation is ongoing and he/she cannot discuss anything further upon the advice of counsel.

3 – The CEO should release a written statement that there was a compromise, but the company has corrected the problem and has no reason to believe that the hacker was able to exfiltrate any customer data.

Considerations at the End of "Day 2"

- Based on the facts provided, what actions would you take?

- How do you handle the interruptions in business operations?

- How should the company deal with media issues?

Day 3: Saturday, September 5, 2020 – 8:00 a.m

- The IT team has been working to restore offsite backups of the impacted systems. The team reports that it will take approximately 10-14 days to recover all systems that have been impacted.

- After exchanges with the ransom negotiators, the attackers have lowered the ransom demand from 110 Bitcoin to 80 Bitcoin ($900,000).

- The IT team reports that certain critical data, including some customer information, may not be able to be restored on some systems as the data is corrupted.

- Given the likely delays and gaps in backups, a decision is made to pay the ransom.

- The attacker provides the decryption keys which are tested by the forensics company and determined to be clean. The IT team begins the decryption process starting with the highest priority systems.

Considerations at the End of “Day 3”

- Based on the facts provided, what actions would you take?

- How is a ransom paid? How do you pay in Bitcoin?

- What happens after a ransom is paid?

Day 6: Tuesday, September 8, 2020 – 9:00 a.m.

- The loan servicing specialist who originally reported the incident calls the IT Help Desk again. After thinking about it over the long weekend, he recalls receiving an email from FedEx two weeks ago regarding an undeliverable package. The email contained a link to verify his shipment.

- The loan officer said that he didn't think that he ordered a package. When he clicked on the link for more information, he received an error message.

Considerations at the End of “Day 6”

- Based on the facts provided, what actions would you take?
- How could you have prepared your employees to better respond to these emails?
- What kind of training do you do?
- Are you testing your employees?
- Do you have mechanisms established to help your employees report phishing attacks?
- What other measures are you taking to keep your employees aware of these potential threats?

Day 10

- The forensics team determines that the root cause of the incident was an email compromise. The attackers accessed the First Place Lending network on September 1, 2020 after the loan officer clicked on the malicious link in the FedEx email. This was two days before the ransomware was deployed.

- It is determined that the attackers were likely from Russia (based upon the IP addresses) and likely deployed the ransomware attack to cover their tracks after exfiltrating the data.

- The forensics team performed a scan of all company servers and employee email accounts and did not see any other compromised accounts. However, approximately 30GB of data was exfiltrated from the loan officer's account prior to the ransomware attack.

- The exfiltrated data from the loan officer's account includes a large amount of personally identifiable information ("PII"), including Social Security numbers.

- Media outlets are contacting the company requesting comment about the incident.

POLLING QUESTION 6

How Should the Company First Respond to the Findings of the Forensic Investigation?

1 – Focus on identifying all individuals whose information may have been impacted and prepare notification letters.

2 – Immediately report the incident to all applicable federal and state regulators.

3 – Review any contractual obligations to notify banks, vendors, or other third parties of the incident and evaluate what information must be provided

Additional Steps in Responding to the Incident

- Perform e-discovery review of the 30GB of data
- Assess whether notice is required to individuals and/or regulators
- Evaluate obligations to notify third parties pursuant to contracts
- Draft individual notice letters
- Obtain ID theft protection/credit monitoring, if warranted or required
- Draft media notices (if required)
- Establish a call center with FAQs for operators
- Develop long-term remediation plan based upon lessons learned
- Conduct additional employee training
- Audit effectiveness of Incident Response Plan and corrective measures

UPCOMING WEBINAR PRESENTATIONS REGISTER TODAY

Foreclosure Discovery and Trial Practice
Friday, August 14, 2020
1-2:15 PM Central Time

Bankruptcy Hot Topics
Tuesday, August 18, 2020
2-3:15 PM Central Time

Dealing with Deceased Borrowers & Heirs
Monday, August 17, 2020
1-2:15 PM Central Time

REGISTER FOR THESE WEBINARS AT www.ALFN.org/answerswebinars

WEBINAR WRAP-UP: QUESTIONS & ANSWERS

If you did not submit a question during your registration process, you may now use your GoToWebinar toolbox on the right side of your screen to submit a question directly to our panelists live on the air. Note: not all questions will be answered during the live Q&A. Should our panelists not be able to address your question, you may reach out to them directly or they will attempt to contact you with further information.

Matt White, CIPP/US, CIPP/E, CIPM
mwhite@bakerdonelson.com

Alex Koskey, CIPP/US, CIPP/E
akoskey@bakerdonelson.com

James McDowell
james.mcdowell@asc.alabama.gov

Jamie Stewart
jamiestewart@janewaylaw.com

Thank You Sponsors

Associate Member Partner

ā360inc™
Technology | Outsourcing | Consulting

Attorney-Trustee Member Partner

PADGETT
LAW GROUP

SAVE THE DATE: Upcoming ALFN EVENTS

View Past ALFN Webinars On-Demand at:
https://www.gotostage.com/channel/alfnwebinars

Bankruptcy Intersect 2021
March 4, 2021 – Marriott Dallas Las Colinas
Irving, TX
www.alfn.org *Registration Opens December 2020*

ANSWERS 2021
July 18-21, 2021 – Hyatt Regency Coconut Point Resort
Bonita Springs, FL
www.alfnanswers.org *Registration Opens February 2021*

ANSWERS 2022
July 17-20, 2022 – Hyatt Regency Tamaya Resort, Santa Ana Pueblo, NM
www.alfnanswers.org *Registration Opens February 2022*

WILLPOWER 2021
April 29-30, 2021 – The Ritz-Carlton Dallas
Dallas, TX
www.alfn.org *Registration Opens November 2020*

Foreclosure Intersect 2021
November 18, 2021 – Marriott Dallas Las Colinas
Irving, TX
www.alfn.org *Registration Opens August 2021*

ANSWERS 2023
July 16-19, 2023 – Park Hyatt Beaver Creek Resort, Beaver Creek, CO
www.alfnanswers.org *Registration Opens February 2023*

Thank you for attending this ALFN webinar presentation.

WEBINAR CONCLUSION

If you have any further questions that were not addressed in this presentation, or want to contact one of our speakers, please email info@alfn.org. Thank you for your participation in this webinar. Please complete the brief survey which you will be directed to at the conclusion of this presentation.

ALFN provides the information contained in these webinars as a public service for educational and general information purposes only, and not provided in the course of an attorney-client relationship. It is not intended to constitute legal advice or to substitute for obtaining legal advice from an attorney licensed in the relevant jurisdiction.

Use of ALFN Webinar Materials

The information, documents, graphics and other material made available through this Webinar are intended for use solely in connection with the American Legal and Financial Networks (hereinafter "ALFN") educational activities. These materials are proprietary to ALFN, and may be protected by copyright, trademark and other applicable laws. You may download, view, copy and print documents and graphics incorporated in the documents from this Webinar ("Documents") subject to the following: (a) the Documents may be used solely for informational purposes related to the educational programs offered by the ALFN; and (b) the Documents may not be modified or altered in any way. Except as expressly provided herein, these materials may not be used for any other purpose, and specifically you may not use, download, upload, copy, print, display, perform, reproduce, publish, license, post, transmit or distribute any information from ALFN Webinars in whole or in part without the prior written permission of ALFN.