

Receivables and Payables: Protections Against Low & High Tech Fraud

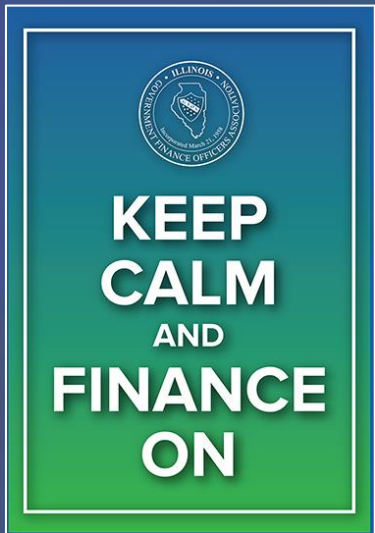
J.P.Morgan Chase Bank

Presenters:

Max Alexander; max.alexander@jpmchase.com

Eileen Roberts; eileen.roberts@jpmorgan.com

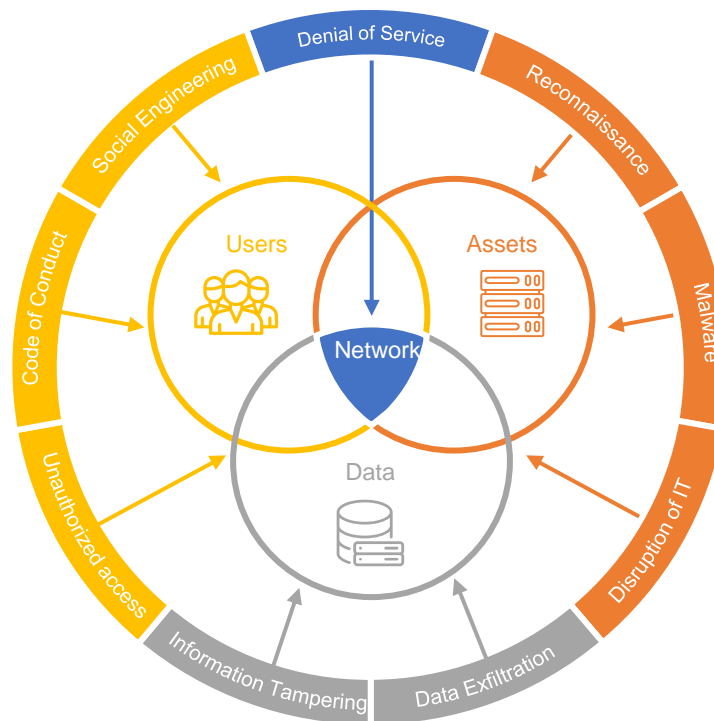
Justin Erkfritz-Gay; justin.r.erkfritz-gay@jpmorgan.com



IGFOA ANNUAL CONFERENCE • SEPTEMBER 13–14, 2021

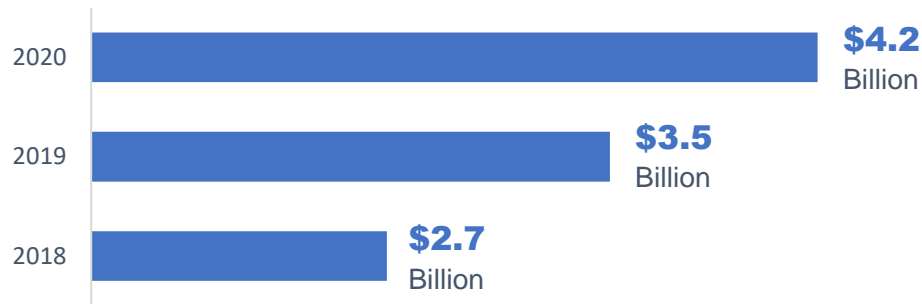
Changing Risk Landscape

- Cybersecurity incidents as it applies to Confidentiality, Integrity and Availability (CIA) triad:
 - **Confidentiality:** Unauthorized data exposure, e.g., exposure/theft of client data, unpublished prices, sensitive information, HR data or cross border/information barrier breaches
 - **Integrity:** Cybercrime and fraud, e.g., manipulation of data with the intention of adjusting payment instructions or prices
 - **Availability:** Malicious disruption of IT, e.g., distributed denial of service (DDoS) attacks, destructive malware attacks intended to delete critical systems (Wiper) or internal sabotage
- Growing business email compromise and ransomware attacks
- Increasing regulation
 - General Data Protection Regulation (GDPR)
 - California Consumer Privacy Act (CCPA)
 - International Regulatory Requirements
- Heightened expectations on internal controls
- Large dependencies on third parties
- Heavy reliance on electronic communication



