KLEHR HARRISON HARVEY BRANZBURG LLP

CYBERSECURITY: What You Need to Know to Protect Your Business

Presentation by: Lisa A. Lori | llori@klehr.com | 215.569.2586

No Matter The Size: This Can Happen To You.

- In 2019, the Better Business Bureau (BBB) released a report with results from a survey conducted among 1,200 small businesses across the nation, showing that scams are a growing risk for businesses.
- Two thirds of those surveyed said they have been targeted by a scammer in the past three years.
- COVID-19 has caused scams to increase.
- April 20, 2020: “FBI Anticipates Rise in Business Email Compromise Schemes Related to the COVID-19 Pandemic.”

THE MAIN VULNERABILITY STEMS FROM THE WAY WE PAY
Wire / ACH.

FBI STATS

FBI's Internet Crime Complaint Center (IC3) saw the highest number of complaints and highest dollar losses reported in calendar year 2019.

467,361 complaints in 2019—an average of nearly 1,300 every day—and more than $3.5 billion in losses to individuals and businesses.

The most frequently reported complaints were phishing and similar ploys, non-payment/non-delivery scams, and extortion.

The most financially costly complaints involved business email compromise, and spoofing-mimicking the account of a person or vendor known to the victim to gather personal or financial information.

Donna Gregory, the chief of IC3, said that in 2019 the center didn't see an uptick in new types of fraud but rather saw criminals deploying new tactics and techniques to carry out existing scams.

"Criminals are getting so sophisticated," Gregory said. "It is getting harder and harder for victims to spot the red flags and tell real from fake."

