VOLUME 5 | FALL 2018

Cybersecurity:

Resiliency and Recovery

Raising Cyber Awareness

Learn how interactive exercises help clients develop and reinforce cybersecurity preparedness plans

Protecting the Sector

A financial services industry group develops a register of potential systemic risks and works with the firm to test the scenarios and build resiliency plans

On the Grid

Read how a “threat grid” helps profile cybercriminals and monitor cybersecurity threats

CHASE

J.P.Morgan

Promoting Resiliency and Recovery

What keeps Jamie Dimon up at night? "Cyber. Cyber. Cyber. Cyber. It is a national risk," said Dimon, Chairman and CEO of JPMorgan Chase & Co., in a recent interview with CNN. "We spend a lot of money and we are very protected, but . . . there's a lot to be done by government and by business to protect itself against cyber."

October marks National Cyber Security Awareness Month, a time for companies to take a more active role in strengthening their processes and controls to guard against a cyberattack. Even though many small businesses and large organizations continue to believe that a cyberattack is unlikely, increasingly companies are strengthening their resiliency plans to recover as quickly as possible after an attack.

According to the FBI's 2017 Internet Crime Report, the agency's Internet Crime Complaint Center (IC3) received more than 300,000 complaints of cyberschemes with reported losses exceeding $1.4 billion. Business email compromise ranked among the top three cybercrimes last year with adjusted losses of more than $675 million, the highest reported losses overall according to the IC3.

In this issue, we'll discuss how developing a comprehensive cybersecurity preparedness plan for your organization is vital to protecting financial information, client accounts, and the personal data of your clients and employees. While cybersecurity education and training are critical steps, it's also important to test resiliency and recovery plans by engaging employees in cyberattack scenarios. Our Exercises and Social Engineering team is working with clients and industry groups to build cybersecurity awareness.

We'll explain how the Financial Systemic Analysis & Resilience Center—a public-private initiative that was created two years ago by a group that included JPMorgan Chase & Co.—has created a register of cybersecurity risks that could threaten the US financial system. The collaboration between financial institutions and government partners shares intelligence and response plans if a threat emerges against one firm or the entire financial sector.

We'll talk with Amy Chang, from our corporate Cybersecurity team, about the importance of a "threat grid" to evaluate and prepare for a variety of cybersecurity schemes—ranging from attacks by nation-states to criminals trying to steal money and activists who launch attacks for political purposes.

> "Cyber. Cyber. Cyber. Cyber. It is a national risk."

You'll read how Elaine Escobar, one of our client service senior associates, relentlessly questioned what turned out to be a fake wire transfer request and stopped a client from suffering a $3 million loss. You'll see how criminals are using invoice fraud or "vishing" schemes, which use phone calls or automated phone services, to trick people into providing confidential information.

Complacency remains the biggest challenge in the battle against cyberschemes, but developing and testing strong resiliency and recovery plans will be significant in minimizing the damage criminals create. ■

Helping FSARC Identify Potential Threats to Combat Cybercriminals

The message from a leading industry group to financial services and government partners regarding cyberattacks is straightforward: Be prepared to be targeted and have a recovery plan in place.

To help identify potential risks and threats that could affect financial systems, the Financial Systemic Analysis & Resilience Center (FSARC)—created two years ago by a consortium of financial services firms including JPMorgan Chase—has developed a confidential register of nearly two dozen cyber scenarios. These scenarios reflect threats to technology and operations that could threaten one financial institution, but have the potential to cascade through the entire sector.

"By developing a risk register, we can prioritize the systemic risks and build actionable steps to promote the resiliency of the financial sector against these threats," said Russell Fitzgibbons, Corporate & Investment Bank (CIB) Operations, who works closely with FSARC as their Director of Risk. "When we identify a critical potential event, we look at the interconnected assets, networks and systems to develop plans to provide a path to recovery."

