CAVIGNAC & ASSOCIATES
INSURANCE BROKERS

FEB 2016

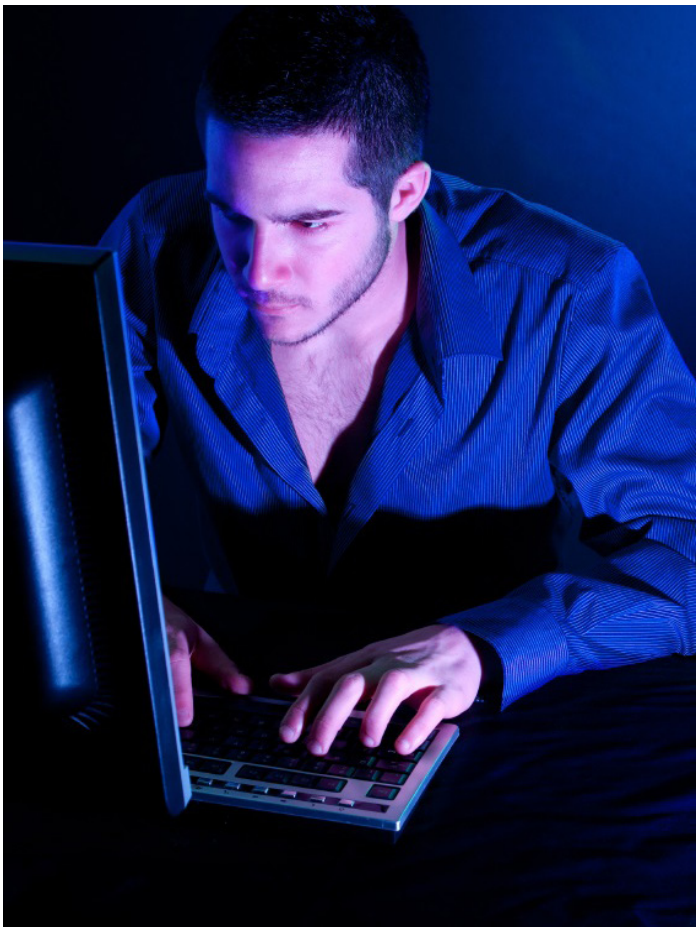
The Modern Day Con Man and the Social Engineering Play!

By Jason White, Managing Director, Swett & Crawford
Jeff Cavignac, CPCU, RPLU, ARM, President, Cavignac & Associates

Your controller receives an email from you directing her to forward funds to a current vendor's new address. No problem, it's from her boss, it's an internal email (or it looks like one) and she doesn't give it a second thought. Hit send…boom…money transferred. A few weeks later the controller gets a call from the vendor's accounts receivable department wondering why they haven't been paid. You know where this is going. The email the controller received wasn't sent by you, it was sent by a cyber-criminal who forged your email. I'd like to tell you that this is an isolated incident, but it isn't. It is happening all the time. The quality and creativity in the deception continues to evolve!

Social engineering is different from other forms of cyber theft like funds transfer fraud and computer fraud. The main difference is that social engineering involves the fraudulently induced, voluntary transfer of property (including money) by an insured. Both computer fraud and funds transfer fraud involve a third party who fraudulently transfers property including money, either from your business or your bank. Looked at another way, human-based social engineering fraud, otherwise known as "human hacking," is defined as the art of influencing people to disclose information and getting 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; they have learned



how to trick their targets into giving them information by exploiting certain qualities in human nature. 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 and can be human- or computer-based. However, security experts recognize that most scams follow a four-stage method:

- Information gathering
- Relationship development
- Exploitation
- Execution

(continued on page 2) **Con Man**

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. According to Check Point Software Technologies, nearly half of global businesses surveyed 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 or more.

Because social engineering is such a threat in today's workplace, it is essential that all employees in an organization be educated and trained on how to detect and prevent this type of fraud. Companies also need to develop and implement specific policies to prevent and respond to an attack (for example, training for employees on what constitutes confidential and sensitive information and how to keep it safe). Companies are advised not to focus their efforts and security budgets entirely on defending against technical attacks from hackers and other electronic threats, and thereby underestimating, or even entirely overlooking, the system weaknesses posed by the human element.

The first step is to understand the various social engineering strategies employed by cyber thieves. Here are a few:

- Impersonating/Pretexting: This common form of deception may involve an attacker using a believable reason to impersonate a person in authority, a fellow employee, IT representative, or vendor in order to gather confidential or other sensitive information.

- Phishing/Spamming/Spear phishing: Phishing can take the form of a phone call or email from someone claiming to be in a position of authority who asks 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.

