SOCIAL ENGINEERING FRAUD

LOSS PREVENTION & CONTROL GUIDELINES

LowersRiskGroup®

Protecting People, Brands, and Profits

Risk Mitigation White Paper Series

SOCIAL ENGINEERING FUNDAMENTALS AND METHODS OF FRAUD

In the context of information security, human-based Social Engineering, otherwise known as "human hacking" is defined as the art of influencing people to disclose information and to get them to act inappropriately.

Some criminals consider it much easier to abuse a person's trust than to use technical means to hack into a secured computer system, mostly because they have learned how to trick their targets into giving them information by exploiting certain qualities in human nature. To do this, they use various forms of communication such as email, the Internet, the telephone, and even face-to-face interactions, to perpetrate their scheme of defrauding and infiltrating companies. Social Engineering attacks can take many forms such as being both human and computer-based; however, security experts have recognized that most scams follow a four-stage method: Information Gathering, Relationship Development, Exploitation, then Execution.

This methodology, along with the tendency for humans to be the "weakest link" in the security chain, creates a vulnerability that can have a serious operational impact. Since Social Engineering is such a real threat in today's workplace, it becomes essential for employees across an entire organization to be educated and trained on how to detect and prevent this type of fraud. There is also a need for companies to develop and implement specific policies (i.e. employee understanding of confidential and sensitive information and how to keep it safe) to prevent and respond to an attack. Companies must be cautious not to focus their efforts and security budgets entirely on defending against technical attacks from hackers and other electronic threats, thereby underestimating, or even entirely overlooking, the weakness posed by the human element.

MOST SCAMS FOLLOW A FOUR-STAGE METHOD:

