Fraud Intelligence
Business intelligence | informa
www.counter-fraud.com

FEATURE › CONFIDENCE SCHEMES

Social engineers – today's 'Greeks bearing gifts'

Just as the Trojans of ancient literature were intrigued by a giant wooden horse, social engineers are assailing countless organisations today under seemingly innocent guises. Deceptive entry techniques are at the crux of the prolific hacking assaults by fraudsters on commercial entities. Peter Warmka of Strategic Risk Management exposes social engineering methodology and the most effective defences.

Throughout history, great empires have spent considerable resources building walls and fortresses to safeguard the riches of their kingdoms from outside threats. The Trojans overconfidently trusted the integrity of their walls after the Greeks repeatedly failed to penetrate the city of Troy for over ten years. However, the Greeks then decided to leverage basic human psychology. As told by Homer and Virgil, they withdrew their army from the sight of the Trojans, only leaving behind a gigantic wooden horse. The deceptive ploy worked masterfully. Believing it was a peace offering, the Trojans triumphantly opened their gates and transported the gigantic wooden structure through the fortifications and into the heart of the city. Once the Trojans were sound asleep, the Greek soldiers, emerging from inside the horse, opened the gates, allowing the rest of the army to penetrate the city and easily defeat their powerful enemy. In deploying the infamous Trojan Horse, the Greeks exploited the basic human tendency to trust. Today's fraudsters, using various social engineering techniques, continue to exploit this same vulnerability, known, in the security context, as the *human factor*.

The human factor refers to the interaction between human beings and the technology meant to protect the organisation. While many senior executives tend to believe that significant investment in technology will provide sufficient protection against threats, fraudsters skilfully bypass these controls, directly targeting humans they consider the weakest link.

The human targets are viewed as *insiders* who may be manipulated for specific ends. For the fraudster's purposes, insiders are not only employees of the organisation; they include anyone who may have unescorted access into a target organisation, which could mean the cleaning crews, catering companies, vending machine stockers, guard force, maintenance contractors, etc.

Prior to launching any type of social engineering attack, professional fraudsters will formulate their plan based on available open source information. While such information may be accessed in various ways, the most frequent medium is simple online research.

A good starting point for collection is the target organisation and the digital footprint that the entity already has on the world wide web. The following are a few of the many online resources that a social engineer may use:

- *Entity webpage*: frequently provides useful data regarding the organisation's history, mission statement, products and services, as well as full profiles of key personnel *(insiders)* along with their pictures;
- Job posting sites such as *Monster.com*, *Indeed.com* and *Careerbuilder.com* - these frequently reveal the IT qualifications sought by employers, providing valuable insight into the operating systems and software programmes the organisations run on their servers.

The job posting gives social engineers an opportunity to submit a cover letter/resumé electronically to Human Resources or someone else in the organisation. That email, along with attachments, may be used to introduce malware into the target's system. While less frequently exploited, such job postings can also yield opportunities for fraudsters to interview with the employer and elicit sensitive information;

- *Glassdoor*: offers very useful workplace insights posted by employees. Ultimately, these reviews provide the social engineer with a pulse on morale in the organisation. Generally, it is much easier to manipulate a disgruntled employee than someone who is happy and loyal;
- *Facebook*, *Google+*, *Foursquare* and other social media accounts managed by organisations will frequently contain uploaded photos and other images revealing physical workspaces; these may include floor plans, office configurations (ie, private versus open shared lounge spaces), security system hardware, IT systems, employee badges, employee dress, etc. Much of this information will be extremely useful when planning a physical intrusion;
- *Wayback Machine* (http://archive.org/web/) is a digital archive of the world wide web. It enables users to see archived versions of web pages, as far back as 1996;
- *Google Maps* and *Google Earth* allow a fraudster to conduct virtual reconnaissance of a target entity, revealing useful information on access points to the facility, including the presence of badge readers, CCTV cameras, guards, etc. Such reconnaissance can also identify businesses near the target location, such as coffee shops, restaurants, bars, fitness centres, office supply stores, etc. The first objective may be to identify places that individuals from the target facility are likely to frequent, allowing the social engineer to orchestrate opportunities to run into them. A second potential objective is the identification of locations in the vicinity that make deliveries to the target's residence/offices, such as restaurants, flower shops, office supplies, etc. Knowing this information, the social engineer could decide to impersonate someone making a delivery to obtain access to the premises.

Now let us consider resources utilised by social engineers to collect data on targeted insiders. Ultimately, they will want to know as much as possible about insiders' personal and professional background as well as an indication of their possible motivations and/or vulnerabilities. With this information in hand, fraudsters can better manipulate them.

The most common start point will be social media sites. The following are just three of many examples:

- *LinkedIn*: here a social engineer will learn about the target's professional profile (academic and work) and interests, and their network of contacts;
- *Facebook*: here the fraudster will find pictures of a target insider, their family/friends and identify their network of social contacts. He may also learn where the target lives, their age, birthday, where they went to school, their hobbies, interests, past travel as well as future travel plans. When faced with a target who has switched on privacy settings, the resourceful social engineer will turn to an account utilised by their spouse and/or children who will frequently not operate the same level of security;
- *Twitter*: play by play action of where the target is, what they doing at that moment, what they are thinking and how they express themselves.

