ISE® North America Executive Forum and Awards 2012

JP Morgan Chase
Trusted Email Registry
Mark Risoldi
Managing Director, Data Protection
J.P. Morgan

- JPMorgan Chase (NYSE: JPM) is one of the oldest financial institutions in the United States. With a history dating back over 200 years, here's where we stand today:
- We are a leading global financial services firm with assets of $2.3 trillion.
- We operate in more than 60 countries.
- We have more than 240,000 employees.
- We serve millions of consumers, small businesses and many of the world's most prominent corporate, institutional and government clients.
- We are a leader in investment banking, financial services for consumers, small business and commercial banking, financial transaction processing, asset management and private equity.
- Our stock is a component of the Dow Jones Industrial Average.
Presentation/Project Overview

• Business Case for the Trusted Email Registry
• Implementation Approach
• Lessons Learned
• Results
• JPMorgan Chase sends 4 billion emails per year to its customers
• 600,000,000 emails are sent annually to JPMC customers that are **FRAUDULENT** and not from JPMC domains
  • 15% of emails going to JPMC customers are fraudulent and potentially malicious resulting in:
    • Customer fraud
    • Brand erosion
    • Dilution of legitimate email effectiveness and the corresponding loss in sales/service opportunities

One of over 100 Million JPMC Exact-Domain Match Phish Messages Delivered per Year at Google and Yahoo alone!

Each Message Purports to be From a JPMC Domain
Many are phishing emails...
> $3M cost per attack to brand-owner
> 2000 brands phished per year
57,000 phish websites per week

Gartner Survey Shows Phishing Attacks Escalated in 2007;
More than $3 Billion Lost to These Attacks

Debit cards emerged as the financial instrument targeted most by fraudsters.

STANFORD, Conn., December 17, 2007—Phishing attacks in the United States soared in 2007 as $3.2 billion was lost to these attacks, according to Gartner, Inc. The survey found that 3.6 million adults lost nine months ending in August 2007, as compared with the

Gartner Says Number of Phishing Attacks on U.S. Consumers
Increased 40 Percent in 2008

Fraudsters focus on higher-volume and lower-value phishing attacks.

STANFORD, Conn., April 14, 2009—

More than 5 million U.S. consumers lost money to phishing attacks in the 12 months ending in September 2008, a 39.8 percent increase over the number of victims a year earlier, according to Gartner, Inc.

700% Increase In Phishing Attacks In 4 Years
Consumers are Losing Confidence

Figure 2. Security Concerns Have Affected Behaviors

- 58.7
- 58.5
-
The Email Ecosystem

- ESPs
- 3rd Party Senders
- MTA Providers
- Campaign Mangmt.
- List Acquisition
- Open Source
- Cloud Service Providers
- Mail Campaigns
- Data Intelligence
- Authentication Controls
- Threat Protection
- ISPs
- Internet

ISE® North America Executive Forum and Awards 2012
Implementation

1. Implement Sender Policy Framework (SPF) and Domain Keys Identified Mail (DKIM)

J.P. Morgan
CHASE

JPMC Registered Domains
Chase.com
Jpmchase.com

3rd Party Domains
Epsilon.com
Emailsender.com

2. Enable email Intelligence
- Implement email authentication monitoring
- Identify 3rd party mailers
- Integrate Malicious URL Takedown
- Implement domain monitoring & alerting

3. Apply Controls to 3rd Party Management Practices
- Document 3rd Party E-Mail Requirements
- Implement through TPO
- Obtain Listing of Delegated sub-domains from DNS
- Deliver email authentication FAQs
- Enforce DMARC for 3rd parties

4. Communicate to Internal Marketing teams

5. Enforce Policies with ISPs
- Notify ISPs on which domains to block mail from
- Enforce policies for exact domains and defensive domains through domain management
Industry Standard

DMARC from Author to Recipient

Author Composes & Sends Email

Sending Mail Server Inserts DKIM Header

Email Sent to Receiver

Standard Validation Tests

Retrieve Verified DKIM Domains

Validate and Apply Sender DMARC Policy

Retrieve "Envelope From" via SPF

Apply Appropriate DMARC Policy

ID Blocklists, Reputation, Rate Limits, etc.

Anti-Spam Filters, etc.

Standard Processing

Passed

Quarantine

Failure Report sent to Sender

Update the periodic Aggregate Report to be sent to Sender
Implementation Status

<table>
<thead>
<tr>
<th>May 2011 – August 2012</th>
<th>Legitimate Messages</th>
<th>Malicious Attempted</th>
<th>Malicious URLs Submitted for Takedown</th>
</tr>
</thead>
<tbody>
<tr>
<td>Messages Purporting to be one of JPMCs domains @ Gmail, Yahoo!, AT&amp;T, British Telecom and Rogers Communications</td>
<td>1.212 Billion</td>
<td>194 Million</td>
<td>1.25 Million</td>
</tr>
</tbody>
</table>


1. Identification of fraudulent email
2. Implementation of DMARC standard
3. Policy enforcement with ISPs
Lessons Learned/Best Practices

• Implementation requires a cross-functional program

• Means changes in vendor management practices

• This can provide a compelling story for customers