J.P.Morgan

Payments Security During Uncertain Times

Due to the global outbreak of the most recent coronavirus (COVID-19), many organizations have directed their workforce to engage in social distancing measures to limit the spread of the virus and protect the overall health and safety of employees. This **decreased face-to-face interaction** has led organizations to adopt increased email, phone, and other less personal forms of communication to effectively maintain business. This change in operating model has **increased risk**, particularly from payments-related fraud and cyber-attacks, where malicious actors seek to take advantage of the uncertain situation by targeting organizations through social engineering attacks and other fraud-related activities.

What types of threats should organizations anticipate?

As organizations continue to implement workforce contingency strategies, including Work From Home (WFH) and split working arrangements, malicious actors have **increased phishing (email), vishing (phone), and SMShing (text message)-related social engineering** due to the perception that companies are operating under reduced security postures. A recent uptick in registration of COVID-19 related fake web domains highlights a growing interest by these bad actors to leverage the global situation to lure targets into divulging sensitive information or clicking on email links and attachments that can expose their systems to compromise.

Additionally, adversaries may look to **abuse an organization's own brand** to target employees or customers – tricking them into making payments to fraudulent accounts or providing sensitive payment information that can be later used to commit fraud. As more employees shift to remote working arrangements, adversaries have shown increased interest in gathering specific information about an organization's remote working plans and capabilities – such as the percentage or type of employees that may be teleworking and how the organization is conducting business continuity. With increased knowledge regarding an organization's infrastructure and operations, attackers can use this information to launch more targeted attacks in the future.

How can organizations remain vigilant?

Organizations must exercise a **heightened sense of awareness** during this time and ensure all employees, particularly those serving in accounts payable and treasury services roles, are **reminded** of the key actions they can take to prevent payment fraud.

Phishing Awareness

- Do not take action before you've verified the email sender & checked for signs of phishing
- Never forward suspicious emails to colleagues or managers – always report directly to your IT department
- Be mindful of COVID-19 related themes, such as emails purportedly from authoritative academic or governmental

Vishing Awareness

- Always verify caller identity
- Do not provide information to unknown callers
- When in doubt simply hang-up or call the individual back using a known phone number
- Ensure the process to report vishing attempts is widely socialized among all staff
- If an email requests a "call back" to validate a payment, only call the number on file

Fraud Awareness

- Be mindful of:
- Fraudsters who may impersonate members of your organization, senior executives, or key vendors
- "Lookalike" email addresses that closely resemble legitimate senders
- Urgent requests requiring changes to account or routing information or to facilitate an urgent payment

What key measures can help reduce risk?

Organizations should consider implementing a set of security measures to help reduce the risk of payments fraud. These measures include setting payment limits at the account and employee level as well as creating approval hierarchies and dual-approval requirements for releasing payments or changing payment instructions. Additionally, implementing heightened monitoring of payments activity can spot anomalies outside normal patterns that may indicate fraud. Monitoring should also include brand protection measures that alert your organization to newly registered "lookalike" domains, enabling takedown of those domains so attackers cannot leverage them to increase the effectiveness of their attacks. Lastly, conducting an end-of-day payments reconciliation process to verify your organization's payments records can improve your chances of detecting fraud and recovering lost funds in a timely manner.

How can J.P. Morgan help?

JPMC offers resources such as Positive Pay and Reverse Positive Pay to help your organization combat fraudulent activity. **Positive Pay** allows JPMC to review checks submitted to your account. If any appear to be fraudulent, we alert you so you can determine whether they should be paid or returned. **Reverse Positive Pay** allows you to monitor checks and then tell us whether to pay or reject any checks. Additionally, capabilities such as ACH Debit Blocking and ACH Transaction Review help your organization avoid the risk of fraudulent, inaccurate, or untracked automated clearing house (ACH) transactions.

Most importantly, if you suspect that you have been a victim of fraud, please **contact your JPMC representative immediately**.