The risk register is maintained and administered by the FSARC. Input and support is provided by the FSARC Risk Committee, which is led by FSARC and the US Treasury, with its committee members representing the 16 financial institutions. Rohan Amin, the firm's Chief Information Security Officer and Chief Technology Control Officer, serves as chairman of the FSARC board. FSARC and its members spend approximately six months identifying and analyzing strategies for addressing each scenario, Fitzgibbons said. That analysis drives the development of comprehensive playbooks that address operational, technology, legal and compliance, and customer strategy components.

The initiatives rely heavily on collaboration among its members and other financial sector participants, with engagement and input from more than 100 industry and cyber experts to create resiliency and recovery plans to help mitigate a broad cyberattack. Our Exercises and Social Engineering (ESE) team conducts exercises with FSARC members, financial market utilities and government partners to test the viability of the plans and solutions, and share key learnings. The ESE team has conducted two resiliency exercises with FSARC examining possible disruptions to the wholesale payments system and US Treasury bond markets. The group is planning a third exercise focusing on global messaging systems in early 2019.

"Developing any resiliency and recovery plan is only as good as testing its execution," said Adam Bulava, Global Head, ESE team. "These types of exercises allow the financial sector and government agencies to collaborate on planning and to validate the effectiveness of recovery and resiliency playbooks."

Last fall, the ESE team led the first cyber exercise based on the committee's Wholesale Payments Initiative (WPI) to examine the plan's viability for a systemic threat on the high-value payments processing system.

The day-long, web-based tabletop exercise tested a simulated multiday outage at a large wholesale payments bank controlled

by cybercriminals, looking at the effects on that one firm, as well as the broader market implications.

More than 300 participants from nine financial institutions, two financial market utilities and several government observers took part in the WPI scenario testing, including representatives from payment operations and technology, business continuity, client service, legal, communications and treasury/liquidity.

Each organization participated from its respective offices around the country, identifying and responding to over 120 unique exercise prompts that used real-world artifacts, such as payment messages, industry intelligence bulletins, news reports, and adversary social media posts. Participants received an exercise phonebook that included contact information to encourage internal discussions, crisis coordination calls and bilateral communications among the members.

Following the simulation, the ESE team shared the key outcomes with the FSARC WPI steering committee to determine next steps for enhancing resiliency and response planning.

"The WPI exercise was a valuable tool for FSARC and participants," Fitzgibbons said. "This was the first validation of an FSARC initiative that stress tested the maturing WPI playbook, its utility within the participating firms and its connectivity to other sector playbooks and processes. The testing also provided the various business, technology, operations and business continuity areas within each firm an enhanced perspective on how to improve coordination and communications during a cyber event. Every role counts."

Successfully combating cyberschemes "isn't just about knowing who the criminals are and how they will attack," said Mike Kelly, Head of Cybersecurity and Technology Controls for Commercial Banking. "It also comes from developing long-term collaborations with other financial institutions and the US government to try to stop the schemes and recover."

A key factor studied by the group is how to coordinate a response if "a sustained event, such as the disruption of wholesale payments systems or the US Treasury bond market, affects one firm or the entire network," said Lester Owens, Global Head of Wholesale Banking Operations and CIB Client Onboarding. "By evaluating the possible scenarios early, we can test controls and help correct any potential gaps now."

While the risk initiatives are building plans to ensure resiliency in the event of an attack, the FSARC Intelligence team and its members are building collaboration capabilities with the Department of Homeland Security, US Treasury and the US intelligence community to better defend prioritized critical infrastructure against an attack.

"Our relationship with other firms and the US government increases awareness about cybersecurity and the need to plan," said Josh Pope, Head of Global Client Service & Implementations and Americas Operations for Treasury Services. "By working together, FSARC and its members identify opportunities to share intelligence and help each other defend against cyberthreats." ■

Engaging Clients Through Cybersecurity Scenario Exercises

Cyberattacks are escalating at record rates, and companies are revising strategies as it becomes apparent the focus has shifted from *whether* an organization will be targeted to *when* it will happen and *what* can be done about it, especially if the attack is successful.

