WHITE PAPER

Cyveillance®
a QinetiQ Company

The New Face of Social Engineering Attacks on the Web

June 2011

EXECUTIVE SUMMARY

Social engineering is an ancient tactic, exploiting human weakness, ignorance, fear, uncertainty, and vanity, to manipulate victims for personal gain.

Today, with users putting more of themselves online in the “social web world,” social engineering scams have rapidly risen to become the #1 most prevalent type of online security threat. Whether through email, IM, Facebook or dozens of other social media outlets, it’s far too easy for scammers to con well-meaning individuals into providing access and information.

Scammers of every variety are using social media networks as an ideal gateway to a vast new source of victims all too willing to disclose highly valuable personal information.

Social engineering in a Web 2.0 world has evolved to a fine art, characterized by highly targeted, customized attacks. In fact, today the biggest scams are happening repeatedly to some of the largest, most respected names in global business, targeting high value corporate assets and intellectual property.

While firewalls, passwords, smartcards and the like can all work to provide businesses with a more secure infrastructure, the human component is always the weakest link. There are steps organizations can take, from cyber safety awareness and formal training to exploring new options in proactive social engineering protection services.

SOCIAL ENGINEERING DEFINED

Simply, social engineering is psychological exploitation: the manipulation of reason, logic and relationships to get people to do something which presents a risk or a threat. It’s all about capitalizing on relationships people have with those they know, their “circle of trust”, manipulating them to divulge information, or outright posing as a trusted source to do the same.

Social engineers appeal to authority, vanity, emotion or logic using verifiable facts and figures to gain access to money, information, anything of value.

Social engineers also rely on the natural helpfulness of people. It’s human nature, for instance, to hold the door open for someone carrying an armload of packages; whether they’re authorized to enter is another question.

Over thousands of years, social engineering has not changed its methods, only its medium Consider these scenarios:

- In the wake of a natural disaster, a mass email is sent from an impostor under the guise of 'The Red Cross' asking for assistance money.
- An official-looking online Christmas card arrives from 'The White House', asking recipients to click on an inviting attachment that turns out to be an infectious link.
- Hundreds of USB sticks are mailed to top U.K. CFOs, supposedly a creative (and exclusive) party invite. As each CFO opened the 'invitation', the drive ran destructive malware.

One of the primary types of social engineering on the Internet is phishing. The schemes are varied and typically involve something like this: The victim receives an email, IM, or text under the guise of a legitimate and respected source with alarming news that his bank account has been compromised. It then asks the victim to enter his ID and password or other sensitive information. It's a direct, upfront request from the criminal for the personal data, which is voluntarily disclosed by the victim before he realizes he's been tricked.

A more insidious, subtle form of social engineering involves malware. In this scenario, the victim clicks on a credible-looking link which has just downloaded malware onto the victim's PC. Every subsequent keystroke, every entry of userids and passwords, every log on to the corporate network gives the perpetrator further visibility and access to a wealth of valuable information.

More devastating than a one-time phishing attack, malware damage can continue for longer periods, feeding the criminals stolen information *over time, with far more opportunity to reap the maximum value of the data*.

A RAPID TRANSFORMATION

Social engineering has rapidly risen from 'one of the oldest tricks in the book' to a fundamental corporate threat that can't be ignored. In fact, security experts predict that as our culture becomes increasingly dependent on information, social engineering will remain the *single biggest threat* to any enterprise or government security system.

Social engineering attacks, particularly through social media sites and services like Facebook and Twitter, are one of the newer and more rapidly increasing threats. Fraudsters have a huge, always-on, target-rich (more than 500 million!) environment at their disposal, many of whom are maintaining a constant Facebook connection through a combination of their work computers, personal computers and smart phones.

The Classic Social Engineering Scam

Now a well-known part of internet folklore, the famous 'Nigerian fraud scam' is a perfect example of a social engineering attack. Emails promised large sums of money to people who wired the scammers a nominal 'advance' fee.

Today, variations on this scheme are plentiful, increasingly sophisticated, and pervasive.

The January 2010 Aurora attack launched from within China against Google and more than 30 other high profile companies was so sophisticated that many experts characterized it as a game-changing threat model. Invaluable source code, product designs and key intellectual property were stolen. The scammers 'social engineered' employees, often posing as Facebook friends in a massive attack that blew a hole in employees' 'circle of trust'. This attack migrated across multiple organizations including some in the defense industry, exposing highly sensitive national security information.

