

Social Engineering Fraud on the Rise

Article provided by Professional Liability Agents Network (PLAN)

It was a typical morning for Ingrid, an accounting clerk at A&J Engineering Services. As she was going through her new emails she came across one from Jack Williams, the new financial manager at key vendor Johnson Supply Company. Jack had called her a couple of days prior to introduce himself and alert Ingrid that Johnson Supply would be making some changes to their banking accounts. Ingrid smiled as she recalled the friendly conversation they had about their pet pugs. Nice guy, she thought.

She opened the email, noticed the usual Johnson Supply logo at the top of the page and read Jack's note. He had included three smiley face emojis following his request to have all future payments wired directly to their new checking account. He included the account number and asked Ingrid if she would get this set up right away. He wrote that he really wanted to impress owner George Johnson with his quick and efficient work and hoped Ingrid would help him.

Ingrid noticed an email trail below Jack's note, where Ingrid's boss Tom had welcomed Jack and said he'd OK'd the new wire transfer deposit plan. Since Tom was good with it, Ingrid was happy to oblige and changed the bank account information for Johnson Supply. She let Jack know everything was set up.

A month or so later, Ingrid was surprised, when Tom stormed into her cubicle visibly upset. He waived a stack of invoices from Johnson Supply in her face

asking why she hadn't paid their most important vendor. Ingrid explained that she had paid all the invoices and followed Jack's new payment instructions exactly.

"Jack?" her boss said. "Who in the heck is Jack?" Ingrid felt a sinking feeling in her stomach.

It was later discovered that the payments had been deposited in an anonymous offshore account. A textbook case of social engineering fraud.



What It Is

Social engineering fraud (SEF) is the process of intentionally getting people to divulge or act on information under false pretenses by exploiting human nature. It is the act of deceiving and manipulating an individual in order to gain access to information, monetary resources or other assets.

Unfortunately, SEF is growing at a rapid pace. The Federal Bureau of Investigation reports that between October 2013 and August 2015, in the United States alone, more than 8,000 SEF victims were defrauded

of nearly \$800 million. The average loss: \$130,000. Travelers Insurance reports that SEF cases have increased by more than 90% annually, with more than 100,000 social engineering attacks launched daily. Approximately one in three businesses are targeted by SEF perpetrators. While large businesses are a favored target, small firms are becoming common victims as well.

Social engineering fraud takes many forms, but most have the following characteristics:

Investigation. The perpetrator cases the company looking for vulnerabilities and identifying likely targets among its employees. In our example above, the perpetrator identified a lower-level clerk who had access to financial accounts.

Impersonation. The SEF perpetrator typically impersonates a real or fictitious individual with a supposed connection to the company -- a vendor, a customer, an employee, a banker, etc.

Relationship building. The perpetrator builds a social relationship with the target employee in order to create friendship and trust. Our perpetrator discovered that Ingrid had a pet pug through her Facebook account and used that information to create a positive, friendly bond.

Exploitation. The perpetrator uses the friendship and trust built with the targeted victim to convince them to do something they wouldn't otherwise do. In our example, Ingrid willingly changed the vendor's bank account number without verifying the change with the vendor or her boss.

Execution. It used to be that attempts to defraud companies and individuals via the Internet were fairly easy to spot because of bad grammar, spelling errors and sloppy graphics on emails and websites. Not anymore. SEF perpetrators create websites, emails, attachments and other documents that look exactly like the real thing. Ingrid was convinced that the email came from Johnson Supply, and the email trail

clearly showed that her boss was on board with the change.

Education, Training and Safeguards Imperative

When it comes to social engineering fraud, the best offense is a good defense. That defense begins with awareness training for all employees. Make SEF a well-known acronym from the front desk receptionist to the board room. Employee ignorance is your company's greatest vulnerability when it comes to SEF.