2016 Risk Management Seminar Series

Sexual Harassment Prevention Training
Friday, March 4, 2015
7:30am Registration
8:00am - 10:00am Program

Workers' Compensation 101
Friday, March 11, 2016
7:30am Registration
8:00am - 10:00am Program

The Most Common Construction Injuries and How to Prevent Them
Friday, April 8, 2016
7:30am Registration
8:00am - 10:00am Program

Reserve Early, Seating is Limited!
To register, click on the 'register now' button in the announcement email, or contact Bethany Mongold at mongold@cavignac.com or call 619-744-0540.

NOTE: Due to the popularity of our seminars and limited space available, we regret we cannot provide refunds or credits with less than 72 hours advance notice of cancellation.

- IVR/Phone Phishing (aka Vishing): This technical tactic involves using an interactive voice response (IVR) system to replicate a legitimate sounding message that appears to come from a bank or other financial institution and directs the recipient to respond in order to “verify” confidential information.

- Trash Cover/Forensic Recovery: Attackers collect information from discarded materials such as old computer equipment (e.g., hard drives, thumb drives, DVDs, CDs) and company documents that were not disposed of securely.
  Quid Pro Quo (“give and take”): An attacker makes random calls and offers his or her 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 target will feel obligated in some way.

- Baiting: A common method of baiting involves leaving an innocent¬ looking, malware-infected device-such as a USB drive, CD or DVD-at a location where an employee will come across it, and then out of curiosity will plug/load the infected device into his or her computer.

- Tailgating/Direct Access: Attackers gain unauthorized access to company premises by following closely behind an employee entering a facility or by presenting themselves as someone who has business with the company. The attacker may state that he or she left 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 and arranging for a package or delivery to be taken to another location.

In addition, social engineers will focus their attention on locating vital data such as account numbers, phone and client contact lists, organizational charts, and other information on key employees who have access privileges and computer system details (on 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 second step is to develop a plan for mitigating the effect of social engineering attacks. It should include a component for raising awareness among employees and educating those who are most vulnerable: 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. It is not enough for a workforce to simply follow a policy guideline; employees must be educated on how to recognize and respond to an attacker’s methods and thus become a “human firewall.”

A proper countermeasure training program should include the following measures:

- Conduct a data classification assessment, identifying which employees have access to what types and levels of sensitive company information. Know who the primary targets of a social

engineering scheme are likely to be. Remember, all employees are at risk.

- Never release confidential or sensitive information to someone you don't know or who doesn't have a valid reason for having it, even if the person identifies himself or herself as a co-worker, superior or IT representative. If a password must be shared, it should never be given out either over the phone or by email.

- Establish procedures to verify incoming checks and ensure clearance prior to transferring any money by wire.

- Reduce the reliance on email for all financial transactions. If email must be used, establish call-back procedures to clients and vendors for all outgoing fund transfers to a previously established phone number, or implement a customer verification system with similar dual verification properties.

- Establish procedures to verify any changes to customer or vendor details, independent of the requester of the change.

- 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. Never forward, respond to or access attachments or links in such emails; delete or quarantine them.

- Avoid responding to any offers made over the phone or via email.

- 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), uses intimidating language or requests confidential information.

- Physical documents and other tangible material such as computer hardware and software should always be shredded and/or destroyed prior to disposal in any on-site receptacles, such as dumpsters.

- Proactively combat 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.

- Train customer service staff to recognize psychological methods that social engineers use: power, authority, enticement, speed and pressure. If it is important enough to move quickly on, it's important enough to verify.

- Consider conducting a recurring, third-party penetration test to assess your organization's vulnerabilities, including unannounced random calls or emails to employees soliciting information that should not be shared.

- Guard against unauthorized physical access by maintaining strict policies on displaying security badges and other credentials and making sure 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.

CONCLUSION

Due to the increasing prevalence of social engineering fraud schemes, it is reasonable to suggest that it may be only a matter of time until a social engineer targets an employee at your organization. Given the potential for loss, and the comparatively low cost of loss control measures, instituting a countermeasure program makes good business sense. ■

LIVE WELL WORK WELL

Health and wellness tips for your work and life—brought to you by the insurance professionals at

CAVIGNAC & ASSOCIATES
INSURANCE BROKERS

FDA Aims to Ban Minors from Tanning Beds

Due to concerns about the rising number of skin cancer cases, in December 2015, the U.S. Food and Drug Administration (FDA) proposed rules that would ban anyone under the age of 18 from using indoor tanning beds.

In winter, it can be tempting to jump into a tanning bed for some added color. However, tanning beds give off radiation that is 10 to 15 times stronger than the sun.

Tanning beds are linked to a number of health risks, including melanoma, the most dangerous form of skin cancer. Health risks increase each time someone tans; therefore, using tanning beds at young age can be especially harmful.

The proposed rule would also require **all** customers to sign a risk acknowledgement form before their first tanning session and every six months thereafter stating they're aware of the health risks.

