# Social Engineering:

## GOOD INTENTIONS, DEVASTATING RESULTS

January 2016

by Devin Harrigan

Social engineering fraud is on the rise. Is your organization prepared to recognize the risks?

*The $500,000 donation from a local business executive was the largest gift to the arboretum in a year. The organization moved quickly to complete the processes and paperwork needed to finalize the transaction, including paying $25,000 in legal and permit fees up front. Yet after the fees were paid, the donation did not arrive. The arboretum discovered the entire donation to be fake, and the "legal and permit fees" were actually wired to a fraudulent overseas account.*

*A horticultural society was contacted by a university in Japan about sending a group of students to attend classes there. The Japanese university would pay for the students' tuition fees, and the local horticultural society agreed to pay for the transportation costs and receive reimbursement later. An employee following up with the university discovered that the initial contact was fraudulent, but only after the firm had wired $18,000 to a fake "travel agency."*

*One dry August morning, an office manager of a botanical garden received a phone call from the local water company: The water bill was seriously overdue. To avoid having the water shut off, the office manager had to wire $15,000 by the end of the day. When the office manager called to confirm the payment had been received, he discovered the water bill had been paid on schedule and the water company had no record of a new payment.*

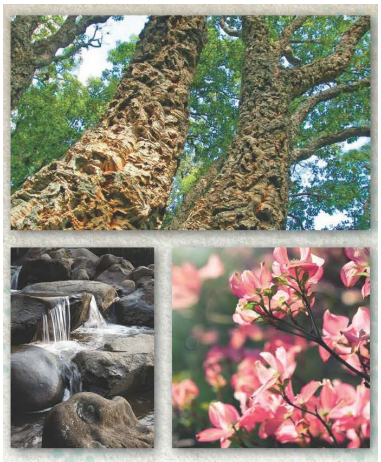
Scenarios like these are more common than you might think. "Social engineering" is the practice of persuading an organization's employees or volunteers to provide sensitive information and ultimately funds through wire transfer or other means to fraudulent parties. By phone, email, or even in person, a hacker poses as a legitimate donor, vendor or other associate. The scammer gleans enough information from online or social media about you and your organization to look legitimate. He or she will also typically use psychological manipulation tactics such as gaining an employee's confidence or subtly threatening an employee to act quickly.

In other words, social engineering scammers use some of your employees' best traits – such as responsiveness and helpfulness – against the organization they work for. A worker's initiative in solving a problem or tending to a task ends up putting the organization's finances at risk.

How big is the problem? Email compromise scams alone resulted in $1.2 billion in losses globally from October 1, 2013 to December 1, 2014, according to the Federal Bureau of Investigation.

Nonprofit gardens may believe their organizations aren't on hackers' radar screens. However, smaller organizations are sometimes targeted because they don't have large information security or risk management departments to help detect and prevent social engineering fraud.

Once funds are lost, the likelihood of recovery is slim. Funds are sent to foreign bank accounts established by organized criminals, which are quickly drained before the victim is aware of their loss. Because of federal banking laws, victim's banks are generally not



GROWING CONFIDENCE
MANAGING RISK

considered responsible. Unfortunately, traditional crime and cyber insurance policies also typically don't respond in these instances, either.

## Derailing Social Engineering

The good news is that many of these schemes can be detected and prevented by taking a few simple steps.

Lowers & Associates, an independent risk management consulting firm, provides the following "best practices" to help mitigate and potentially avoid social engineering fraud.

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

## Get What You're Expecting

Insurance can be an important extra level of protection from social engineering fraud. To help assess how well you're covered, ask the following questions:

- *What would it take to get social engineering included in my crime insurance policy, and what would be the cost?* Inquire with your agent or broker, who will be able to explain your options. Typically, a short application is necessary, as well as potentially an additional premium.
- *What exclusions apply?* Be aware that even with social engineering insurance, there may be exclusions. Among the most important, many companies, *but not all*, have a "callback" provision stating that if an employee does not call back to verify a request for funds, the loss will not be insured.

Criminals will continue to find ways to use your information to their advantage. But by being aware of the risks, and the steps to help address them, you can help keep your information – and assets – out of criminals' hands.

CHUBB

*Devin Harrigan is a manager for the Chubb Group of Insurance Companies in Troy, Michigan.*