INFORMATION GATHERING

RELATIONSHIP DEVELOPMENT

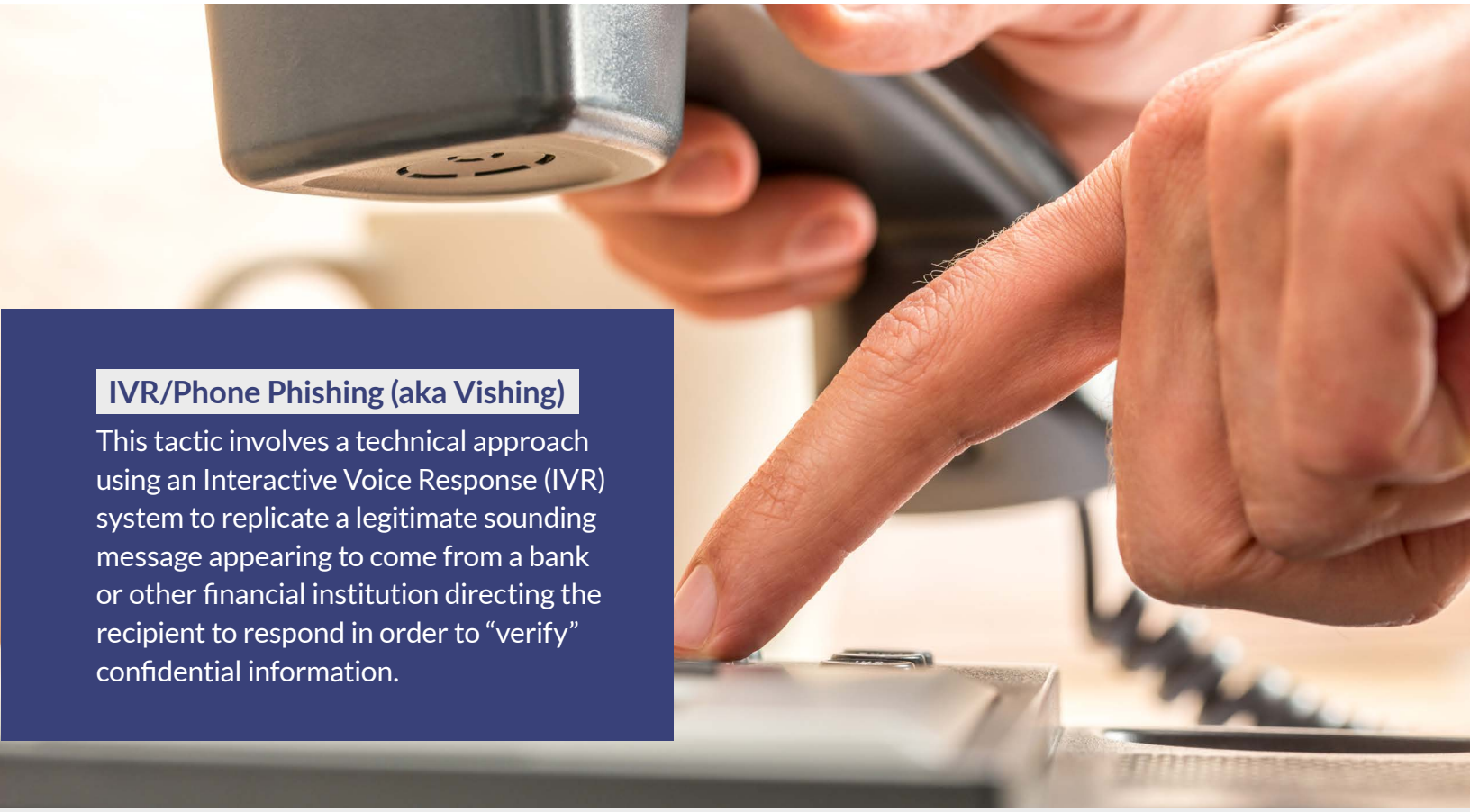
EXPLOITATION

THEN EXECUTION

A plan to mitigate the effect of Social Engineering attacks should be a part of any comprehensive security policy with a component that raises awareness among employees and educates those who are most vulnerable such as new hires, help desk personnel, contractors, executive assistants, human resource personnel, senior managers, and executives, as well as information technology (IT) employees who handle technical and physical security.

According to a survey sponsored by Check Point Software Technologies in 2011, nearly half of the global businesses they contacted reported being the victim of one or more Social Engineering attacks that resulted in losses ranging anywhere from $25,000 to $100,000 per occurrence.

Social engineers use many different strategies for gathering information from their targets and some of the methodology used includes the tactics listed below:



IVR/Phone Phishing (aka Vishing)

This tactic involves a technical approach using an Interactive Voice Response (IVR) system to replicate a legitimate sounding message appearing to come from a bank or other financial institution directing the recipient to respond in order to "verify" confidential information.

Impersonation/Pretexting

A common form of deception may involve an attacker using a believable reason to impersonate an authority, pretend to be a fellow employee, IT representative, or vendor in order to gather confidential or other sensitive information.

Phishing/Spam/Spearphishing

Phishing can come in the form of a phone call or email from someone claiming to be in a position of authority asking for confidential information, such as a password. Phishing can also include sending emails to organizational contacts that contain malware designed to compromise computer systems or capture personal or private credentials.

SMS Phishing (aka SMSishing)

This attack occurs when an SMS message is received that is purportedly sent from a reputable source, such as your bank, asking for personal details. SMSishing is a newer form of attack, but one that is on the rise with the proliferation of smart phones and sophisticated attackers.

Bluesnarfing/Bluejacking

Bluesnarfing is the unauthorized access of information from a wireless device through a Bluetooth connection, often between smartphones, desktops, and laptops. Direct access to calendars, contact lists, emails, text messages, and on some phones, pictures and private videos, can be made. Both Bluesnarfing and Bluejacking exploit others' Bluetooth connections without their knowledge. Usually harmless, Bluejacking involves only the transmittal of data to the target device, whereas Bluesnarfing is the theft of information from the target device.

Trash Cover/Forensic Recovery

Attackers collect information from discarded materials like old computer equipment (i.e. hard drives, thumb drives, DVD, and CDs) and company documents that were not disposed of securely.

Quid Pro Quo (Give and Take)

An attacker makes random calls and offers his targets a gift or benefit in exchange for a specific action or piece of information with the goal of rendering some form of assistance so that the victim will feel obligated in some way.

Baiting

A common method used in this type of attack involves leaving a malware-infected device such as a USB drive or CD/DVD at a location where an employee will come across it, and then out of curiosity will plug/load the infected device into their computer.

