Global Security & Investigations

Cyber Awareness Training

J.P.Morgan

Financial Crime

Angel Cruz

Assistant Vice President, Global Security & Investigations

J.P.Morgan

GLOBAL SECURITY & INVESTIGATIONS
INVESTIGATIVE SERVICES DIVISION

Fraud, Identify Theft, and your J.P. Morgan Accounts

- Electronic Crimes Investigations:
  - Our primary mission is to protect you (the client) and J.P. Morgan.
  - This group's focus is almost totally on external fraud.
  - From October 2013 to August 2015, Business Email Compromise (BEC) scam continues to grow and evolve and it targets businesses of all sizes. There were 8,179 victims and over $798 million in exposed dollar loss relating to BEC reported to the Internet Crime Complaint Center.
  - We advise J.P. Morgan business units on designing and implementing effective countermeasures in order to mitigate the risk of the client becoming victims of electronic fraud.

FRAUD, IDENTIFY THEFT, AND YOUR J.P. MORGAN ACCOUNTS

"You know, you can do this just as easily online."

Courtesy: *The New Yorker*

Trends

Five years ago:

75% of our investigations were related to social engineering.

- Mail theft
- Layered Pretext Calling
- Dumpster diving
- Almost entirely mass market customers: Low dollar, high volume.

Today:

75% of cases can be traced to some form of Malware (Malicious Software).

- Skimming and Merchant Breaches
- Compromised home computers, laptops, tablets, and smart phones
- Compromised client email accounts
- All customer markets are affected, even Corporate Banking.

The Fraudsters:

They are professionals; frequently tied to organized crime groups operating both here and abroad.

They are constantly adapting:

- They have two advantages over the industry:
  - They are always "on offense."
  - They can introduce change much faster than we can.

Attacks are most commonly directed at you, the customer; not directly toward financial institutions.

Why The Trend to Malware?

- The Internet offers invisibility and anonymity to credential theft.
- It makes large-scale credential theft a reality.
- The malware is readily available for purchase.
- No coding skills necessary.
- Easily customized by non-technical criminals to perform specific functions or attack specific victims.
- Modern malware is resistant to anti-virus software detection.
- Increasingly sophisticated reduce effectiveness of advanced identification and authentication controls like hardware tokens.
- With access to accounts, they use “Money Mules” to move the funds; making this a virtually risk-free enterprise for the masterminds.

Current Malware Threats

Dyre Malware

- Computers are infected through email attachments.
- Monitors for users entering any one of over 200 financial institution URLs.
- Once the URL is entered, the malware is activated and notifies the fraudster.
- Dyre can record keystrokes and gives the fraudster "remote desktop" access to the infected machine. They see every mouse movement, every ID and password, etc.
- The fraudster can push customized pop-up screens to the infected computer, asking for more information or just to buy time while they're entering transactions in the background.
- The fraudster may instruct you to have a second user log in on this computer or they may even call you, pretending to be "J.P. Morgan Tech Support" to persuade you to do this. This is a **RED FLAG**.

Current Malware Threats

Email Spoofing

- Will appear to be from a trusted source:
  - Your CEO/CFO
  - A known vendor/supplier
- New or altered wire instructions
- New or altered invoice payment accounts
- The messages will commonly share two characteristics:
  - The request is urgent and time sensitive: It must be done now!
  - The sender cannot be reached until later.
  - These are **RED FLAGS**. Consider verification before proceeding.

What JPMorgan is doing to counter the threats:

Global Two-Way Intra-Firm Communication

- We communicate new and evolving fraud trends with our technology, risk, and operational units around the world daily.

Constantly Refining and Adjusting Procedures

- Exchange of information between our business units
- Maintaining the balance of protection and ease of access

Robust Cybersecurity, Audit, and Investigative Resources

- Electronic Crimes Investigations: Technical investigations capabilities across all businesses.
- Cybersecurity: intelligence, infrastructure protection, and technical resources.

Close Working Relationships with Law Enforcement & US/Int'l Industry Peers

Protecting Your Computers

Limit network access to the computers you use for funds transfers:

Network Segmentation

- Use firewalls to restrict inbound/outbound traffic to only those protocols and services required for identified business functions.
- Outbound traffic limited to identified business partners.
- Physically or logically segmented networks to isolate computers used for funds management from the rest of the company's network.

Employ the concept of "least privilege"

- Avoid use of accounts with Administrator privileges.

Limited-use computers

- Financial Institution transactions only
- No email accounts on these computers
- Run only processes and services required for the business function
- Local restrictions to limit what websites can be visited

Protecting Your Computers

Today, most malware is delivered by email. Therefore:

- Don't open emails from unknown sources.
- Be suspicious of emails from people you know that seem out of character.
- Never open email attachments you weren't expecting to receive, even from people you know.
- Never click on the web links in emails you weren't expecting to receive.
- Avoid web-based mail accounts for sensitive activities.
- Use the junk mail filters available in your mail program.
- Encrypt sensitive information!

Questions?