To help clients understand the need for controls, employee training and recovery plans, our Exercises and Social Engineering (ESE) team began conducting a series of tabletop exercises at industry events earlier this year to increase cybersecurity awareness.

"These exercises allow our clients to prepare for high-risk scenarios as well as possible exposure of their information," said Rohan Amin, Chief Information Security Officer and Chief Technology Control Officer for the firm. "The exercise modules identify potential areas of risk and prompt executives to consider various cyber readiness, response and recovery options to protect critical systems."

Some of the proposed scenarios involve data breaches and stealing financial or personal information. Others include denial of service attacks, payments fraud, ransomware, malware and other securities or foreign exchange threats. The exercises are simulated for the audience, but the audience knows that a real attack likely will have long-term consequences. According to the 2018 Association for Financial Professionals (AFP®) Payments Fraud and Control Survey Report, 78 percent of companies surveyed were targets of attempted or actual fraud.

"We leverage these unique cybersecurity exercises as opportunities to encourage clients to adopt tools and controls before an attack," said JF Legault, Global Head of Cybersecurity Operations. "We want to reinforce the need to have resiliency and recovery plans in place to minimize damages and lost time."

The ESE team conducted these exercises at two client forums in the US. The one-hour program allows stakeholders to discuss roles and responsibilities during a cybersecurity disruption. Participants are divided into functional teams to analyze the threat scenario, examine existing systems and controls, and decide if additional processes are needed for resiliency, such as building a response playbook. The program focuses on business, technology and cybersecurity, and also includes representatives from other areas, including business resiliency, legal, compliance, risk and communications to simulate a realistic response.

"Employees across many departments can be impacted by a cyberattack and need to know how to establish recovery plans in their areas," said Adam Bulava, Global Head, Exercises and Social Engineering team. "Through these exercises, clients learn how and when to respond to the media, regulators, and answer client requests for information. We also remind them to consider engaging law enforcement and cyber insurance providers following a cybersecurity disruption to help mitigate impacts."

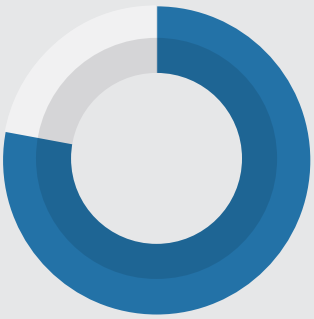
During the exercises, participants discuss approaches and strategies for addressing the simulated incident, and answer a series of instant polling questions—the results of which are shared with the clients. The outcomes have guided improvements within organizations, such as improving incident response times and developing a wider range of cybersecurity training protocols for employees.

"The exercises reinforce the need for companies to identify potential gaps in technology and business controls, and to assess the overall readiness of a company's ability to respond to a cyberattack," said Anish Bhimani, Commercial Banking's Chief Information Officer.

The ESE team plans to continue its expansion of the client exercise program into 2019. ■

RESILIENCY | **RECOVERY**

Education, testing and basic systems hygiene help prevent criminals from accessing your data—but what do you do when your company falls victim to a cyberscheme?



78% of companies surveyed were targets of a wide range of payments fraud

Source: 2018 Association for Financial Professionals Payments Fraud and Control Survey Report

Did you know?

Clients who notify the firm within "The Golden Hour" after an attack have a better chance of recovering stolen funds before the transaction moves between countries and people.

Report and Escalate

If an online session makes you uncomfortable, especially at login, discontinue the session and call us immediately.

If you've been targeted by a fraud scheme, become suspicious after sending a wire transfer or your login credentials have been compromised, contact your relationship team or call your Help Desk:

- J.P. Morgan Access® (866) 872-3321
- Chase Connect℠ (877) 226-0071 [government entities and not-for-profit organizations call (855) 893-2223]

Audit Systems

Perform a complete security audit of your systems and fill any gaps.