Cyberfraud by the Numbers

Total losses from cybercrimes in **2020**¹

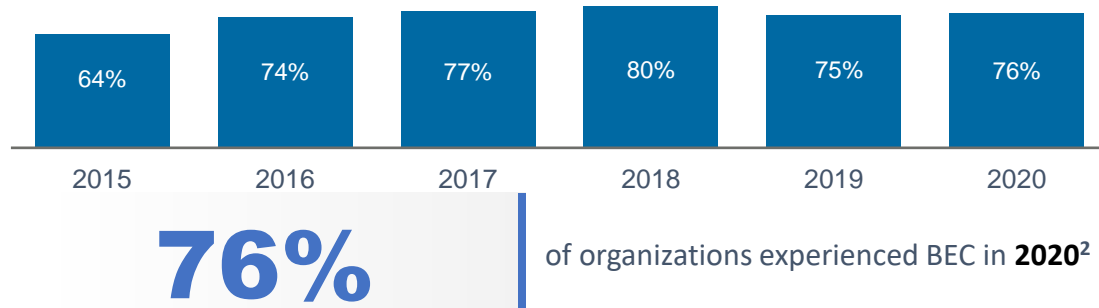


Percent of companies targeted by **Fraud Attacks**

74%

of surveyed companies were targets of attempted or actual fraud in **2020**², a decrease from 81% in 2019

Business email compromise (**BEC**) attacks near all-time high



Complaints to the **FBI**

791,790

Complaints were reported to the FBI's Internet Crime Complaint Center in **2020**¹, up from **467,361** reported in **2019**. That's more than **2,000** complaints a day

¹Federal Bureau of Investigation's 2020 Internet Crime Report; ²The 2021 Association for Financial Professionals Payments Fraud and Control Survey Report

No Industry is Immune



FINANCIAL

- **Feb. 2021:** The U.S. DOJ accused North Korean actors of conspiring to steal and extort more than \$1.3 billion in cash and cryptocurrencies.
- **Aug. 2020:** A five-day long DDoS attack against the New Zealand Stock Exchange forced a trading halt. The attackers may have been seeking extortion payments.



GOVERNMENT

- **Nov. 2020:** The U.S. conducted offensive cyber operations against Iran to prevent U.S election interference
- **Oct. 2020:** Unknown actors targeted the U.S. Census Bureau, likely to collect bulk data, alter registration information or compromise census infrastructure.



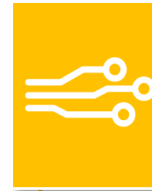
TRAVEL

- **May 2020:** Chinese state actors accessed the travel records of 9 million customers of U.K. airline group EasyJet.
- **March 2020:** The information of 5.2 million Marriott guests was accessed using stolen employee login credentials.



HEALTHCARE

- **2020:** North Korean, Russian and Chinese state actors targeted government agencies and pharmaceutical companies for COVID-19 vaccine information.
- **Sept. 2020:** Universal Health Systems suffered a ransomware attack causing hospitals to revert to manual backups, divert ambulances and reschedule surgeries.



TECHNOLOGY

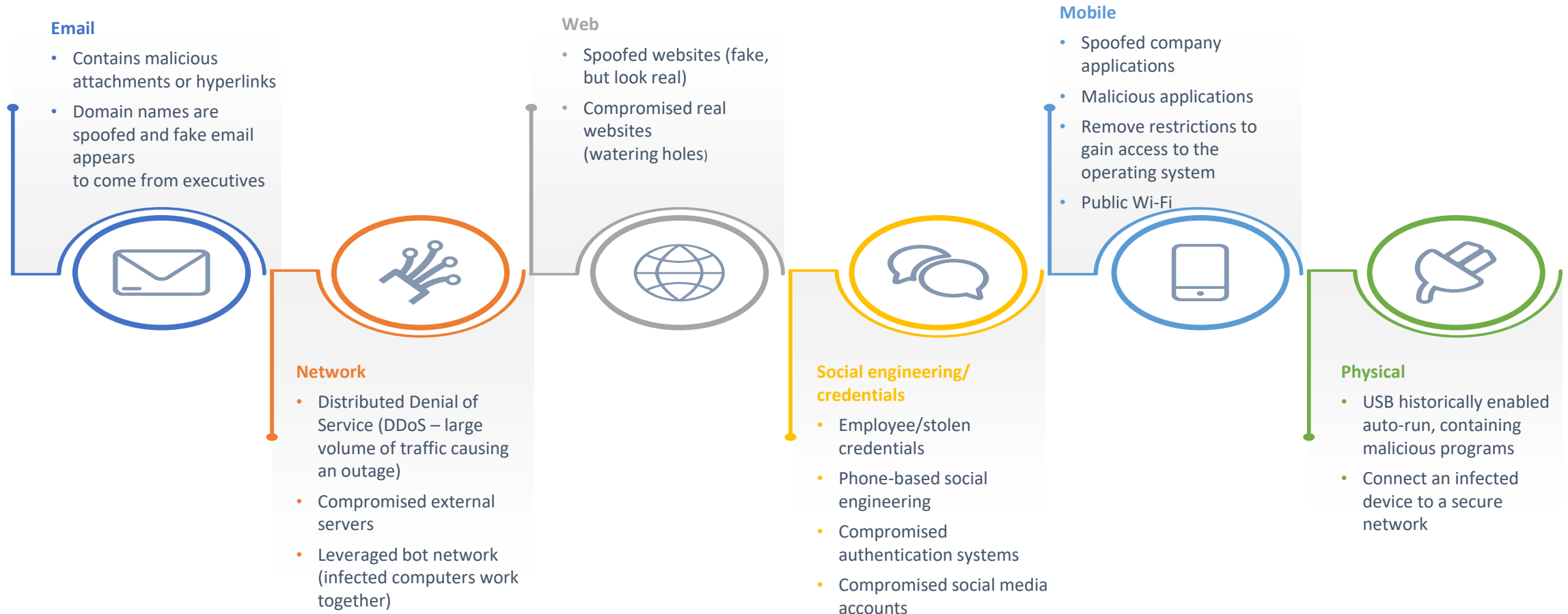
- **Dec. 2020:** Over 200 organizations worldwide including U.S. technology and government agencies were impacted by a software supply-chain attack against SolarWinds.
- **Oct. 2020:** German software giant Software AG suffered a ransomware extortion attack, which demanded a \$20 million payment and leaked stolen data.