The FDA will take comments from the public on the proposal for 90 days. If approved, violators could be subject to penalties, tanning bed confiscation and legal action.

The Importance of Good Posture

Posture is something that most people don't think twice about. We tend to sit or stand in whatever way feels the most comfortable at the time. However, poor posture can wreak havoc on a person's body, causing back and neck pain, muscle fatigue, digestive issues and even breathing problems.

Many Americans work at jobs where they spend most of their days sitting in front of computers. They then often go home and continue to sit after a long day at work. In the winter, individuals may spend even more time sitting when temperatures drop and outdoor activity becomes more difficult.

Spending many hours a day sitting and looking at a computer or a phone can lead to tight muscles in the back of the neck and upper back, which places stress on your bones and joints. Slouching or sitting in a scrunched position can also compress your abdomen and interfere with normal digestion.

To avoid the dangers associated with poor posture while sitting, make sure your computer monitor is at eye level to avoid straining your neck by constantly looking down. In addition, avoid holding a phone on your shoulder throughout the day. Instead, use a hands-free device like a headset or one with Bluetooth capabilities. Taking the time to stretch and strengthen core muscles can also help correct muscular imbalances.

Poor posture is something that affects you more over time. By taking steps now to be conscious of your posture, you can decrease your chances of developing joint pain and improve your overall well-being.

Fudgy Fruit

Celebrate Valentine's Day this year with this easy, healthy dessert recipe.

- 6 Tbsp. semi-sweet chocolate chips
- 2 large bananas, peeled and quartered
- 8 large strawberries
- ¼ cup unsalted peanuts, chopped

Directions

Place chocolate chips in a small microwave safe bowl. Heat on high for 10 seconds and stir. Repeat until chocolate is melted, about 30 seconds.

Place fruit on a small tray covered with a piece of waxed paper. Use a spoon to drizzle the melted chocolate on top of the fruit.

Sprinkle the fruit with chopped nuts. Cover the fruit and place in the refrigerator for 10 minutes or until the chocolate hardens. Serve chilled.

Makes: 4 servings

Nutritional Information (per serving)

Total Calories	151
Total Fat	10 g
Protein	3 g
Carbohydrates	24 g
Dietary Fiber	4 g
Saturated Fat	2 g
Sodium	2 g

*Percent Daily Values are based on a 2,000 calorie diet.

Source: USDA

Preventing Foodborne Illnesses

Each year, approximately 1 in 6 Americans get sick from food poisoning. It's not uncommon to hear about food being recalled or a new foodborne illness outbreak daily. Most people recover without any long-lasting effects; however, those who are pregnant, the elderly or those with chronic conditions are more at risk for developing complications.

Prevent foodborne illness at your home by being conscious of food safety guidelines. For instance, avoid eating raw or spoiled meats and eggs by checking expirations dates before purchasing and preparing food. Wash your hands, cutting boards and knives with antibacterial soap and hot water after handling raw meat, seafood or eggs. Never serve meat on the same plate it was placed on when it was raw. Use a food thermometer to make sure meat is cooked to a safe temperature.

In addition, avoid thawing food at room temperature; instead, defrost foods in the refrigerator and do not refreeze food once it's been fully thawed. Wash fruits and vegetables thoroughly before eating, especially those that will not be cooked (like fresh apples or pears) in order to prevent foodborne illness.

Food Poisoning Prevention Tips

Wash hands before and after preparing food.

Cook chicken and turkey to a temperature of 165 degrees Fahrenheit.

Cook ground beef, steaks and roasts to a temperature of 160 degrees Fahrenheit.

Read all FDA recalls and alerts about contaminated food.

Avoid unpasteurized milk or juices.

Spotlight On

Cavignac & Associates is proud to support local and non-profit civic organizations, including Monarch School.

monarch school
education. opportunity. transformation.

Monarch has served San Diego for nearly three decades, beginning as a one-room education center and expanding into a K-12 comprehensive school designed to educate homeless youth.

There are more than 1.2 million homeless students across the country and 22,000 in San Diego County alone. Research shows homelessness contributes to a wide range of challenges including physical and psychological problems, safety fears and academic struggles. It's estimated that 75% of homeless students do not receive a high school diploma. The barriers these students face, hinder their ability to become contributing, successful members of their families and society and place them at a high risk of becoming tomorrow's homeless adults.

At Monarch, we give students the skills and tools they need to overcome these odds.

Sandra McBrayer founded the school in 1987 recognizing the need to get homeless youth off the streets and in school. She was later named Teacher of the Year by President Bill Clinton for her work. In 1999, the Monarch School Project a 501 (c)(3) was established by San Diego Rotary to help relocate the school to a new facility. Today, the partnership between the school and the non-profit continues to make Monarch a recognized leader in the education of homeless youth.

For more information about , visit www.monarchschools.org