- Have robust systems and procedures in place for backing up files.
- Ensure anti-virus software is current and update and patch your computers and devices.
- Check security and firewall protection on all company computers and laptops.
- Check that vendors and suppliers follow strict cybersecurity standards.
- Review your arsenal of cybersecurity tools. Authentication tools are critical in fighting cybersecurity schemes.

Educate and Test

Training is an effective tool that equips employees to spot—and stop—fraud schemes before a loss occurs.

- Conduct cybersecurity training and tests to enable employees to detect phishing emails or other cyberschemes.
- Require strong passwords with special characters, symbols and upper and lowercase letters.
- Create a cyber team to test your systems using the same techniques criminals use.
- Run simulations and drills to validate security capabilities.
- Have cybersecurity teams use tabletop exercises and live scenarios to test the processes you use.

Client Service Associate Insists on Validating New Request, Stops $3 Million Fraud Attempt

Elaine Escobar, a Client Service Senior Associate in New York, refused to take "yes" for an answer recently when she received an odd payment request from a client. And her persistence and curiosity helped a client avoid a potential $3 million loss when it became clear the client was the target of a fraud scheme.

Escobar received an email from our banking operations team asking her to validate a $3 million wire transaction to a vendor. Payment instructions had been changed and it was not clear why. As part of the firm's process, Escobar called the client's controller.

"There were a couple of red flags," Escobar said. "Something just didn't feel right. The payment instructions had been changed to a bank outside the US that the client had not sent a payment to before. I decided to hold the payment."

The controller said the request was valid and that the company's chief financial officer (CFO) approved the payment. Escobar was told, please release the payment. She recommended that the controller contact the CFO for verification. Following that advice, the controller sent an email via the client's corporate email system to the CFO and copied Escobar.

Then Escobar reviewed the controller's email she had been copied on, which contained the original payment request from the vendor. She read the email trail and saw that that the vendor's email domain name was misspelled in the initial email address. Escobar replied to the controller and the CFO, asking them to review the spelling on the email domain. She then received several emails from the fake CFO—criminals had taken control of the CFO's email account—demanding that she release the wire. But without a verbal confirmation, Escobar still was not convinced and continued to hold the money.

Five minutes later, Escobar received another email from the real CFO: Do not release. Her telephone rang. It was the genuine CFO calling to say that the wire request and the other emails all were fake. The client had been targeted in a business email compromise scheme.

"Confirming the payment instructions with an established contact at a known telephone number is critical to avoiding fraud schemes," Escobar said. "As we saw here, asking clients to validate by email is not effective because they could be communicating with the criminals at a bogus email address."

> There were a couple of red flags . . . something just didn't feel right.

This case is an "excellent example of why the firm implemented additional validation processes," said John Gambardella, Region Manager, Middle Market Banking & Specialized Industries. "Clients sometimes question why we double-check transactions. But by taking those extra steps, and refusing to act until she was sure it was legitimate, Elaine stopped a significant loss for our very grateful client." ■

Using a Threat Grid to Evaluate Cyberattack Intelligence

Key Terms

Cyber Kill Chain®:

The seven stages of a cyberattack: Reconnaissance, Weaponization, Lure/Delivery, Exploitation, Installation, Command and Control, and Action on Objective.

Threat Actor/Threat Actor Group:

Group to which responsibility for specific cyber incidents/attacks is widely attributed.

Threat Grid:

Assessment and scoring methodology used to profile and rank threat actors/groups.

Threat Group:

Threat actors sharing motivation(s), acting on behalf of the same interest group, or using shared tactics, techniques, and procedures.

Threat Score:

Numerical value assigned to threat actors/groups that is calculated using a formula based on capabilities and intent.

Amy Chang is a Senior Threat Intelligence Analyst for Cybersecurity Operations at the firm. She is responsible for collecting, analyzing and disseminating intelligence related to external threats to the firm. Chang also serves as a liaison to the Financial Systemic Analysis & Resilience Center, where she works closely with top financial institutions, US government partners and the intelligence community to identify and analyze threats to the financial sector.

