

FORENSIC ACCOUNTING & FRAUD

Low-tech con artists prey on people's kindness

By **TODD SNAPP**

An old adage says 'Fool me once, shame on you; fool me twice, shame on me.' But the fact is, whether they are willing to admit it or not, people are gullible. It is no wonder that businesses must face the reality of hackers bringing age-old con artistry methods into the 21st century.

As organizations wage war on computer hackers, the focus continues to be on technology defences. Firewalls, access controls, intrusion detection, and secure communications are all essential components of a security barricade. But in recent years, an alarming number of security breaches have come through what some have dubbed the 'human firewall,' more simply, the employees.

The practice of conning employees is certainly not new. The classic con artist, or 'social engineer,' hacks with a focus on employees rather than computers. As IT departments scramble to slam the gate on network infiltration, social engineers turn to infiltrating through people.

Social engineers have accomplished some of the largest security breaches and most vicious terrorist attacks in history. T-Mobile, Choicpoint, Club Monaco, Hewlett-Packard, TJX and even the 9/11 attacks were all made possible by skilled human deception. Industry analysts such as the Gartner Group say such activity shows no signs of slowing. They call it the greatest security threat of the next decade.

What better way to access sensitive information than with stolen credentials or information handed to you by an unsuspecting employee? What better way to view secured organizational information than to walk in the front door and open a file cabinet, or sit down at an unlocked computer? What better way to learn the executive secrets of an organization than to listen in on their conference calls?

There are no intrusion alarms, no denials of service, no suspicious activity, just an 'employee' accessing information made readily available to him.

According to the U.S. Privacy Rights Clearinghouse, a non-profit privacy and identity theft watchdog, close to 75 per cent of reported IT security breaches in the last year were accomplished with methods other than computer hacking.

These breaches include all different types of fraud and theft that don't require technical skills or a computer at all. Yet, in a society where people pride themselves on enlightenment and independence, few will admit that they were a rube for con artists. Fewer still

know enough to recognize the creative techniques used by social engineers.

Even so, most employees' sense of security about business fraud causes them to think that they will know what to do when victimized. History shows that employees are an easily accessible sieve of information. Most often the breaches go unnoticed until private data gets

most anyone who needs their help. For the majority of employees, a call or message from a hacker is unexpected and peculiar, requiring the employee to make a quick decision and rely on instincts to prevent a security breach.

For people in this situation, five factors slow their reaction time:

- Reluctance to call another person

- IT security departments have enough to worry about without opening up the social engineering can of worms;

- Definitions of social engineering are included in an organization's basic training program and this is all that is needed;

- The organization is well aware of its points of weaknesses and will

public embarrassments, when organizations are breached and IT security managers are the first on the chopping block. Progressive security managers identify the threat and develop creative solutions leveraging positive reinforcement and the employee's common knowledge of identity theft.

The combination of social engineering skill and employee kindness has made it so that even a poorly developed scam can have unprecedented success (case in point: the Nigerian bank e-mail scam).

Social engineering threats merge security, organizational, and psychological weaknesses. In order to establish a successful shield against the onslaught of employee-targeted attacks, organizations must first take the threat seriously and then implement strong policy, training, and assessment tools. These will equip their 'human firewall' to protect themselves from attacks.

Todd Snapp is the president of RocketReady, a Tampa, Florida based security company focused on the human side of security. He has made it his career goal to enlighten corporations and government to the serious threat posed by low-tech



in the open.

The effectiveness of social engineers can be tied to the skills and behaviors of the three main parties involved: the social engineer, the victimized employee and the organization's management.

The social engineer is a clever and polished hacker who is quite aware of human tendencies. They select their targets carefully and strategize their attack so that their victim will often be apologetic that they could not provide more information.

When performing his low-tech scam, the social engineer is careful to pace himself and may even spend days or even weeks acquiring seemingly useless details, which are building blocks for pursuing the items he is really after.

In most cases, the building blocks are contact information, organizational structure, or internal terminology that will give him credibility when communicating with employees. The truly desirable items can be as simple as an employee ID or as damaging as private customer data or secure system passwords.

The most significant factor in a social engineer's behavior is his apathy toward his victim. Attacks are ruthless and can even include aggressive or intimidating methods. Regardless, the social engineer is well-prepared and is not concerned about defrauding or offending the victim.

The victimized employee

For most organizations, customer service is a top priority. Employees are encouraged to be accommodating and respectful to

a liar;

- Fear of personal consequences (loss of job or some reprimand);
- Training to be helpful and never rude to a caller;
- Rationalization that the suspicious behavior is just a strange request by a legitimate person; and
- Desire to avoid conflict or awkwardness.

Desire to avoid conflict may be the greatest obstacle in defending against attacks. Many employees will often fulfill a suspicious request just to avoid tension. Even more damaging is the reluctance to report events once they have occurred. Rarely is a security breach prevented because of a proactive report by an employee.

The organization's management

From a management perspective, a social engineering attack can be frustrating and difficult to identify. In particular, some IT security managers have struggled to develop defenses against an ever-changing threat to an ever-changing employee base.

Since these attacks can result in long-lasting damage to the organization's reputation, managers are motivated to devise a response. However, procedural obstacles cause many executives to become cynical about the threat.

Cynical reactions to employee security threats usually fall into six categories:

- Social engineering will eventually fade away like so many other methods of hacking;
- Employees will always be the weakest link in security. There is nothing you can do to prevent employees from being duped;

keep an eye out for issues; and

- Documented policies are clear about restricting the employee from giving out sensitive information, and if they are followed there will be no problems.

These attitudes set the stage for

Our Results-Driven Advice™ comes in a wide range of services

- Assurance
- Tax
- Business risk
- Business consulting
- Financial advisory

For forensic accounting & investigative services please contact:

Jennifer Fiddian-Green
CA•IFA, CFI, CFE, CAMS, CMA
(416) 360-4957
jfiddian-green@GrantThornton.ca

David Malamed
CA, DIFA, CPA (Illinois), CFE
(416) 360-3382
dmalamed@GrantThornton.ca

Peter Fatjewski
CFE
(416) 360-4998
pfatjewski@GrantThornton.ca

Grant Thornton

**Chartered Accountants
Management Consultants**

www.GrantThornton.ca