Explain to employees how SEF works. Warn them to be vigilant and report to management when a potential perpetrator tries to convince them to take actions that could make the company vulnerable.

Management should identify what company information and resources might attract a SEF attack and, equally important, who has access to those resources. Identify primary employee targets and focus ongoing training and monitoring there.

Examine your policies for handling financial and other sensitive information. Prohibit any single employee from releasing such information without specific high-level clearance. Don't allow any individual to single-handedly complete a financial transaction above a certain dollar threshold. Require managerial review and approval for any requests for changes to customer or vendor accounts. If you receive a phone or email request from a vendor or customer to change account information, follow up by phone or an in-person meeting to verify that the request is legitimate.

Work with your accounting firm to set up these and other fraud safeguards. You might want to consider hiring a consulting firm to conduct SEF penetration tests by phone and email to probe for vulnerabilities.

Are You Insured?

Despite your best efforts, you cannot make your company 100% safe from social engineering fraud.

Insurance is your final financial safeguard to minimize or eliminate SEF losses.

Companies who have purchased cyber insurance may be shocked to find that this type of insurance likely does not cover losses from social engineering fraud. Most cyber policies cover losses resulting from unauthorized entry into or the failure of the company's computer network. With SEF, the targeted employee is typically authorized to enter the network, which is likely working just fine.

Similarly, some crime policies may deny coverage for SEF losses. These policies may have language that limits coverage to "direct" fraud and excludes coverage when losses are the result of a "voluntary parting" with company resources -- i.e., when assets are released with the knowledge and consent of an employee.

Fortunately, forward-thinking insurance companies are now offering specific social engineering fraud endorsements to their crime and fidelity policies. These endorsements bridge the SEF coverage gaps created by traditional cyber and crime policies. Indeed, they extend coverage to specifically include instances of social engineering fraud perpetuated by perceived vendors, clients and others.

To obtain SEF coverage, you may be required to fill out a supplemental application outlining the policies and procedures you have in place to combat SEF. Insurance limits can be as low as \$10,000 or as high as \$1 million or more.

SEF Risk Analysis

We would be happy to help you analyze your current insurance policies and identify potential coverage gaps that leave you vulnerable to SEF losses. We can also get you quotes on an SEF policy endorsement that matches your exposure. Don't wait until you're the next victim of social engineering fraud. ■

Risk Management Seminar Series



Heat Illness Prevention and Enforcement 101

Friday, March 17, 2017

7:30am Registration

8:00am - 10:00am Program

Navigating Leaves of Absence

Friday, April 14, 2017

7:30am Registration

8:00am - 10:00am Program

Risk Management Bootcamp: The Triangulation of Human Resources, Safety and Claims Management

Friday, May 12, 2017

Note: This is an all-day workshop with separate sessions that can be registered for individually

Reserve Early, Seating is Limited!

To register, click on the 'register now' button in the announcement email, or contact Bethany Mongold at mongold@cavnac.com or call 619-744-0540.

LIVE WELL WORK WELL



Health and wellness tips for your work and life—

Cavignac & Associates

Workplace Stress Levels Dropping

Stress in the workplace is on the decline, according to a recent study from health portal provider MediKeeper, Inc.

The majority of respondents said, on a scale of one to five, that their stress level was at a two in 2016. This is down from 2014, where the majority said they were at a level three.

Similarly, the number of people who reported a level one increased by 58 percent over the same two-year period.

Curb your stress with these helpful tips:

- Make to-do lists of tasks that need completing and cross off items as you finish them.
- Talk with a co-worker about things that are bothering you. Getting support from friends is a great way to relax and reduce anxiety.
- If you continually run late, set your clocks and watch ahead to give yourself extra time.
- Read over your job description so you know exactly what is expected of you.

This article is intended for informational purposes only and is not intended to be exhaustive, nor should any discussion or opinions be construed as professional advice. Readers should contact a health professional for appropriate advice.

© 2017 Zywave, Inc. All rights reserved.