Previously Chang served as the Staff Director of the Asia and the Pacific Subcommittee for the US House of Representatives Committee on Foreign Affairs. She was responsible for federal oversight and legislation on political, security, and economic issues in the greater Indo-Asia-Pacific region. She is an Affiliate (Non-Resident) with the Belfer Center's Cyber Security Project at the Harvard Kennedy School.

Q: Financial services firms are routinely targeted by cybercriminals. How does the firm assess and prioritize cyberthreats?

A: Our firm operates an internal Threat Intelligence organization that collects, analyzes and disseminates information related to cybersecurity threats to the firm and other institutions. Recently we developed a "threat grid" methodology used to profile and rank what the cybersecurity industry calls "threat actors," "threat actor groups" and "threat groups." These actors and groups are the entities responsible for cyberattacks.

The grid is an important tool because it allows us to rapidly process information, helps us to prioritize threats and enables us to take action to better defend the firm.

Q: What kinds of threat actors and threat actor groups are out there?

A: There are three major categories of threat actors. We call the first Advanced Persistent Threat (APT) groups, which are highly sophisticated actors with extensive funding. They possess significant research and development funding and logistical resources, and they are often sponsored by a nation-state. Typically motivated by nation-state interests, APT groups focus on espionage, surveillance, intellectual property or data theft, and disinformation campaigns.

Cybercriminal groups, a second category, have varying levels of planning and targeting skills. Some are highly organized and possess or are able to access sophisticated tools and technical and engineering skills. Typically they are motivated by financial gain, and their schemes may include ransomware attacks, extortion, credential stealing and various phishing and "vishing" scams.

Hacktivist groups, a third category, often use publicly available tools and scripts

> The grid is an important tool because it allows us to rapidly process information, helps us to prioritize threats and enables us to take action and better defend the firm.

AMY CHANG

VICE PRESIDENT, CYBERSECURITY OPERATIONS, THREAT INTELLIGENCE

developed by others because they do not possess the resources, knowledge or skills to develop or re-engineer tools on their own. They are motivated by ideology and select their targets to achieve a vision of socioeconomic justice, drive a geopolitical or patriotic agenda, discredit authorities or seek attention.

Q: How does the grid and threat-scoring process work?

A: It's a two-step process based on technical capability and intent. We use the grid to create a profile of the threat actor or group, weigh their technical skills and resources against each of the seven stages of the Cyber Kill Chain®, and assign an overall capability score. Next we score their intent based on their key motivations such as financial gain, military and defense goals, or political influence.

Capability scores and intent scores range from one (low) to five (high). We multiply the capability score by the intent score to arrive at the overall threat score. The threat score ranks the threat actor or group and the magnitude of the threat they may pose.

Capability × Intent = Threat Score

For example, if a threat actor scores 4.25 for capability and 3 for intent, their threat score would be 12.75 out of a possible 25 points, which means it's a moderate threat. The higher the score, the greater the threat.

Q: What are the benefits of using a grid methodology?

A: The grid helps us monitor and prioritize cybersecurity threats facing the firm on an ongoing basis. It dynamically informs our cybersecurity program decisions—any significant cyber incident or geopolitical change will trigger a review of the actors involved—imparting effective intelligence.

We can hone in on the actors or groups with the greatest potential to do harm, map the tactics they use and predict how they may employ those tactics against us. This information enables us to bolster our defenses and helps to protect our clients and the firm.

Q: How can clients benefit from the grid concept?

A: Clients benefit from the work that we do to help protect them and the firm. Though we would not expect them to use a threat grid, developing a similar methodology specific to their industry may help organizations assess threats particular to their sector.

It also may reveal gaps in an organization's cybersecurity defenses and allow the organization to adjust and strengthen them in effective ways.

It's important to remember that low-tech solutions like training employees to spot phishing attempts and requiring strong passwords are critically important. ■

Escalating Business Email Compromise Schemes

Cybercriminals are increasing the complexity of business email compromise (BEC) attacks, using the telephone as an additional method to increase the effectiveness of the campaign, the FBI reports.