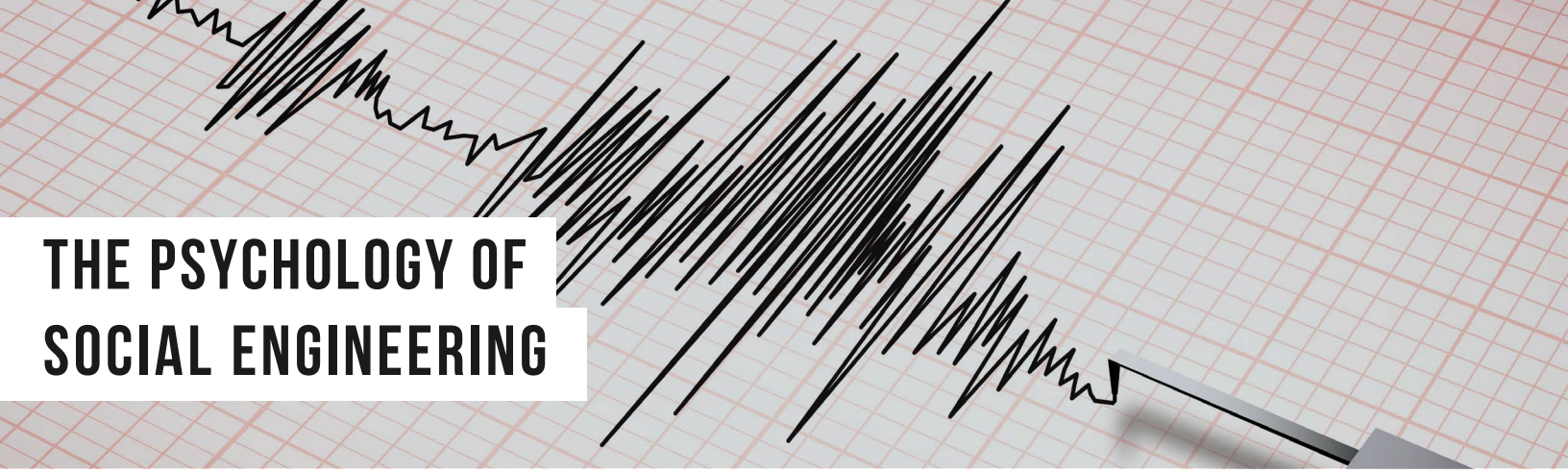
Tailgating/Direct Access

This type of activity refers to attackers who gain unauthorized access to company premises by following closely behind an employee entering a facility or present themselves as someone who has business with the company. In this instance an attacker may state that they left their security credentials inside the facility or at home if challenged by an employee while entering the facility.

Diversion Theft

The methodology in this attack involves misdirecting a courier or transport company; arranging for a package or delivery to be taken to another location.

Social engineers will focus their attention on locating other vital data such as account numbers, phone and client contact lists, organizational charts, as well as other information on key employees who have access privileges and computer system details (i.e. servers, networks, intranets, etc.) during their Information Gathering phase. They have also been known to go after tangible property such as keys, access cards, and identity badges especially in cases where their method of operation is through Direct Access.