OTHER

- **March 2021:** Chinese state actors targeted zero-day vulnerabilities in Microsoft's enterprise email software to steal data from over 30,000 organizations worldwide, including government agencies, law firms, defense contractors and infectious disease researchers. Once revealed, other groups exploited the vulnerabilities to conduct their own operations.

Vectors of Attack



Business Email Compromise (BEC)

- All companies and industries are affected and at high risk for large fraud losses and reputational damage

BEC occurs when criminals use email to trick victims into sending them their money or data.

Email Phishing

Most BEC attacks start with an email compromise that impacts the victim or their business partner. Phishing attacks are a very popular method to compromise email accounts.

Lookalike Domains

Fraudsters will sometimes use compromised email accounts to communicate with victims, but in many cases will use email domains that look deceptively similar to the email domain they are impersonating. For example, if they are pretending to be “company.com,” they might use the domain “cornpany.com” by replacing the “m” with “rn.”

Executive Impersonation BEC

Fraudsters use email to impersonate a corporate executive to trick an employee at the targeted company to send money to the fraudsters.

Business Partner/Vendor Impersonation BEC

Fraudsters use email to impersonate a client’s vendor and trick the victim into changing payment instructions for legitimate invoices. When the victim receives the legitimate invoice, they pay the fraudster instead of their vendor. This can go on for some time until their legitimate vendor contacts them about non-payment of the invoices.

What Does BEC Look Like?

Best Practices

- Train employees on suspicious email trends and test them regularly
- Consider available email security solutions to defend against lookalike domains
- Enable controls so all emails from outside your company are marked as external
- Establish parameters to detect inbox forwarding rules that send emails to external addresses or prohibit the practice altogether
- Ensure employees verify all payment account changes

Key Message

Always perform a callback to the person making a request using a phone number from a system of record for any requests for payment, change of payment instructions or change of contact information.

Vendor BEC Example

The screenshot shows an email client window titled "Tue 3/3/2020 8:34 AM". The email header includes "From: Alissa Teal <a.teal@marquettefarm.com>", "Subject: Urgent Vendor Payment", and "To: James McKnight". The body of the email starts with "Jim," followed by "Can you help me with an urgent payment? Please respond." and "Kindly email me as soon as possible." Below this is the signature "Alissa Teal, Chief Executive Officer, Marquette Farm Equipment (123) 456-7890".

Security annotations are overlaid on the email:

- A green thumbs-up icon and "Good domain marquettefarm.com" are shown above the email header.
- A red thumbs-down icon and "Bad domain marquettefarm.com" are shown above the email header.
- A yellow warning triangle icon is placed next to the word "Kindly" in the body text, with a callout box stating "Classic BEC word 'Kindly' instead of 'Please'".
- A yellow warning triangle icon is placed at the bottom of the email body, with a callout box stating "Putting pressure on the reader through a sense of urgency by authority".

Red dashed lines connect the domain annotations to the email header and the "Kindly" annotation to the body text. The email client interface includes standard buttons like "Cc Bcc", "Send", and "Star" at the bottom.

Phishing

Phishing is the fraudulent practice of sending either blanket emails to large groups or targeted emails to individuals within a company.

Cyber criminals use phishing schemes to trick victims into directly divulging information or downloading malware to be used for financial fraud or as a way to infect or gain access to systems.