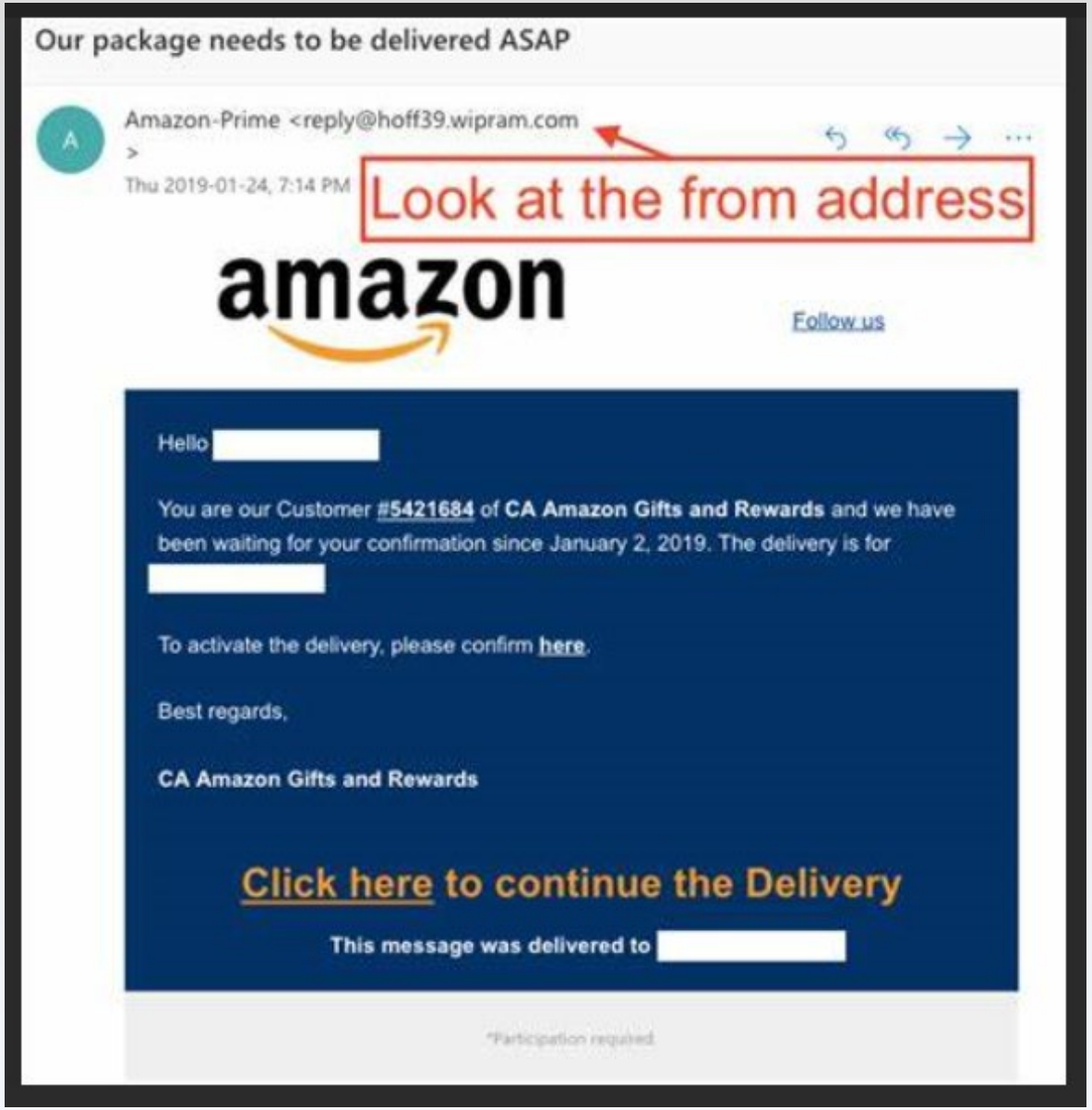
The Most Common Cyber Threats Today

1. Phishing
2. Business Email Compromise (BEC)
3. Ransomware
4. Data Leak
5. Hacking
6. Insider Threat

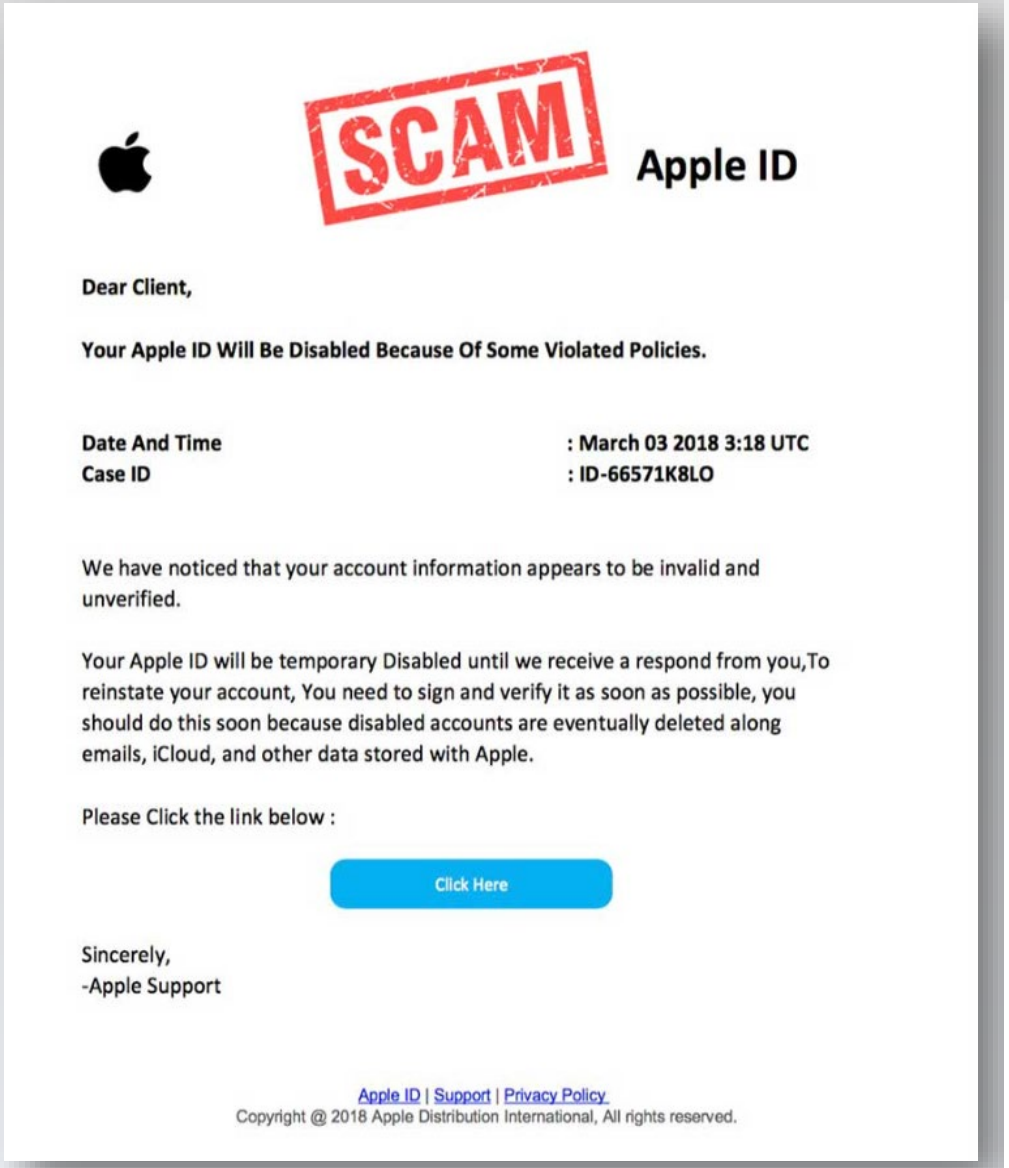
1

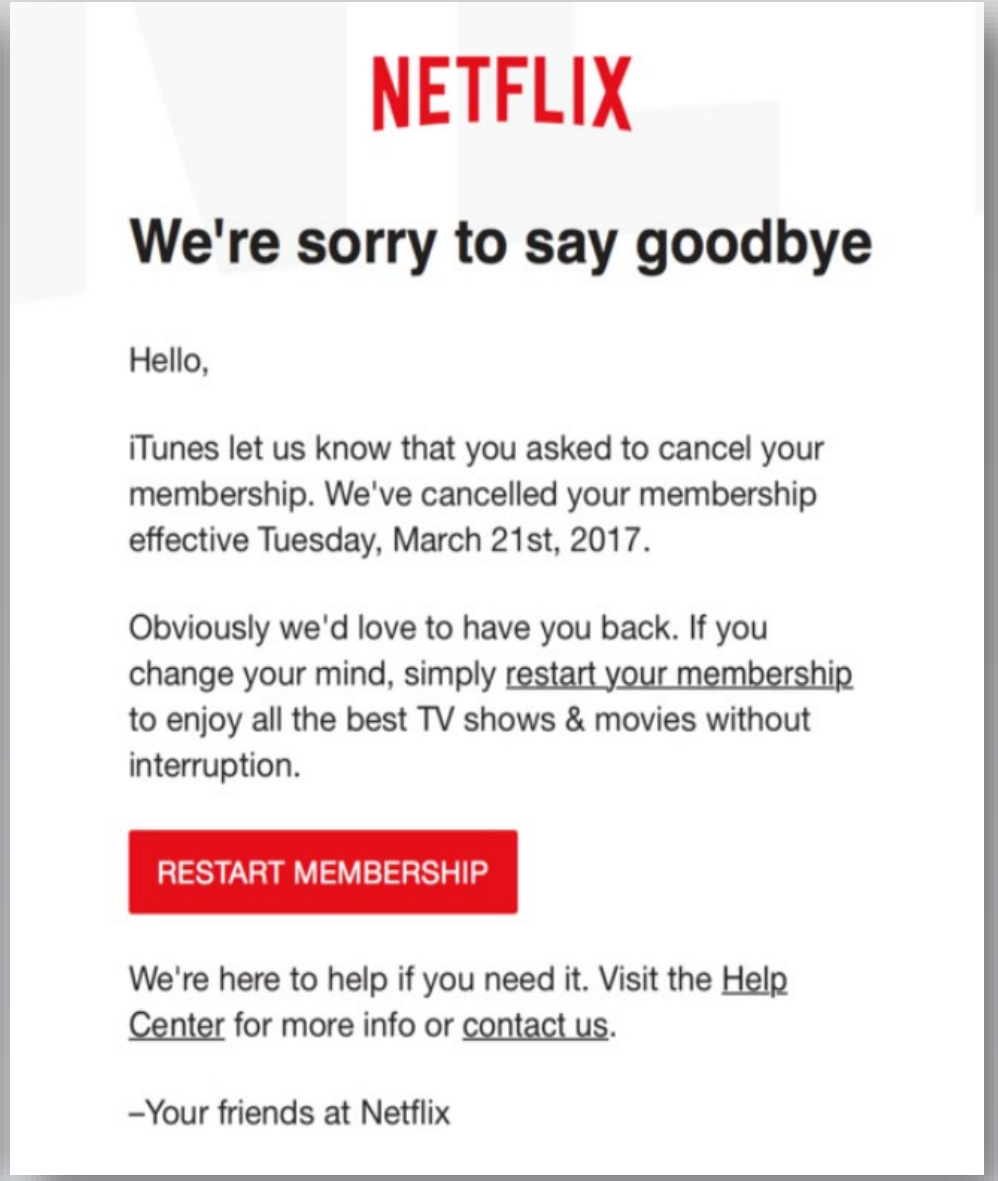
Phishing Scams

Phishing is a type of social engineering attack often used to steal user data, including login credentials and credit card numbers. It occurs when an attacker, masquerading as a trusted entity, dupes a victim into opening an email, instant message, or text message.



Phishing Scams





2 Business Email Compromise (BEC)

A criminal spoofs or mimicks a legitimate email address.

Criminals send an email message that appears to come from a known source making a legitimate request, such as a message that appears to be from an executive within their company or a business with which an individual has a relationship.

The email will request a payment, wire transfer, or gift card purchase that seems legitimate but actually funnels money directly to a criminal.

2 BEC Scams: How They Happen

A CYBER SCAMMER MIGHT:

Spoof an email account or website. Slight variations on legitimate addresses (susan@abcdef.com vs. susan@abcdf.com) -- victims think these fake accounts are authentic.

Send spearphishing emails. These messages look like they're from a trusted sender to trick victims into revealing confidential information. That information lets criminals access company accounts, calendars, and data that gives them the details they need to carry out the BEC schemes.

Use malware. Malicious software can infiltrate company networks and gain access to legitimate email threads about billing and invoices. That information is used to time requests or send messages so accountants or financial officers don't question payment requests. Malware also lets criminals gain undetected access to a victim's data, including passwords and financial account information.

OR A COMBINATION OF THE ABOVE.

2

Business Email Compromise Timeline

Step 1:
Identify a Target

Organized crime groups target U.S. and European businesses, exploiting information available online to develop a profile on the company and its executives.

Step 2:
Grooming

Spear phishing e-mails and/or telephone calls target victim company officials (typically an individual identified in the finance department).

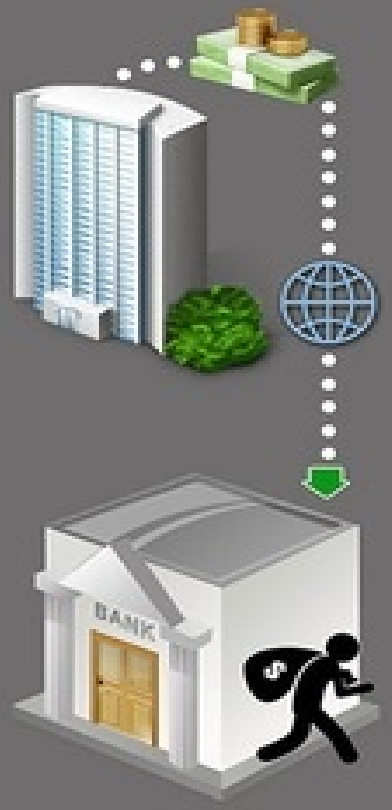
Perpetrators use persuasion and pressure to manipulate and exploit human nature.

Grooming may occur over a few days or weeks.

Step 3:
Exchange of Information

The victim is convinced he/she is conducting a legitimate business transaction. The unwitting victim is then provided wiring instructions.

Step 4:
Wire Transfer



Upon transfer, the funds are steered to a bank account controlled by the organized crime group.*

*Note: Perpetrators may continue to groom the victim into transferring more funds.

Source: FBI (https://www.fbi.gov)

EXAMPLES OF BEC SCAMS

FINANCIAL THEFT

Cybercriminals pose as a senior exec to request a wire transfer by email. These scams are often labeled as urgent, and are personalized to incorporate the employee's name whose help is being solicited.

W-2 AND PII THEFT

Cybercriminals pose as an admin or senior exec to request that someone from the HR or finance department send them employee W-2 information or PII over email.

PURCHASE ORDER FRAUD

Cybercriminals obtain publicly-available purchase order forms but change the contact/shipping info to receive goods they won't ever pay for.