Thanks to social media, a new generation of hackers can target nearly anyone in short order. Consider this: in less than five minutes, scammers using Google, Facebook and other social sites can draw a highly personalized, detailed 'digital footprint' – favorite charities and sports activities, religious affiliations, family connections, vacation preferences, for example — making it extremely easy to craft a convincing message that can put individuals, families, and companies at risk.

In fact, ready-to-go spear phishing attacks targeting specific individuals or organizations can be launched literally within moments of breaking news about serious global events or natural disasters. Even a seemingly innocent tweet with a late-breaking news alert about a popular celebrity can lead an unsuspecting user right into a landing page with destructive malware.

SOCIAL ENGINERING TODAY: HIGH STAKES, HIGH REWARDS

Today social engineering on the Web is characterized by the following:

Greater stealth and patience on the part of the criminal.

Increasingly, criminals are more anonymous. Particularly in the case of malware attacks, these highly motivated criminals may intentionally go "quiet" and live inside a network indefinitely. For weeks or months, they take their time doing diligent background investigative work in order to zero in on the most high value targets. In fact, organized crime groups with literally limitless resources at their disposal, are quite comfortable working far under the radar screen for long periods of time in order to reap the long-term rewards.

Highly targeted and highly customized to specific individuals.

"One of the most frightening aspects of social engineering is that the con artists are coming after you *personally*," says Eric Olson, Vice President of Solutions Assurance for Cyveillance. Unlike the mass distribution scams that target huge groups of people, today's threats are highly customized – your friends, your family, your preferences, your habits. Research shows men and women are targeted equally, and are equally susceptible.

Going after the big score.

Perpetrators are going after 'the big prize'. Targets have gone beyond login credentials to high value intellectual property such as designs, confidential company or industry data, and customer information. Criminals are looking for anything and everything of value, even when that value may not be obvious. And when a breach does occur, the first question should be 'Who does this breach benefit?' 'Who would gain from acquiring this specific intellectual property, and know how to use it?' In nearly every case, the list of potential perpetrators is very short.

Sometimes it's not about the dollar amount of what's taken, but the nature of what's taken. Take the Night Dragon attacks -- a series of persistent, coordinated 'industrial espionage' attacks against as many as a dozen international energy utilities since November 2009 -- all with the goal of extracting highly sensitive(and valuable) data. According to Bloomberg Businessweek, computer hackers working through Internet servers in China reportedly broke into and stole proprietary information from the networks of energy companies including names such as Exxon Mobile Corp. and Marathon Oil Corp. In some cases the criminals had undetected access to company networks for more than a year. Hackers targeted computerized topographical maps worth millions that show locations of potential oil reserves. Though highly effective, the attacks themselves have been characterized as "unsophisticated," using a cocktail of conventional intrusion methods including social engineering phishing attacks.

No sophisticated or highly technical tools required.
The simplest scams can be the most devastating. As one security expert says, “It doesn’t matter how many locks you have on the doors if you can con someone into giving you the keys.” While the latest technology tools are not necessary, criminals are, however, showing more advanced communication tactics and greater sophistication in terms of writing and web design skills.

It’s not just big enterprise targets.
Any organization that assumes it is not at risk is mistaken. The neighborhood grocery store may seem an unlikely target; but a database for the customer rewards program, for example, holds precisely the type of personal information social engineer scammer’s value. The bottom line: criminals are finding endless ways to monetize just about anything.

It’s often the context AND the content that’s the problem.
Increasingly, the most dangerous social engineering scams may take the form of harmless-looking emails with no infected attachments. It’s all about the ‘intent’ behind the sender. Traditional phishing solutions cannot evaluate both and typically rely on attachment or url analysis, more is needed as the sophistication of these attacks.

WHAT YOU CAN DO

According to Cyveillance Cyber Intelligence Director Dr. Terry Gudaitis, “Any organization with the most sophisticated network security technology can still remain vulnerable to old-fashioned social engineering. At the end of the day, it boils down to individual responsibility, awareness and training.” Here are some guidelines.

Have a safer online ‘attitude’. Monitor your behavior, how you interact, where you click, how you act and react. Think about who the message appeals to and why. Who is asking? Imagine the communication from the perspective of the criminal. Assume any message from an unknown party is malicious. Cyber security training can provide practical tips such as insights into common tipoff’s within an email. Likewise, think about the type of information you share; one moment an employee is sharing weekend plans on Facebook, the next moment innocently mentioning the international travel plans for the CEO.

Understand your own digital footprint. Every American who has a cell phone and email has a wide open dossier of high value, specific information. While banking and criminal records are protected, an astounding amount of valuable information is readily available.