Risks

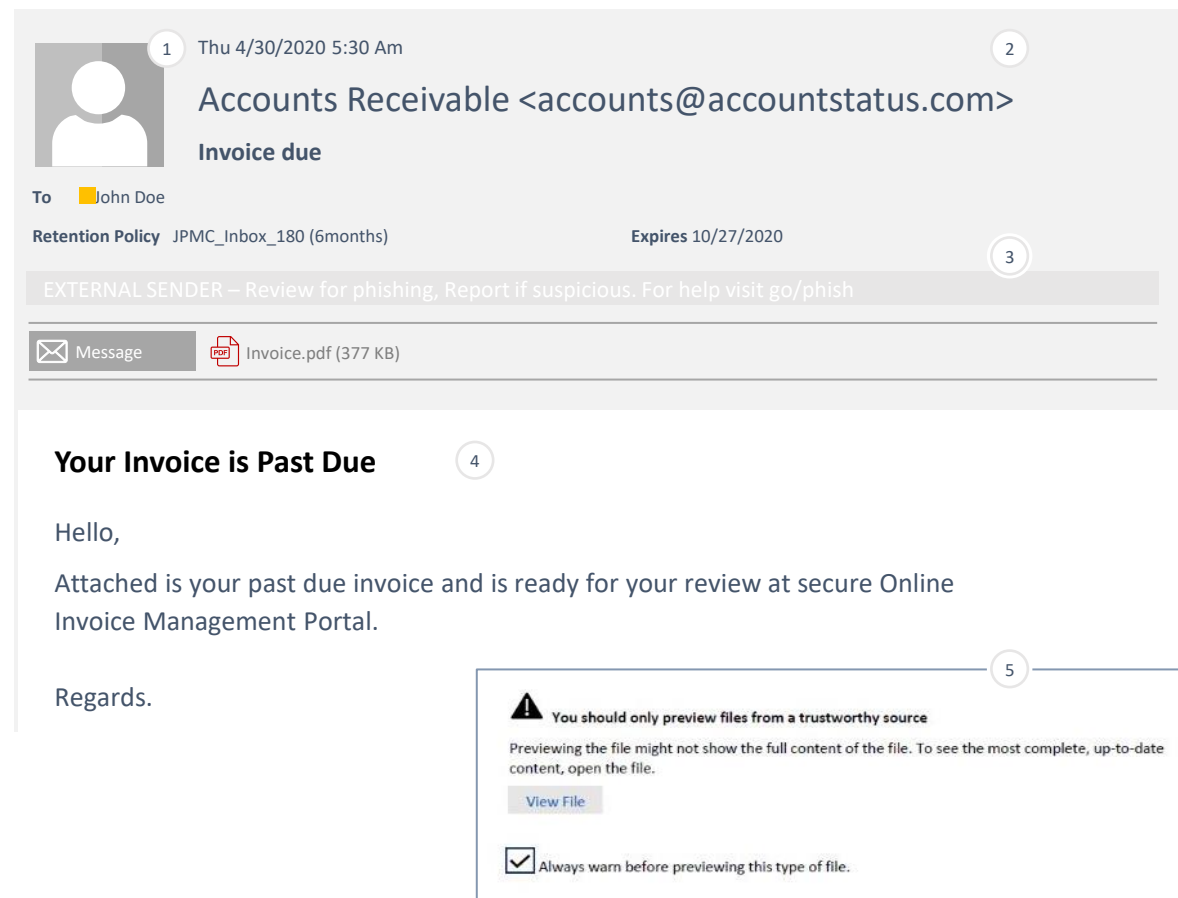
- Do not click on suspicious links or open attachments from employees or known vendors. This can spread the phishing virus to others.
- Suspicious emails will have a sense of urgency or ask for personal information.
- The language in the email may include typos or other misspellings.
 - Recent phishing trends are becoming more sophisticated and don't always include grammatical errors.
- If you are not sure if the sender of the email is legitimate, hover your mouse over the email address to confirm the spelling and web domain.

What Does Phishing Look Like?

Warning Signs

- Sender name is vague and generic
- Sender address has a suspicious domain
- Email includes an external banner indicating it's coming from outside the company
- Uses urgent or authoritative language demanding a quick response
- PDF attachment "View File" button is a link but not a PDF

Phishing Example



SMiShing & Vishing

SMiShing (short for “SMS phishing”) is a social engineering attack conducted via text message.

Vishing, a combination of “voice” and “phishing,” is another form of social engineering designed to lure an employee into providing sensitive or personal information.

Signs of SMiShing



Incoming phone number

Blocked, short or similar to your phone number – but be careful! Real phone numbers can be spoofed as well.



Call to action

The text asks you to click a link, respond or call a phone number to solve a problem



Urgency

The text makes you feel like there could be negative consequences for not taking immediate action (e.g., your account will be locked)



Unexpected

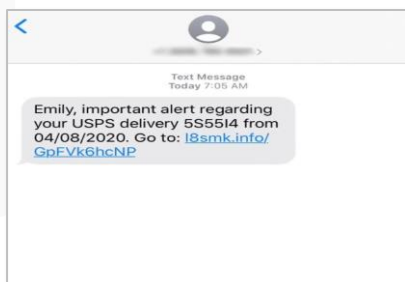
Anything that feels abnormal probably is! For example, tech support calling about weekend upgrades, the CEO calling about a funds transfer or HR calling to ask for personal information



Unprofessional Spelling and/or grammatical mistakes

Signs of Vishing

- The incoming phone number may look odd or very short, or even similar to a cell phone or company phone number.
- A criminal may mumble fake information in order to obtain real personal information by attempting to have the victim clarify the information.
- There may be a sense of urgency to the request. A criminal might imply that there will be problems if the employee doesn't provide the information quickly, or they use a positive approach, saying, “If you get this for me right now you will be a hero!”
- Be on the alert for unexpected calls offering or requesting help. A criminal may ask for help while impersonating another employee or executive. Always validate these types of requests by calling the employee or executive at a known telephone number.