ATTORNEY IMPERSONATION

Cybercriminals pose as attorneys or legal reps and then claim to be handling a case in order to request a fund transfer to cover "associated costs."

3

Ransomware/Malware

Ransom malware, or **ransomware**, is a type of **malicious software** that prevents users from accessing their system or personal files and demands ransom payment in order to regain access.

Ransomware cyber criminals - demand payments be sent via cryptocurrency or credit card.

Ransomware is often spread through phishing emails that contain malicious attachments or through drive-by downloading. Drive-by downloading occurs when a user unknowingly visits an infected website and then malware is downloaded and installed without the user's knowledge.

Ransomware Attacks Spike 148% Amid COVID-19 Scams

A new organization will fall victim to ransomware every 14 seconds in 2019, and every 11 seconds by 2021.

Ransomware attacks cost businesses in excess of $7.5 billion in 2019 alone.

4 Hacking

- **Hacking** generally refers to unauthorized intrusion into a computer or a network. The person engaged in **hacking** activities is known as a **hacker.** This **hacker** may alter system or security features to accomplish a goal that differs from the original purpose of the system.

5 Insider Threats

- An **insider threat** is a malicious **threat** to an organization that comes from people within the organization, such as employees, former employees, contractors or business associates, who have inside information concerning the organization's security practices, data and computer systems.
- **One-third** of all organizations have faced an insider threat incident.

Recent Cyber Scams

Pitney Bowes - October 2019

- A malware/ransomware attack “encrypted information on some systems and disrupted customer access to some of our services.”
- Second attack March 2020.

Honda - June 2020 (Ransomware)

- "Honda can confirm that a cyber-attack has taken place on the Honda network," the Japanese car-maker said in a statement.
- It added that the problem was affecting its ability to access its computer servers, use email and otherwise make use of its internal systems.
- "There is also an impact on production systems outside of Japan," it added.
- One of its internal servers was attacked externally.
- Honda added that "the virus had spread" throughout its network,
- Honda did not provide further details.

Alpha Broder (AB)

One of the largest suppliers of promotional apparel in the U.S.

Revenues of over $1.6 billion

In October and November of 2019, become a victim of a ransomware/malware attack

Order processing system was disabled

Alpha Broder (AB) Hack

Hacker organization entered AB's system through phishing email

One AB employee clicked on a link in the email and unknowingly allowed hacker to enter AB's system