Determine who has access to high value information or systems. Know the digital footprint of these individuals. And bear in mind that it’s not always the high profile senior executive who’s most susceptible. Sometimes the most low profile mid level individual can be a target. It’s all about who holds the keys.

An Eastern European cybergang has been stealing millions of dollars from Europe’s carbon registries through equal parts ‘digital con game’ and digital burglary. As Byron Acohido reports in a January 2011 USA Today story, Europe’s carbon registries let companies buy and sell pollution credits. The gang that scammed them put a fresh spin on phishing. Basically the gang impersonated employees charged with buying and selling carbon emission permits. After gathering intelligence about the carbon registries in 25 nations, the gang began to target specific employees, sending them carefully-crafted emails enticing them to open a document infected with the Nimkey banking Trojan. From that foothold, the crooks methodically harvested account log-ons and closely monitored trading processes. At the proper moment, someone would log on as an authorized trader, execute a transaction and divert the proceeds into accounts controlled by accomplices. In one sting the gang stole $31 million from a Romanian cement company; in another, they called in a bomb threat to the Czech Republic registry. While the building was cleared, the bad guys exfiltrated $25.6 million. As a result, the majority of Europe’s carbon registries remain closed.

Heighten company-wide awareness and education of how social engineers operate. Training targeted at both the executive team and employees is imperative. Build a culture where every employee understands their part in the overall cyber safety of the organization. What's more, training must stay up to date with the latest threats. Organizations may provide security training, but all too often it's outdated and focused only on "yesterday's" threat vectors.

Proactive ongoing monitoring is essential for success. Every organization must take responsibility for implementing a continuous, comprehensive monitoring strategy that takes into account changing risk situations, including both leaked internal data as well as external data. It's important to monitor social media environments for general and specific threats alike to protect both personnel and core business operations.

Be prepared to act quickly. Have a complete social engineering protection service in place, complementary to your existing security measures, that is able to protect against social engineering attacks in real time. The Social Engineering Protection Appliance™ (SEPA) from Cyveillance is the first of its kind to be entirely focused on the rapid detection and protection against new forms of social engineering attacks.

CONCLUSION

Social networking websites have become a hotbed for online criminals, making literally hundreds of millions of people from all walks of life prime targets. With the emergence of interactive online communication tools such as social networks, blogs, microblogs and more, every employee and any organization can be targeted for a social engineering attack.

Today's savvy social engineer scammers want to infiltrate your personal correspondence, making targets like Facebook far more interesting and profitable to them.

Social engineering scams will continue to evolve and become even more convincing, more international, and more professional.

Prevention begins with education about the value of information, increasing awareness of how social engineers operate, and having the right services in place to protect against attacks in real time. Today every organization, small and large, has the data and information easily monetized by criminals. Now more than ever, cyber security is everyone's business.

The Real Deal or Social Engineering?

USA Today columnist Craig Wilson reported in his March 2, 2011 column:

"I got one of those e-mails from someone who was stranded at an airport in Europe. They'd been robbed, lost their passports, and desperately needed $1,000 to get their affairs in order and get back home. Could I help?

I was about to kill the little scam out of my system when I realized that I actually knew the people in need. Pam was one of my oldest friends from high school. And her husband, Jon, was on the e-mail too, spelled as his name really is. Jon. Could it actually be? Could this be the real deal, I wondered?

So I e-mailed them back. I told them how sorry I was to hear about their predicament but needed to ask them a few questions first. What is your brother's name? Where did you go to school? Your mom's maiden name?

I awaited the answers ... Almost immediately came a reply. "I don't understand."

And so I killed it out. Later in the day the real Pam and Jon surfaced in an e-mail apologizing to everyone that their account had been hacked and that they were not stranded in London, but happily at home.

ABOUT CYVEILLANCE

Cyveillance, a world leader in cyber intelligence, provides an intelligence-led approach to security. Through continuous, comprehensive Internet monitoring and sophisticated intelligence analysis, Cyveillance proactively identifies and eliminates threats to information, infrastructure, individuals and their interactions, enabling its customers to preserve their reputation, revenues, and customer trust. Cyveillance serves the Global 2000 and OEM Data Partners – protecting the majority of the Fortune 50, regional financial institutions nationwide, and more than 30 million global consumers through its partnerships with security and service providers that include AOL and Microsoft. Cyveillance is a QinetiQ Company. For more information, please visit www.cyveillance.com or www.qinetiq-na.com.

Cyveillance, Inc,
2677 Prosperity Avenue
Suite 400
Fairfax, Virginia 22031
888.243.0097
www.cyveillance.com
info@cyveillance.com

Cyveillance®
a QinetiQ Company