SMiShing example

Ransomware

Ransomware is a growing trend in which cybercriminals extort organizations by encrypting and holding their data hostage until a ransom payment is made

Risk

- Loss of the ability to run your organization and potential permanent loss of data.

How much is the ransom?

- The cost of the ransom varies and depends on the type of ransomware and the cybercriminals behind it.
- The average paid ransom is \$170,404.10 (in U.S. dollars).

Should I pay the ransom?

- The FBI does not support paying a ransom to a cybercriminal because payment does not guarantee an organization will regain access to its data. In fact, some organizations report never having received decryption keys after paying a ransom.
- A recent survey found that only 8% of organizations managed to get back all of their information after paying money to ransomware operators, while 29% received no more than half of their data.¹

How do I ensure my organization is resilient?

- Perform a Business Impact Analysis (BIA): A BIA predicts the consequences of a disruption to a business function or process, and gathers information needed to develop recovery strategies.
- Identify critical systems: This process begins by identifying what systems or resources your organization needs to continue or resume operations after a disaster.
- Develop the plan: Once you have identified which systems are a priority for recovery, the next step is to determine how you are going to do it. You'll want to decide a timeframe to restore your systems, what resources you will need and who will implement the recovery efforts.
- Test and exercise: It is critical to test a recovery plan, especially considering the plan is what your organization will rely on during its worst day.

¹ Sophos The State of Ransomware in 2021 Survey

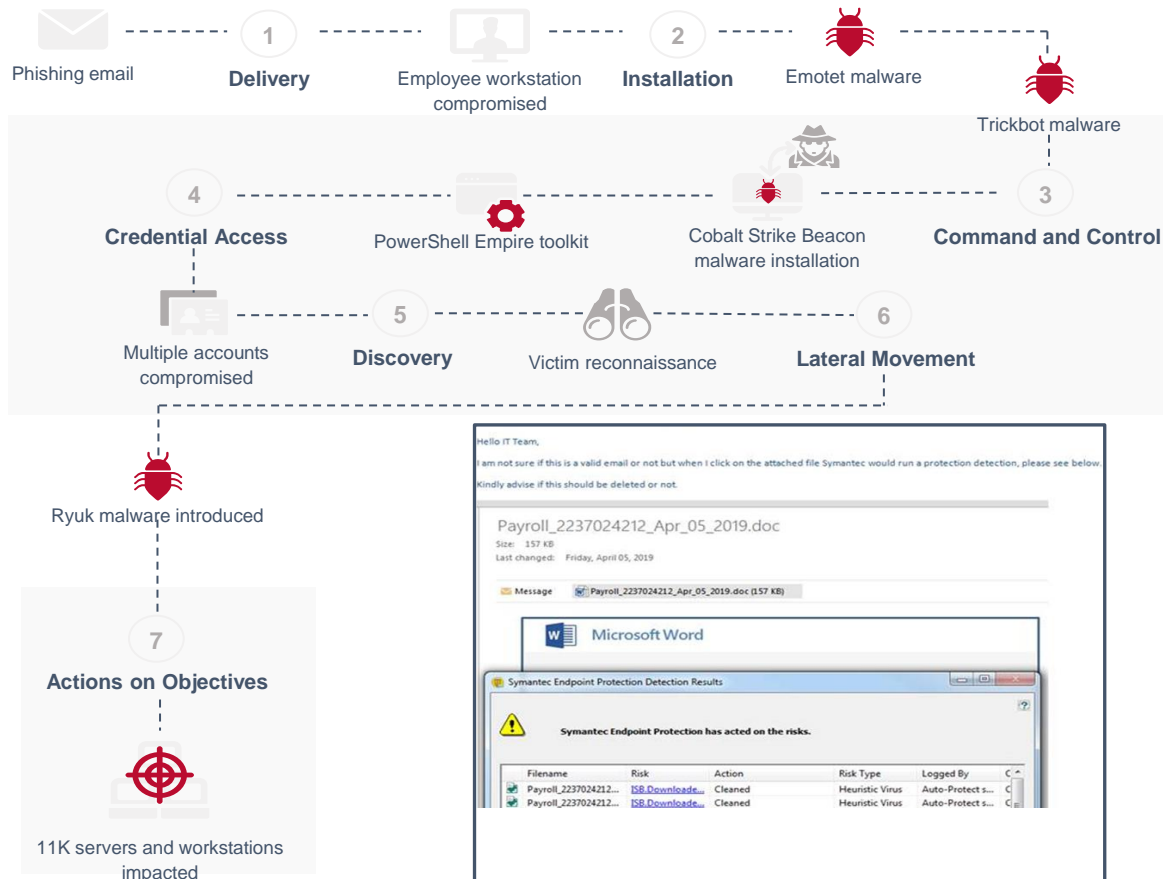
Anatomy of a Ransomware Attack

Attack Stages

1. Delivery
2. Installation
3. Command and Control
4. Credential Access
5. Discovery
6. Lateral Movement
7. Actions on Objectives