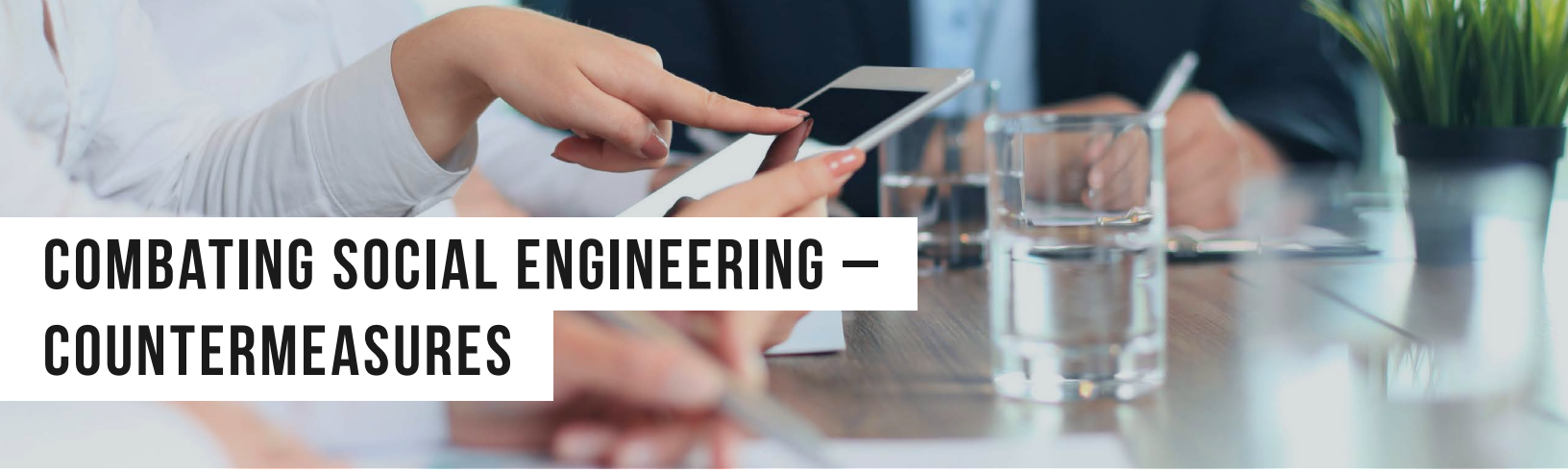
THE PSYCHOLOGY OF SOCIAL ENGINEERING

At this point the questions become, what is the motivation behind a Social Engineering attack and why are they effective? A scheme involving Social Engineering can have any number of goals; however, more often than not, it is simply for financial gain. Attackers have learned to leverage the human qualities of trust, helpfulness, and fear to manipulate their targets. Through 'pretexting', they play on the inherent desire of most people to trust another individual as well as rely on company policies that foster employees to be helpful, especially those in service-oriented positions. Social engineers have become adept at exploiting these traits as they go about gathering their information.

In addressing the trust issue, former hacker turned security consultant Kevin Mitnik explained in his book, The Art of Deception – Controlling the Human Element of Security:

"Why are social engineering attacks so successful? It isn't because people are stupid or lack common sense. *But we, as human beings, are all vulnerable to being deceived because people can misplace their trust if manipulated in certain ways. The social engineer anticipates suspicion and resistance, and he's always prepared to turn distrust into trust. A good social engineer plans his attack like a chess game, anticipating the questions his target might ask so he can be ready with the proper answers. One of his common techniques involves building a sense of trust on the part of his victim."*

Social engineers have also learned to exploit other human traits as well, including the natural tendencies to avoid doing something wrong or getting in trouble. If an attacker can make an employee feel they have caused a problem or performed a task incorrectly then they may become open to suggestion and thereby agree to compromise a policy or standard in order to correct the perceived error, which then leads to a breakdown in information security protocols. An employee may also be made to feel that they must "cut corners" in order to avoid a situation where their superiors become angry with them for possibly doing something wrong.



COMBATING SOCIAL ENGINEERING – COUNTERMEASURES

The best defense for combating Social Engineering fraud is awareness through corporate culture, education, and training. It is not enough for a workforce to simply follow a policy guideline; they must be educated on how to recognize and respond to an attacker's methods and become a "human firewall." Some effective solutions for inclusion into a proper countermeasure training program include the following recommendations:

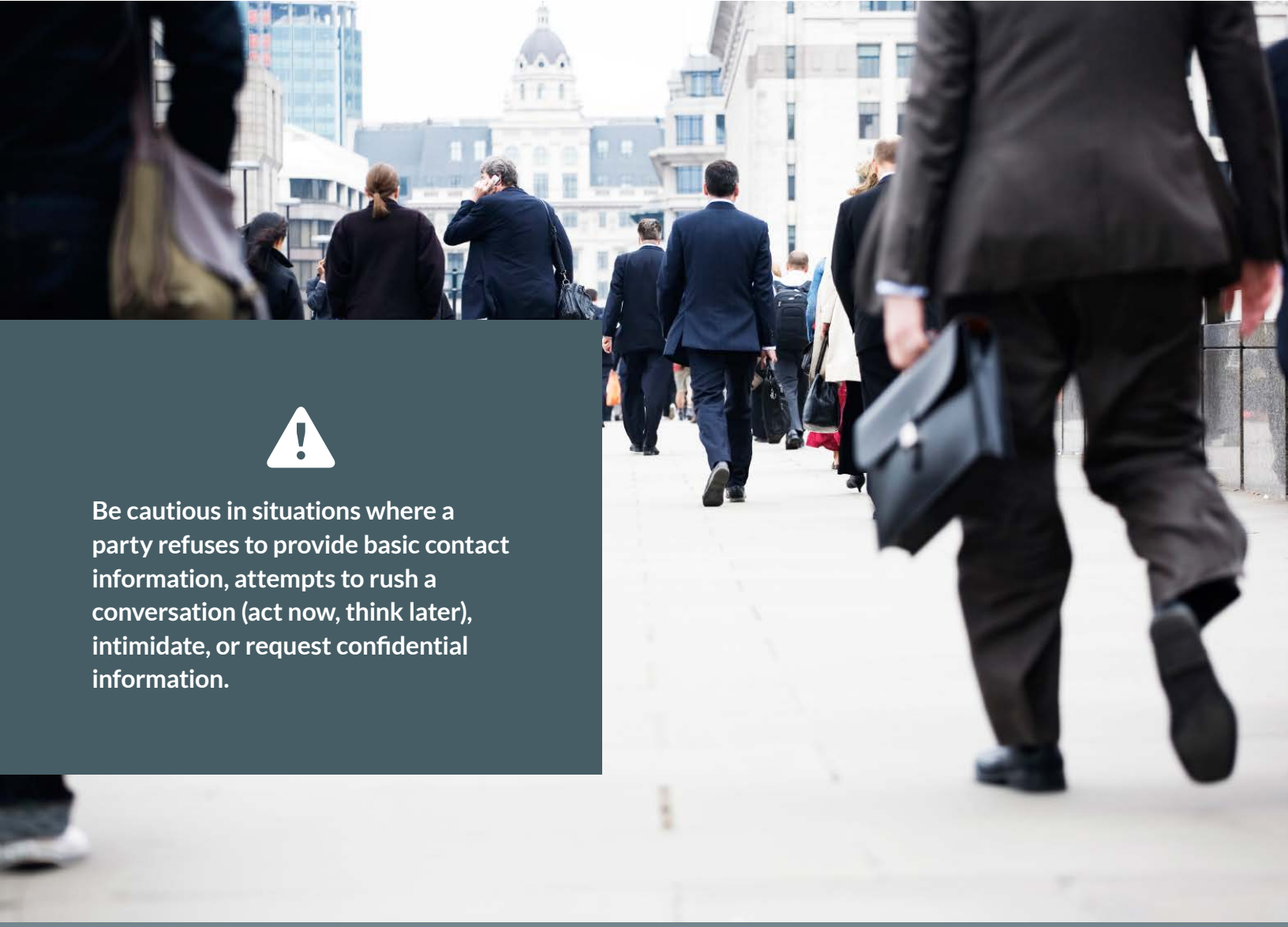
- **Prepare a Data Classification and conduct a Data Security Risk Assessment (DSRA),** which together identify business critical data both at rest and in motion, which employees have access to what types of information and why, and what levels of security are in place restricting/providing access to that information. Know who the likely primary targets of a Social Engineering scheme may be in your organization and which secondary targets are most at risk given their roles, the nature of their work, and/or the sensitivity of data to which they may have access.

- **When communicating either in person, over the phone, via email, or the Internet never disclose confidential or sensitive information** to someone you don't know or who doesn't have a valid reason for having it. Don't disclose passwords to anyone, even if they identify themselves as a co-worker, superior, or IT representative. Passwords should also never be given out over the phone or by email either.

- **Avoid using or exploring "rogue devices"** such as unauthenticated thumb/flash drives or software on a computer or network.

- **Be suspicious of unsolicited emails** and only open ones from trusted sources and never forward, respond to, or access attachments or links in them – delete or quarantine them.

- **Avoid responding to any offers made over the phone or via email** because if it sounds too good to be true, then it probably is. This could include unsolicited offers to help to solve a problem such as a computer issue or other technical matter.



Be cautious in situations where a party refuses to provide basic contact information, attempts to rush a conversation (act now, think later), intimidate, or request confidential information.

- **Physical documents and other tangible material such as computer hardware and software should always be shredded** and/or destroyed prior to disposal with any onsite receptacles, such as dumpsters.
- **Be proactive in combating information security complacency** in the workplace by implementing internal awareness and training programs that are reviewed with employees on an ongoing basis. This includes developing an incident reporting and tracking program to catalog incidents of Social Engineering and implementing an incident response strategy.
- **Consider conducting a reoccurring, third-party penetration test to assess your vulnerabilities.**
- **Guard against unauthorized physical access** by maintaining strict policies on displaying security badges and other credentials and making certain all guests are escorted. Politely refuse entry to anyone "tailgating." Keep sensitive areas such as server rooms, phone closets, mail rooms, and executive offices secured at all times.
- **Monitor use of social media outlets, open sources, and online commercial information** to prevent sensitive information from being posted on the Internet.