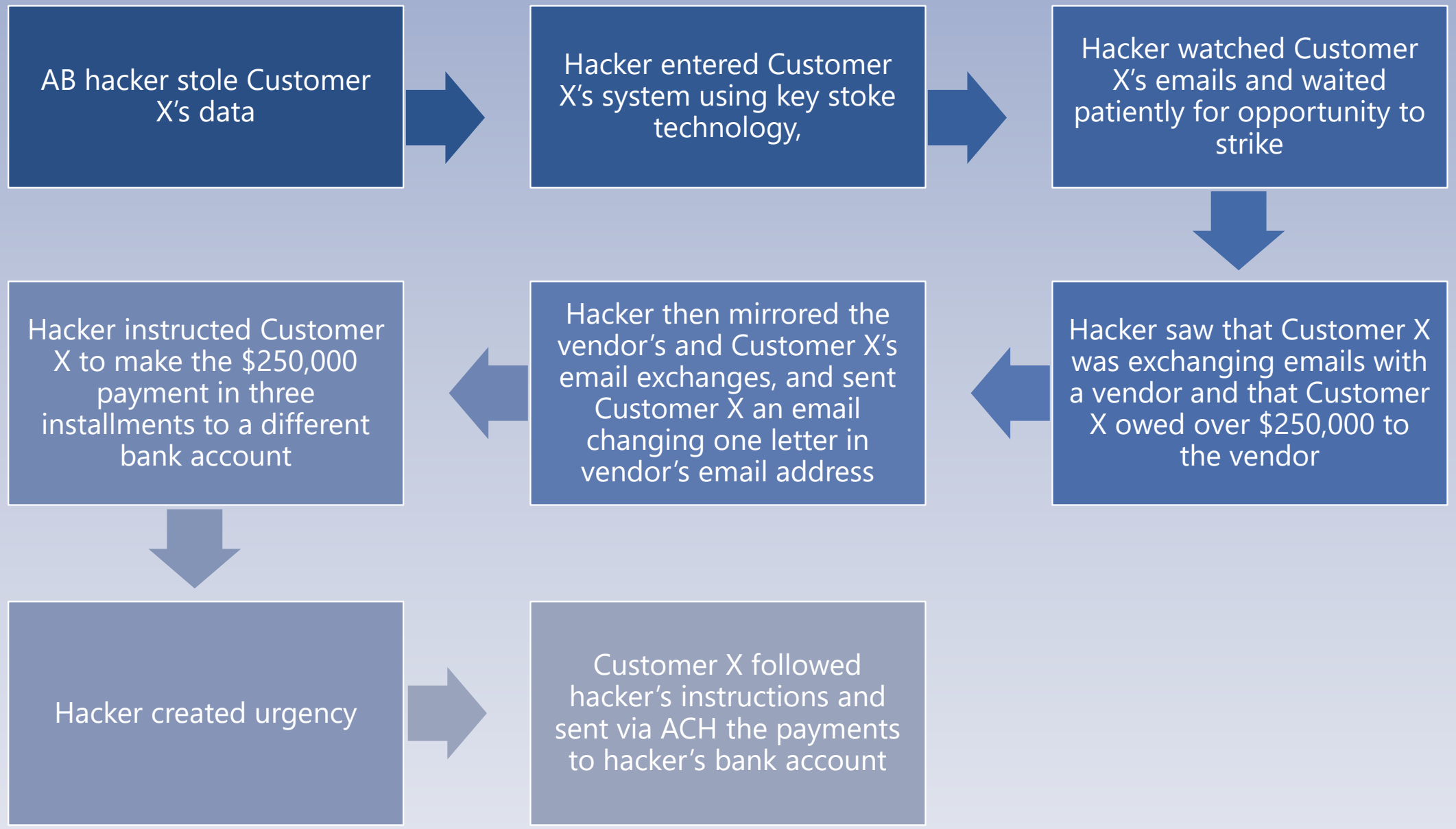
Hacker seized AB's system and took AB's data, including distributor/customer email addresses

Hacker proceeded to extort cash from AB in exchange for releasing AB's system

Hacker used AB's data to target the AB customers/distributors, including Customer X

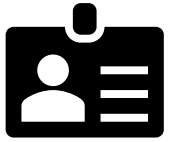
Led to AB's Customer X getting hacked through a BEC scam

AB Customer X



Protecting Yourself and Your Business from Attacks

Check the email address that it is coming from – while the name of the sender may appear legit, the email address behind it won't be. If any doubt, call the sender to verify.



If you have clicked to download an attachment, immediately disconnect your device from your network. If you are using a wired connection, unplug it. If you are accessing WiFi, disable the connection. Contact your help desk or your IT Service for next steps (Geek Squad) etc.

If you have accidentally followed a link and entered your password details, change your password immediately and contact your help desk or IT service for next steps. You may want to lockdown your account for a period to block out any attempted logins.

Slow down and look for dead giveaways

Verify, Verify, Verify

If it feels wrong, it probably is.
Trust your gut and verify.

- ✓ If you are asked to remit payment anywhere, even if from a known vendor or partner, DON'T. Call the vendor/partner and VERIFY the request.
- ✓ Look for strange grammar or requests to change payment details.
- ✓ If you are directed to a sign in page from any email, check the legitimacy of the sender and the URL.
- ✓ Check the email address to make sure it is exact not "close but no cigar."
  e.g., jim@betterbusiness.com vs. jim@beterbusiness.com

Simple Protective Measures

- When you walk away from your device (computer, phone, iPad etc.), ensure it is locked. Passwords should be set to a min of 8 characters with a mixture of upper, lower, numeric and symbols.
- Never share your password.
- Ensure that passwords you use for business are different from any other passwords you may use in your personal life. (this means that if someone else has a breach e.g. Netflix, Amazon, Skype etc., the password you used in their system doesn't allow the criminal who now has it to access your work accounts).
- Likewise, if you use more than one password for business related accounts, ensure that they are different for each account--if the criminal gets into one of your accounts, they can't then jump to others.
- Change your passwords frequently. It's inconvenient, but it will offer you protection. A password locker app can help to keep track of it all.