Ransomware Tactics

- Today's attacks are a compilation of old and new tactics.
- Impersonation of executive leaders
- System lock out with threats to delete files
- Targeted attacks
- Data theft publicly released



January
10

February - April

April 25

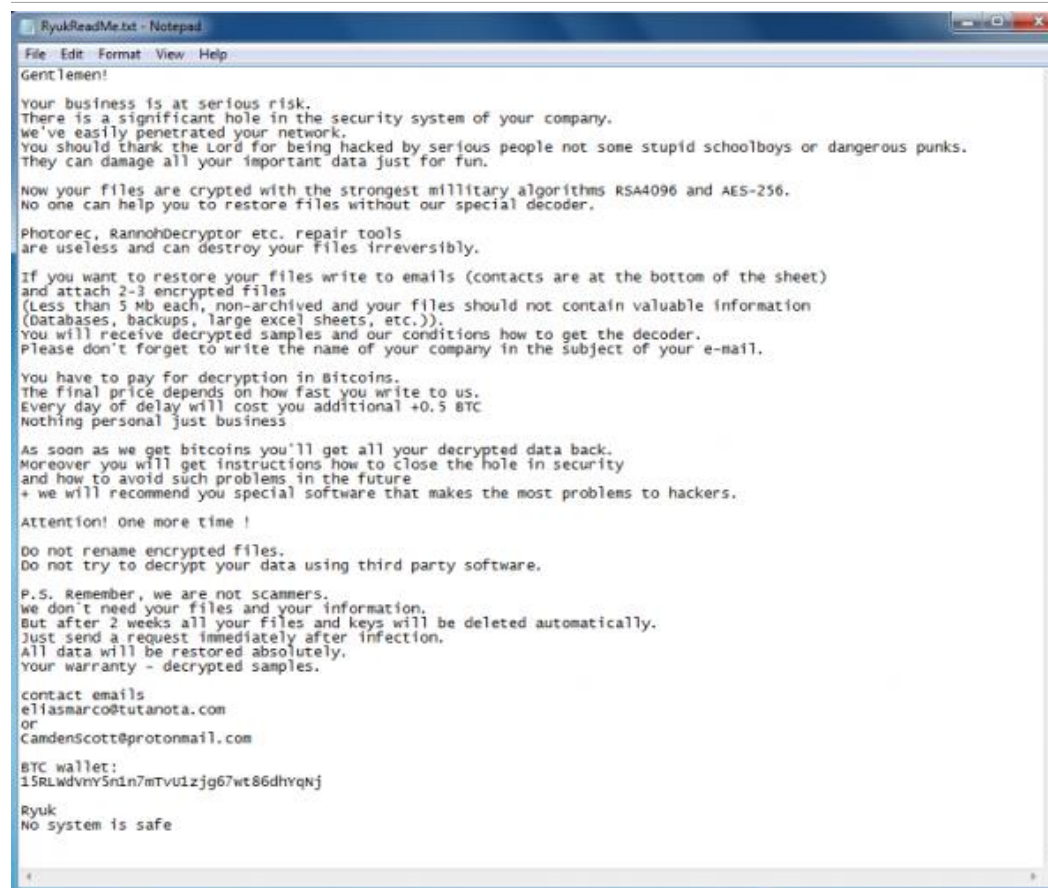
May 11

What Does Ransomware Look Like?

Best Practices

- Practice good cybersecurity hygiene
 - Conduct regular back-ups
 - Segment your network
 - Update and patch systems and software
 - Allow list applications
 - Protect your email
 - Protect your endpoints
 - Prevent end-users from installing new applications
- Test yourself
- Provide and invest in end-user training
- Consider purchasing cyber insurance
- Consider incident response as a service

Ransomware Example



Insuring for the Worst-Case Scenario

Cyber insurance is designed to help an organization mitigate risk exposure, through risk transference, by offsetting costs involved with recovery after a cyber-related security breach

General liability policy vs. cyber insurance

- It provides protection over a general liability policy, which typically only cover bodily injuries and property damage resulting from an organizations' products, services or operations.

Why consider purchasing cyber insurance?

- Most organizations, large or small, do not have the financial resources to bear the risk of a loss due to a cyber attack.
- Organizations have a responsibility to their clients, investors and employees to protect sensitive data, including personally identifiable information, protected health information and proprietary information.
- Failure to provide adequate data protection can result in a loss of competitive advantage, a drop in stock value, regulatory fines, civil litigation, and, in some cases, criminal prosecution.

Costs of a Cyber Attack and What Risks Insurance Can Transfer



How to Protect Yourself

Social engineering is psychologically manipulating people into performing actions or divulging confidential information.