Provided below are some notable case studies involving different methods of social engineering fraud perpetrated against various types of businesses:

CASE STUDIES

CASE STUDY #1 VENDOR EMAIL HACKED

Private Company, less than 250 employees, less than $250M annual revenue

The controller of a private distributor of component parts was responsible for making regular payments to overseas vendors from which the company purchased product for resale in the United States. After many months of working with the vendor and receiving regular shipments, the controller received an email which appeared to come from his contact, indicating that the vendor's bank was having issues with accepting payments, and asked if the next payment could be made to a new bank. The vendor was located overseas, making verification a challenge. After some pressure was applied by the supposed vendor, the invoice was paid by wire transfer. The following month, when the real vendor realized that their best customer was late on their payment, an investigation determined that the vendor's email was hacked, and an imposter had been socially engineering the company into believing that the change in bank information was authentic. In the end, almost $250,000 was handed over to the fraudster.

THE CONTROLLER RECEIVED AN EMAIL INDICATING THAT THE VENDOR'S BANK WAS HAVING ISSUES WITH ACCEPTING PAYMENTS, AND ASKED IF THE NEXT PAYMENT COULD BE MADE TO A NEW BANK

CASE STUDY #2
FAKE PRESIDENT SCAM

Public Company, more than 250 employees, more than $150M annual revenue

The regional CFO of a subsidiary of a large, publicly traded company received an email purporting to be from the assistant to the CEO in the United States. The email requested that the CFO transfer a large sum of money immediately to facilitate covering a tax payment in China. When the CFO questioned the request, a follow up phone call was made to the CFO, assuring him that the proper authority was granted, and that it had come "from the highest levels" within the organization. With intimate knowledge of company policies, and an official looking letter "authorizing" the transfer on company letterhead, the CFO wire transferred the money. The scam was detected after another attempt made at transferring funds was stopped by the company's bank. After recovering only a portion of the original wire transfer, the customer suffered a $1,000,000 loss.

WHEN THE CFO QUESTIONED THE REQUEST, A FOLLOW UP PHONE CALL WAS MADE TO THE CFO, ASSURING HIM THAT THE PROPER AUTHORITY WAS GRANTED

CASE STUDY #3
ILLEGITIMATE CLIENT

Private Company, less than 50 employees, less than $100M annual revenue

A business manager handling bill payment and bookkeeping services for a client received an email purportedly from their customer, inquiring about her balance and availability of funds for a wire transfer. The email included details regarding the scope of services that were provided, as well as information about other transactions that had recently been performed. The wire was to go to an offshore account, purportedly for the purchase of a new piece of real estate. After answering his client's questions, the client purportedly authorized the wire of funds to the account requested. After noticing some activity in the client's spam account, the client grew suspicious and contacted their bank, requesting the wire to be stopped. Unfortunately, no part of the wire could be, and all $100,000 was lost.

THE EMAIL INCLUDED DETAILS REGARDING THE SCOPE OF SERVICES THAT WERE PROVIDED, AS WELL AS INFORMATION ABOUT OTHER TRANSACTIONS THAT HAD RECENTLY BEEN PERFORMED

ABOUT LOWERS RISK GROUP

Lowers Risk Group integrates the services of three industry-leading companies – Lowers & Associates, Proforma Screening Solutions, and Wholesale Screening Solutions – to create a complete risk management service offering for any organization. Employed in concert or on a standalone basis, the Lowers Risk Group companies excel in providing comprehensive enterprise risk management and human capital risk solutions to organizations operating in high-risk and highly-regulated environments. Our specialized background screening and crime and fidelity risk mitigation services protect people, brands, and profits from avoidable loss and harm. Our satisfied customers have come to expect and rely upon our experienced and professional approach for their risk assessment, compliance, investigation, claims, due diligence, background screening, and related risk mitigation needs to help them move forward with confidence.

LowersRiskGroup®

Protecting People, Brands, and Profits

LowersRiskGroup.com 540-338-7151