Once the professional fraudster has collected useful contextual data, he will utilise one or more of the following four general social engineering attack vectors:

1. **Phishing** currently represents over 90 per cent of all social engineering attacks. It usually takes the form of an unsolicited email from the fraudster requesting that the recipient click a link or open an embedded attachment. If the recipient complies it might lead to downloading of malicious tools, potentially compromising his computer, if not his entire IT network. Professional social engineers will use *spear phishing,* which tailors the email to a specific target, leveraging information previously gleaned from data collection. The spear will greatly enhance the likelihood of the target clicking on the link or opening the attachment.
2. **Smishing** is very similar to phishing, but instead of using email as a medium to deliver the attack, the social engineer will send a link or attachment via text message. The result is the same. While smishing is not yet as common as phishing, we can expect it to begin mirroring trends in mass marketing – which is beginning to favour SMS due to high open rates.
3. **Vishing**, while requiring a little more skill, is typically much more effective than phishing and/or smishing. Here, the social engineer will telephone the target using any one of several ploys – such as pretending to be a fellow company official, IT personnel, building security, an important client, financial institution where the organisation maintains accounts, etc. The fraudster requests sensitive information and/or persuades the target to undertake a specific action. To increase credibility, the social engineer will frequently *spoof* the call. Service providers, such as *spoofcard.com*, provide the mechanism to manipulate the caller ID seen at the recipient's end.
4. **Direct intrusion** using any of a variety of pretexts - the fraudster will interact face-to-face with the target or individuals with access to the target. Examples include: posing as someone who has a business appointment inside of the building; posing as IT support needing to carry out an urgent upgrade/repair; posing as a fire inspector conducting a survey; or posing as a member of contracted service providers such as the cleaning crew, catering company or guard force. Another effective ploy is to present as someone delivering a package that requires the recipient's signature.

Once inside the facility, if unescorted, the social engineer can utilise a variety of tools to further breach the target's security. The social engineer may place listening devices in conference rooms or keyboard loggers to capture specific information such as network usernames and passwords. A fraudster can easily leave several thumb drives around the premises marked '*Confidential Payroll*'. Betting on the nature of human curiosity, the social engineer would expect that at least one employee picking up such a thumb drive would insert it into his computer hoping to see the compensation others are receiving. Once this action is taken, the social engineer has succeeded in uploading malicious files, potentially compromising the network.

Another very successful ploy is to pose as an executive recruiter. Without need to divulge the name of a specific client, the 'recruiter' can directly contact a target insider. The recruiter will claim to be impressed by the insider's professional background as detailed on LinkedIn and emphasise that the target may be a great candidate for an attractive position they are trying to fill. Feeling they have nothing to lose, the target will frequently allow the social engineer, either over the telephone or during a personal meeting, to elicit considerable information regarding the target's own background, in addition to confidential details about current and/or past employers.

The main reason social engineering works is that humans tend blindly to trust everyone, even people they do not know. It is this trust that makes it easy for social engineers to deceive and manipulate their victims.

So, how can organisations protect themselves from social engineering? First, organisations need to minimise the amount of unnecessary, yet exploitable, data they put out on the internet. In addition to establishing clear policies on content employees are authorised to post online regarding the organisation, there must be someone responsible for scanning key sites periodically to ensure compliance. The more data available to social engineers, the more likely it is the organisation will be on a list of targets. While unenforceable, the same practice of limiting sensitive disclosure should be encouraged among employees in their use of social media.

A second measure is to establish Social Engineering Awareness Training in the organisation. The purpose is to help employees recognise potential social engineering attacks. Once alerted, employees also need to know how to react. Simply not complying with the social engineer's request is not enough. Organisations need to have incident reporting in place to enable the employee promptly to bring the attack to the attention of security.

All insiders need to understand that if they are approached by someone, whether by email, SMS text, telephone call or in person, they must first verify that the person is who they say they are and that they have a legitimate request. 'Verify before Trusting' will be the most effective first line of defence to counter such fraud.

■ **Peter Warmka** CFE, CPP, CIA-U is managing director at Strategic Risk Management (www.astrategyforrisk.com), based in Orlando, Florida. He previously served as a senior intelligence officer with the United States Central Intelligence Agency and has worked abroad extensively, in Europe, Africa and Latin America.

Fraud Intelligence is published by Informa Law, Third Floor, Blue Fin Building, 110 Southwark Street, London SE1 0TA. *Fraud Intelligence* gives you practical insight, analysis and tools to combat fraud, whether you're in the corporate or non-commercial sector. Our financial crime content is available online via single-user subscriptions or multi-user licences at https://www.i-law.com/ilaw/financial.htm including *Lloyd's Law Reports: Financial Crime* (ISSN 1756 7637) and *Compliance Monitor* (ISSN 0953 9239).

Client Services: Please contact Client Services on tel: +44 (0)20 7017 7701; +65 65082430 (APAC Singapore), or email clientservices@i-law.com

Editorial queries: Please contact Timon Molloy on tel: +44 (0)20 7017 4214, or email timon.molloy@informa.com

Informa Law is an Informa business, one of the world's leading providers of specialist information and services for the academic, scientific, professional and commercial business communities.

Registered Office: 5 Howick Place, London SW1P 1WG. Registered in England and Wales No 1072954.

Print managed by: Paragon Customer Communications.

Stock images supplied courtesy of www.shutterstock.com.

Informa Law
Business intelligence | informa