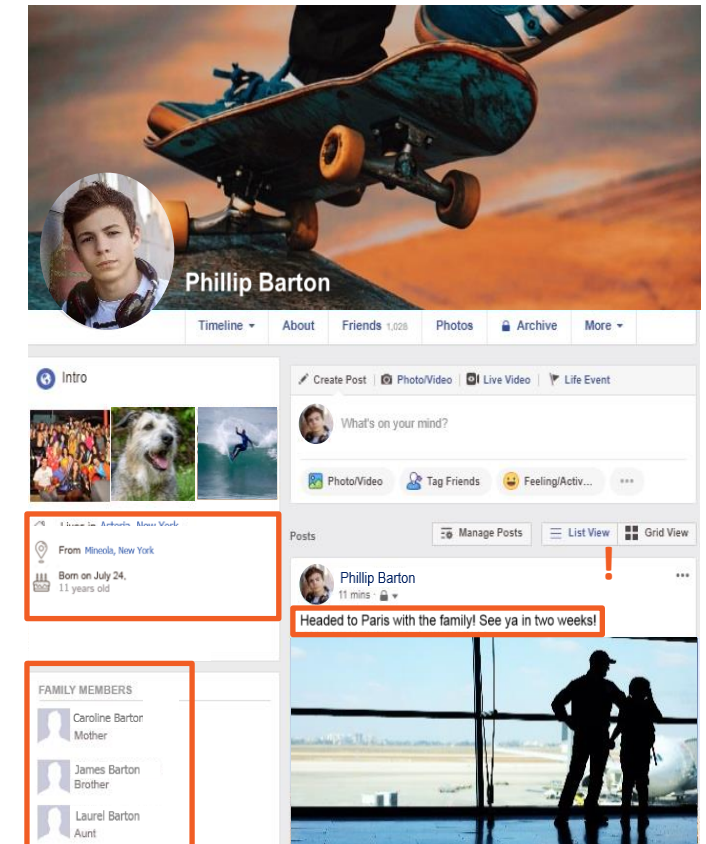
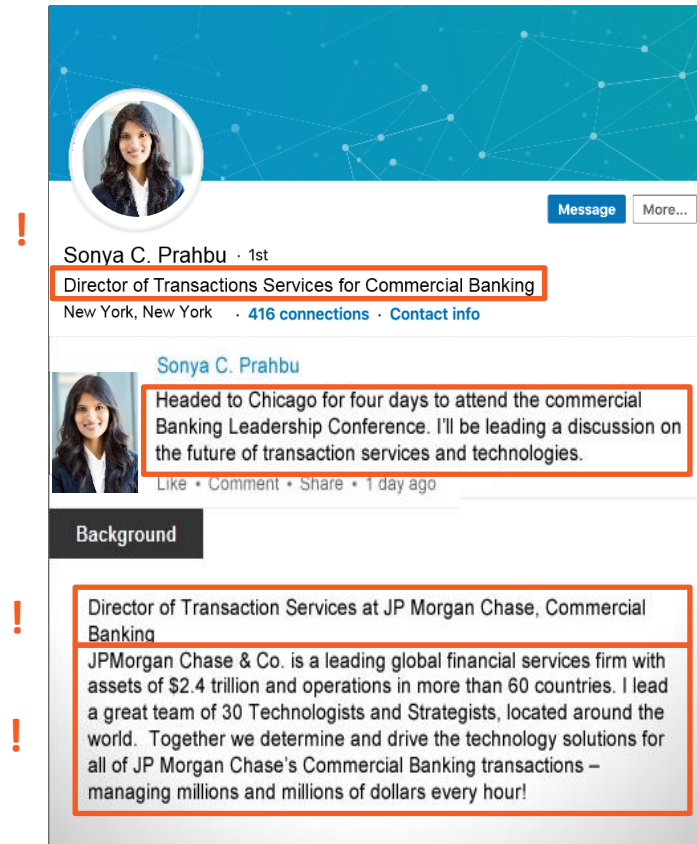
Risks

- Cybercriminals will use the information to initiate unauthorized payments.
- Cybercriminals may use harvested information (login credentials, etc.) to pivot and pursue a variety of other fraud schemes.











Social Media Best Practices

Restrictions on social media in regards to personal information such as:

- Job title / description
- Location
- Travel plans



10 Ways to Protect Yourself and Your Information

1.  Choose a reputable email provider that offers spam filtering and multi-authentication.
2.  Be cautious of clicking on links or attachments sent to you in emails.
3.  Turn off Bluetooth when it's not needed.
4.  Keep screen lock on, choose strong passwords and use biometric tools when available.
5.  Create one network for you, another for guests and children.
6.  Change the default password to your wireless network.
7.  Install and keep up to date anti-virus and ad-blocking software.
8.  Keep software, browser and operating systems up-to-date. (Review the system requirements page: www.chase.com/chaseconnectrequirements)
9.  Download software only from trusted sources.
10.  Never use public Wi-Fi to enter personal credentials on a website.