In a recent announcement, the FBI indicated that companies suffered more than $3.6 billion in fraud losses over the last five years. Much of these losses are the result of BEC attacks.

As organizations implement tighter security, criminals are modifying their own approach after launching a BEC attack by calling potential fraud victims to obtain employee names and contact information, and then attempting to gather additional personal data. For example, criminals are calling company help lines or are using social media engineering to obtain employee information.

The FBI's Cyber Division recommends using these practices to help stop a potential BEC threat or phone scam:

» Provide basic training and advanced education for employees so they are alert for BEC and phishing email attacks, as well as the increased threat from phone reconnaissance.

» Do not provide payment information over the phone.

» Monitor information that is available on the company's recorded phone lines, public-facing websites and social media accounts.

» Increase monitoring of the company's email exchange server for changes in configuration or custom rules for specific accounts.

» Consider adding an "external" banner to any email received from outside the company.

» Verify changes to existing invoices, bank deposit information and contact information by calling a known telephone number, and ensure that employees are trained in verification best practices.

» Validate any email requests for changes in payments or personnel records by telephoning a known contact at a known phone number in the company directory.

» Require two signatures on payment transfers.

» Be suspicious of anyone requesting secrecy or pressuring employees to take action quickly.

» Criminals are highly focused on perfecting new ways of stealing your information and your money. Remember, you and your employees are the first and best line of defense.

How We Can Help

We encourage all clients to complete training and use the security measures we offer. To register for the training, please log on to J.P. Morgan Access® Online℠ and register for the Cyber Fraud & Secure Online Banking Webinar via Support > Education.

Chase Connect℠ clients may complete the online banking and payments security training webinar by visiting chase.com/cybersecurity.

You also may contact the Chase Connect Service Center at (877) 226-0071; government entities and not-for-profit organizations call (855) 893-2223.

Cyberfraud Scenarios

Criminals continue to expand their attacks against companies and organizations as a growing number of firms report being the targets of business email compromise (BEC) schemes. In these sophisticated fraud schemes, criminals pose as executives or known third-party suppliers or vendors who send fraudulent payment instructions to a company's payments employees to induce them to send payments to a bank account controlled by the criminals. Often, criminals use look-alike or forged domains that are very similar to the company's and/or compromise an executive's email account. Companies are implementing best practices and training for employees, and are becoming more aware of these types of threats and the need to help prevent these types of attacks.

Clients who do not use appropriate fraud-prevention tools increase their risk of losses and are liable for all losses incurred for payments originating using any authorized users' security credentials or the credentials of others who have designated transaction authority.

What to Avoid

An attorney emails her client with payment instructions for a pending real estate transaction. A cybercriminal, who already had gained access to the law firm's computer server, sends a follow-up email to the client, appearing to come from the attorney, with new payment instructions. The client, assuming the change is legitimate, does not call the attorney to confirm and instead sends the updated wire instructions to the bank's staff. The staff follows bank protocol, and calls the client back to validate the change in payment instructions. The client confirms again, without verbally confirming the change with the attorney, and authorizes the bank to release the funds. Later, the client realizes the fraud and contacts the bank, and together they work to recover a portion of the funds.

Result: The client bears the loss of the unrecovered funds.

An employee receives a fraudulent email from a criminal posing as a known third-party supplier, with instructions for a payment to be made to a new bank account. The client does not verify the payment instructions with the supplier and sends a significant amount of money to the criminal's account. Too late, the company realizes the mistake and tries to recover the funds.

Result: The client bears the loss.

A criminal launches a BEC scam against a company by impersonating the chief executive officer and sending an email to a payments employee with instructions to send a payment to a new bank account. Without validating the request by calling the CEO at a known telephone number, the employee transfers the money to the criminal's bank account.

Result: The client bears the loss.

Best Practices

A payments employee receives an email from a criminal posing as the chief financial officer at a large company. The email authorizes a wire transfer for a new account in Europe, and the employee verifies the request. By calling the executive to confirm the payment instructions, the employee learns the CFO's email has been compromised and does not release the funds.