Wire vs. ACH

- **Sometimes Slower is Really Better**

- Sadly, often in the case of cyber crime, once a payment has been sent it is long gone and recovery is next to impossible
- Wire transfer are immediate near impossible to recover
- ACH – takes 3/5 days to clear, if the transfer is caught quickly you may be able to reverse the funds – **quick and persistent action is the key**

Oh No! I sent a payment to a cyber criminal by mistake. What can I do?

You need to act fast and be persistent:

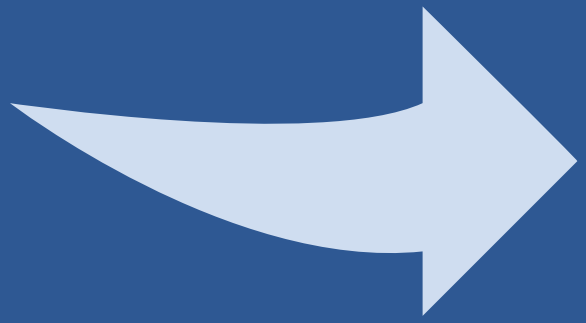
- ❑ Remember this is fraud.
- ❑ **Report it to your local authorities and file a report,** your bank will need this if there is any chance to recover the funds.
- ❑ **Report it to the FBI:** https://www.ic3.gov/complaint/default.aspx
- ❑ Call both your financial institution and the receiving financial institution and report the fraudulent activity.
- ❑ **BANKS WILL RUN YOU AROUND. ESCALATE THE SITUATION.**
- ❑ Go to your local branch and make friends who can help you assist you in escalating/navigating the bank.
- ❑ Bring counsel in if needed to assist in escalating.
- ❑ Do not continue to engage with the cyber criminals in hopes of getting your money back.
- ❑ Lock them out and change all passwords immediately.

Remember:

Always:

- Slow down
- Verify
- Confirm
- Stay vigilant
- Change passwords frequently

Final Action:

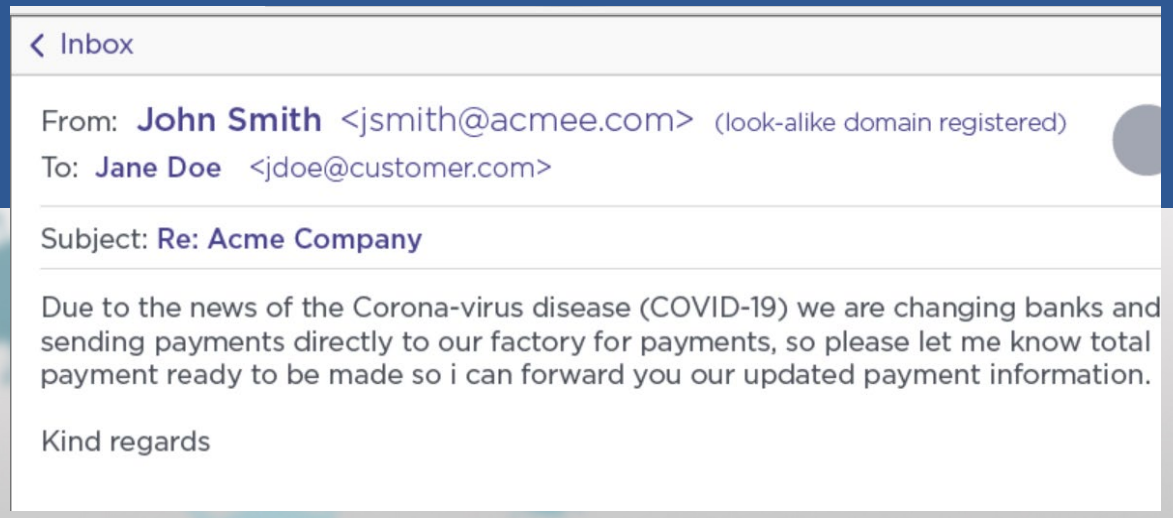


- Close the “at risk” bank account, new accounts will need to be opened
- Investigate your financial institutions cyber crime protections
  - If you approved the wire is it fraud?
- Put a fraud alert on your accounts – to alert you if anyone tries to open credit accounts in your name. You can do this by contacting any of the credit reporting agencies (Equifax, Transunion, etc.)
- Set up protections through Credit Wise / or Life Alert
- Share your story to protect others from falling victim