Best Practices: Payment Security and Controls



USER ACCESS

- Know who has access to your banking relationships and accounts; review entitlements regularly.
- Set payment limits at account and employee level based on payment trends/history (e.g., 12-month history).
- Establish multiple approval levels based on various thresholds (dollar amounts, tenure).
- Ensure robust and multi-level approvals required in areas such as accounts payable.
- Don't have multiple users log in from the same computer to initiate or release payments.
- Use approved templates/verified bank lines and restrict use of free form payments.
- Require multifactor authentication (MFA) to provide additional security beyond usernames and passwords when initiating payments.



RECONCILIATION

- Perform daily reconciliation of all payment activity. Immediate identification and escalation is critical.
- Validate that vendors have received payments on payment date. If volume is an issue, perform sampling or set thresholds such as validating payments over a certain amount, e.g., \$250,000.



VERIFICATION

- Don't move money based solely on an email, text or telephone instructions, even from trusted vendors or company executives.
- Perform validation callbacks in circumstances such as a request for payments, establishing or changing payment instructions or changing contact information.
- Callbacks should be made to the actual person making the request using a phone number retrieved from a system of record.
- Numbers obtained from sources such as email, pop-up messages, texts or voicemail should not be used for validation.
- Always validate the sender's email address by clicking reply and carefully examining the characters in the email address to ensure they match the exact spelling of the company domain and the spelling of the individual's name.
- Never give any information to an unexpected or unknown caller.
- Establish with your customers and business partners how changes in account information will be communicated and validated. Confirm how you expect them to validate changes to your banking information.
- Have a process to respond to your financial institution when they call about suspicious payments. Ensure that your payment controls processes were followed correctly.

Best Practices: Payment Security and Controls



ANOMALOUS PAYMENTS

- Establish a process to Identify and validate irregularities (first time beneficiaries, cross-border payments).
- Verify payment values and velocities.
- Establish criteria to verify or release payments.
- Track and trace where a payment is in the environment point-to-point and if altered at any time.



TRAINING AND EDUCATION

- Conduct periodic cybersecurity/fraud training and testing for employees.
- Teach employees how to identify and report suspicious emails, especially ones that relate to payment transactions.



RESPONSE

- Develop a fraud response plan before an incident occurs.

How Can Your Bank Help?

- Receivables Products

- Virtual Reference Numbers
- ACH Transaction Review/ACH Blocks

- Payables Products

- Positive Pay w/ Payee Name Verification
- Post No Checks
- Virtual Cards

- Thought Leadership and Advice

QUESTIONS?

Disclaimer

- Chase, J.P. Morgan, and JPMorgan Chase are marketing names for certain businesses of JPMorgan Chase & Co. and its affiliates and subsidiaries worldwide (collectively, “JPMC”, “We”, “Our” or “Us”, as the context may require).
- We prepared these materials for discussion purposes only and for your (“The Company”) sole and exclusive benefit. This information is confidential and proprietary to our firm and may only be used by you to evaluate the products and services described here. You may not copy, publish, disclose or use this information for any other purpose unless you receive our express authorization.
- These materials do not represent an offer or commitment to provide any product or service. [In preparing the information, we have relied upon, without independently verifying, the accuracy and completeness of publicly available information or information that you have provided to us. Our opinions, analyses and estimates included here reflect prevailing conditions and our views as of this date. These factors could change, and you should consider this information to be indicative, preliminary and for illustrative purposes only. This Information is provided as general market and/or economic commentary. It in no way constitutes research and should not be treated as such.
- The information is not advice on legal, tax, investment, accounting, regulatory, technology or other matters. You should always consult your own financial, legal, tax, accounting, or similar advisors before entering into any agreement for our products or services. In no event shall JPMC or any of its directors, officers, employees or agents be liable for any use of, for any decision made or action taken in reliance upon or for any inaccuracies or errors in, or omissions from, the information in this material. The Company is responsible for determining how to best protect itself against cyber threats and for selecting the cybersecurity best practices that are most appropriate to its needs. JPMC assumes no responsibility or liability whatsoever to any person in respect of such matters, and nothing within this document shall amend or override the terms and conditions in the agreement(s) between JPMC and the Company.
- The information does not include all applicable terms or issues and is not intended as an offer or solicitation for the purchase or sale of any product or service. Our products and services are subject to applicable laws and regulations, as well as our service terms and policies. Not all products and services are available in all geographic areas or to all customers. In addition, eligibility for particular products and services is subject to satisfaction of applicable legal, tax, risk, credit and other due diligence, JPMC’s “know your customer,” anti-money laundering, anti-terrorism and other policies and procedures.
- Products and services may be provided by Commercial Banking affiliates, securities affiliates or other JPMC affiliates or entities. In particular, securities brokerage services other than those that can be provided by Commercial Banking affiliates will be provided by appropriate registered broker/dealer affiliates, including J.P. Morgan Securities LLC and J.P. Morgan Institutional Investments Inc. Any securities provided or otherwise administered by such brokerage services are not deposits or other obligations of, and are not guaranteed by, any Commercial Banking affiliate and are not insured by the Federal Deposit Insurance Corporation.
- JPMorgan Chase Bank, N.A. Member FDIC.
- © 2021 JPMorgan Chase & Co. All rights reserved.