Result: No client funds are lost.

A criminal tries to gain access to a large company by sending a fraudulent email impersonating a vice president. A payments employee reviews the email request, which includes an invoice and a W-9 form. The employee does not notice that the executive's email account has been compromised and then releases the payment. Shortly afterward, the employee speaks with the executive about the email, learns that the payment instructions were fake, and contacts the bank's client service professional. By quickly reporting the incident, the company is able to stop the payment.

Result: No client funds are lost.

A criminal sends a wire request to an employee asking for a payment to a new bank account. Carefully reviewing the sender's email address, the employee notices the domain looks very similar to—but is not—their company's domain name and realizes that the request is fraudulent.

Result: No client funds are lost. ■

We have a broad range of current articles and videos about cybersecurity and how to help protect your firm on our Insights website at jpmorgan.com/pages/insights.

Contact your relationship manager if you have questions or need assistance.

Cybersecurity Awareness: Combat Vishing

"Vishing," which is a combination of "voice" and "phishing," is a form of social engineering in which criminals use phone calls or automated phone services to lure an employee into providing sensitive or personal information. Often, they impersonate third-party vendors, payments employees or executives at a company in an attempt to gain the employee's trust.

Criminals often use a variety of questions and approaches to obtain personal information that will help them gain access to a company's financial accounts and transfer funds to a bank account that they control.

Potential 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 the 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 impersonate another employee or executive asking for help. Always validate these types of requests by calling the employee or executive at a known telephone number.

Criminals may use these vishing approaches to persuade an employee to provide confidential information:

» "You need to make a transfer to a safe account."
» "We've detected fraud on your account."
» "I'm a police officer."
» "I'm one of your suppliers."
» "Please confirm your online banking code."
» "I'll need your card details."
» "Your payment hasn't gone through."
» "Tap your Personal Identification Number (PIN) into the phone."
» "Just for security reasons . . ."
» "Please confirm your account password."
» "I'm calling from your bank."
» "Your payment is overdue."

What to Do.

Verify and validate an unknown caller's identity at a known telephone number before revealing any sensitive information about the company or employees.

If a caller claims to be a client, third-party vendor or regulator, ask for a telephone number and say you will call back. Then verify the number is correct before calling back.

Validate any change in payment requests or instructions including the use of a new bank account number with a known contact before processing.

Block the caller's number and notify the company's IT or cyber controls department of the vishing attempt. ■

Cybersecurity Awareness: Invoice Fraud

Criminals frequently use invoice fraud to target companies using third-party suppliers and vendors as a way to redirect payments to fraudulent bank accounts and steal funds.

What to remember.

Establish a designated point of contact with a third-party supplier. That contact will coordinate regular payments with the company and will answer any questions about invoices.

» Implement a dual approval or multistep validation and verification process.

» Verbally confirm banking details before initiating payments. Inform the supplier after an invoice has been paid and request confirmation of payment.

Direct employees responsible for processing payments to remain vigilant and watch for changes to payment instructions, particularly banking details, as well as invoiced amounts or a sense of urgency from the sender.

» Verify all changes to outstanding payment instructions by implementing a callback process using a known telephone number.

» Be vigilant in checking for spoofed emails that appear to be sent from a known source. Criminals may create a fake look-alike email domain to pose as a trusted sender, e.g., @**deanco**LLC.com can appear similar to a known vendor @**cleanco**LLC.com.

» Check bank statements carefully. Report all suspicious debits to us immediately.

Protect your personal and business information.

Cybercriminals often conduct extensive online and offline research to identify vendors and third parties with whom you work.

» Remove extraneous information from the company's website, social media channels and other publicly available materials.

» Be prudent in what employees share about roles and responsibilities via social media.

» Never leave sensitive materials such as invoices, account information and client data unattended.

We can help.

If you believe you may have been a victim of invoice fraud, contact us immediately. ■