Post-COVID-19 Cyber Scams

- April 2020: **"FBI Anticipates Rise in Business Email Compromise"**
- Scams are targeting purchasers of personal protective equipment or other supplies needed in the fight against COVID-19.
- In a typical BEC scheme, the victim receives an email they believe is from a company they normally conduct business with, but this specific email requests funds be sent to a new account or otherwise alters the standard payment practices.
- **Recent examples of BEC attempts include:**

A financial institution received an email allegedly from the CEO of a company, who had previously scheduled a transfer of $1 million requesting that the transfer date be moved up and the recipient account be changed "due to the Coronavirus outbreak and quarantine processes and precautions." The email address used by the fraudsters was almost identical to the CEO's actual email address with only one letter changed.



Advice from the FBI

To protect from this fraud, be on the lookout for the following red flags:

- Unexplained urgency.
- Last minute changes in wire instructions or recipient account information.
- Last minute changes in established communication platforms or email account addresses.
- Communications only in email and refusal to communicate via telephone or online voice or video platforms.
- Requests for advanced payment of services when not previously required.
- Requests from employees to change direct deposit information.

The following can help protect yourself and your assets:

- ✓ Be skeptical of last-minute changes in wiring instructions or recipient account information.
- ✓ Verify any changes and Information via the contact on file—do not contact the vendor through the number provided in the email.
- ✓ Ensure the URL in emails is associated with the business it claims to be from.
- ✓ Be alert to hyperlinks that may contain misspellings of the actual domain name.
- ✓ Verify the email address used to send emails, especially when using a mobile or handheld device, by ensuring the sender's email address appears to match who it is coming from.
- ✓ If you discover you are the victim of a fraudulent incident, immediately contact your financial institution to request a recall of funds and your employer to report irregularities with payroll deposits. As soon as possible, file a complaint with the FBI's Internet Crime Complaint Center at ic3.gov or, for BEC and/or email account compromise (EAC) victims, **bec.ic3.gov**.

Minimizing Cyber Breaches

Conduct an asset audit, including identifying and prioritizing assets (such as customer information, banking information, manufacturing processes, payment processing information, trade secrets, etc.)

Identify and prioritize threats and vulnerabilities to those assets-i.e., what would happen to the company if there was a breach that exposed or compromises these assets or data?

Identify ways to protect those assets/data.

- Identify document information flows—e.g., how is the data obtained, where is it stored, how does it flow and who at the company has access to it.
- Establish policies and procedures for cybersecurity.

Maintain hardware and software inventories.

Identify all third-party contracts and document those relationships, including access they have to your business information.

Minimizing Cyber Breaches

Develop and implement safeguards for ensuring that your critical information, processes and data ca be recovered in the event of a breach.

- Conduct regular back-ups and maintain one back-up offline.
- Limit access to data to only employees or individuals who need to know the information to perform their jibs.
- Use encryption.

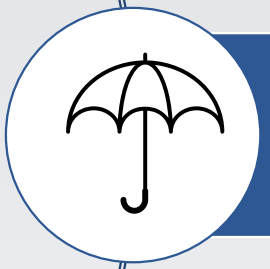
Create a response and recovery plan in the event of a breach and include communication and notification protocols.

Protect your network with patches and appropriate software and firewalls.

TRAIN YOUR EMPLOYEES and have them sign off on your company's cyber-policies and consequences of non-compliance.

Cyber-Insurance

Cyber-insurance may provide coverage for internet-based risks, including IT infrastructure, data breaches.



In some cases, it may provide coverage for cyber scams.

Speak with insurance broker to determine if this insurance is appropriate for you.

Cyber-Insurance

Typically covers financial losses that result from data breaches and other cyber events.

Can include both first-party and third-party coverages.

First-party coverage pays expenses your company directly incurs as result of the breach, such as the cost of informing your customers about a hacker attack.

Third-party coverage applies to claims against your company by customers/vendors who injured as a result of your actions or failure to act. (E.g., a customer sues you for negligence after a hacker steals his personal data from your computer system and releases it online.)

Not all losses are covered.

Thank You!

Questions?

Lisa A. Lori, Partner

llori@klehr.com | 215.569.2586

KLEHR HARRISON
HARVEY BRANZBURG LLP