Prepare for Tax Season

Tax season is almost upon us and it is important that you have all the information you need to file your 2016 tax returns. Below is some general information to help you understand the filing process. If you have any specific questions related to your filing situation, it is important to consult with a tax professional.

How to File

Many people elect to file their tax returns electronically. This can be done in a variety of ways, including tax-preparation software, like Turbo Tax, consulting a tax return professional or using the IRS' [Free File](#) software, if you qualify.

Forms to Include

If you are filing with a paper form, there are certain documents you must be sure to include. Required forms include the following:

- A copy of your W-2 for each of your employers over the last calendar year.
- A copy of Form W-2C (a corrected W-2 form), if received from your employer.
- A copy of Forms W-2G and 1099-R, if federal income tax was withheld.

For more information on how to file, what forms to include, credits you qualify for or any other filing-related questions, please visit the IRS' [Interactive Tax Assistant](#) tool. This interactive tool was designed by the IRS to help individuals navigate the tax filing realm.

ROASTED HERB POTATOES

- 1 pound potatoes (3 cups cubed)
- 2 tsp. vegetable oil
- ½ tsp. rosemary
- ½ tsp. salt

PREPARATIONS

1. Preheat the oven to 450 F. Use vegetable cooking spray to coat a baking sheet large enough to fit the potatoes.
2. Wash and peel the potatoes. Next, cut them into ½-inch cubes and place into a bowl.
3. Combine the rosemary, oil and salt in a small bowl. Then, pour the mixture over the potatoes and stir to coat them evenly.
4. Spread the potatoes evenly on the baking sheet. Bake for 25 to 30 minutes, or until golden brown.

Makes: 6 servings

Nutritional Information (per serving)

Total Calories	70
Total Fat	2 g
Protein	2 g
Carbohydrates	13 g
Dietary Fiber	1 g
Saturated Fat	0 g
Sodium	190 mg

Source: USDA



Spring Break Travel Tips

Traveling is usually the most stressful part of any vacation. Things like bad traffic, airport security or misplaced travel documents can set a bad tone for the rest of the trip. Here are some tips to help avoid travel woes.

Plan Ahead

A good trip is often well thought out and incorporates as many details about the vacation as possible. Things like coordinating transportation to and from airports and hotels, packing appropriate clothing for the destination climate, and having all required travel and reservation documents is essential for a smooth trip.

Arrive Early

If you are flying, it is recommended that you arrive at the airport at least two hours ahead of your departure. This will ensure you have time to queue through security checkpoints and settle in at the gate before boarding the plane.

Pack Smart for TSA

Security is a time-consuming and unavoidable ordeal at the airport. Make the process a little quicker by storing liquids in a separate, clear bag so you can pull it out at the screening checkpoint.

Top 5 Spring Break Destinations

1. Miami Beach
2. Cancun
3. Bahamas
4. Cabo San Lucas
5. Maui

Source: U.S. News & World Report



Spotlight On



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



Since 1970, Serving Seniors has been the leading provider of programs and services for low-income seniors in San Diego County. We are the only organization in San Diego, and one of the few in the country, that provide such a broad base of vital services to a vulnerable, at-risk population of older adults. Our innovative approach to providing wrap-around services including nutritious meals, health education, social services, case management, affordable supportive housing and lifelong learning opportunities has earned national recognition as a model for keeping seniors healthy and independent.

Serving Seniors serves adults 60+ regardless of race, color, religion, sex, marital or civil union status, sexual orientation, gender identity, national origin, place of birth, ancestry, citizenship, military or veteran status or disability. Serving Seniors is dedicated to providing the highest quality of service to enhance the health and well-being of individuals, families and the community at-large. Our staff, board and volunteers believe each and every person is created equal and worthy of dignity and respect. We strive to create a safe place for all with zero tolerance for discrimination.

For more information about visit www.servingseniors.org