WHITE PAPER

Hampering the Human Hacker and the Threat of Social Engineering

Using Automation to Protect Your Customers and Your Business

2014 was yet another banner year for security breaches that resulted in compromised customer records. According to the 2015 Data Breach Investigations Report (DBIR) issued by the Verizon RISK Team there were 700 million compromised records in 2014, based on contributions they received from around the world. These compromises resulted in estimated financial losses of $400 million. More than two-thirds of those compromised records were accessed using social engineering tactics. Victims were chosen simply because it was easy to obtain, and subsequently misuse, their information.

The estimated financial loss in 2014 from compromised records is $400 million.

While financial information is the most commonly discussed topic when it comes to data breaches, the digitization of healthcare and growing number of Internet of Things (IoT)-enabled devices that collect and transmit data mean other, more personal information is also at risk. Clearly, companies of all sizes and in all industries need to understand the deceptive practices that social engineers use, and how to protect themselves and their customers from attacks. In the following pages we'll take a look at:

- The definition of social engineering
- How it is used to gain access to corporate information and customer data
- Why to combine education and training with automation in the form of applications and services, to prevent attacks by social engineers

Social engineering attacks are not only among the most prevalent but are often the most damaging. Companies can however, begin the process of stopping social engineering attacks in their tracks by understanding how social engineering tactics work and training personnel to recognize them. Adding specialized applications and services designed specifically to prevent intrusions by social engineers can protect automated voice response systems and agents in a contact centers. As a result, companies can ensure the integrity of their data and the privacy of their customers.

Social Engineering – What Is It?

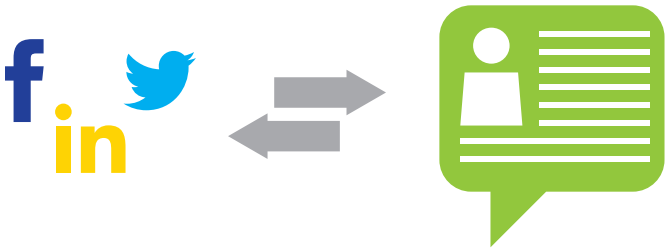
Everyone, every day, uses social engineering. It's how we get our children to go to bed at night or eat the "right" foods. It's how doctors and psychologists get their patients to do the things that are "good for them". Social engineering in these contexts is often a positive thing.

Social engineering can also be used to manipulate people into doing things they shouldn't or giving away confidential information. Wikipedia defines this type of social engineering as "the act of manipulating people into performing actions or divulging confidential information. While similar to a confidence trick or simple fraud, the term typically applies to trickery or deception for the purpose of information gathering, fraud, or computer system access."

Social Engineering Tactics and Tools – Using Deception to Break In

Social engineering attacks are based on one thing – information. Without information about your customers, social engineers aren't able to use the elicitation and pretexting tactics that are described below.

This information is relatively simple to obtain. A good social engineer can spend a few hours researching a target online and have enough information to make even the most seasoned contact center agent believe the social engineer is someone they are not. The increasing amount of personal information that's available using search engines, Whois databases, social media (Facebook, LinkedIn, Twitter, etc.), blogs, and photo sharing sites makes it very simple for them to find or determine. Even social security numbers are available from some paid research services.



In addition to researching individuals, social engineers may cast a broader net. "Phishing" is the term given to campaigns that generally involve fraudulent e-mails or texts sent to a large number of people, posing as an institution such as a bank or retailer, attempting to convince the recipient that they need to resolve an issue with their account. If the email or text impersonates the company well enough, it may persuade the user to enter their user name, password and/or other personal information on a site set up to collect that information for future account compromises, or to install malware that will compromise their computer and allow this type of personal data to be collected.

Phishing may target individuals or organizations. Sometimes, a single, high-ranking individual at an organization will be targeted (known as "spear-phishing"). For example, a 2015 case of spear-phishing involves a US magazine publisher's CEO being spear-phished so that his identity could be used to initiate large bank transfers.

23% of recipients open phishing messages, and 11% click on the attachments.

- Source: 2015 Data Breach Investigations Report

If your customers receive a phishing message, unfortunately, many of them will respond to it. The Verizon 2015 DBIR notes that 23% of recipients now open phishing messages, and 11% click on their attachments.

Once the social engineer has relevant information, whether gathered through research, phishing or a combination of the two, they use it in these highly effective human-hacking tactics:

- Elicitation
- Pretexting

Elicitation

The National Security Agency of the United States Government defines elicitation as "the subtle extraction of information during an apparently normal and innocent conversation." Social engineers use the information they've gathered to get their target to first trust them. The approach might be based on a common interest or experience.

Once trust or rapport has been established, they use conversational skills and tactics to encourage their target to take action (perhaps send a "replacement" credit card to a hotel for a traveler) or provide in depth information. Those tactics include:

- Appealing to one's ego
- Expressing a mutual interest
- Making a deliberate false statement
- Volunteering information
- Assuming knowledge
- Leading questions
- Assumptive questions

Elicitation tactics are often very effective in convincing a contact center agent to provide that one "extra" piece of information a social engineer needs to steal a customer's identity or gain access to their data.

Pretexting

According to the Merriam-Webster Dictionary, pretexting is "the practice of presenting oneself as someone else in order to obtain private information." Pretexting is more than a lie. It often includes using publicly available information to create a new identity — and then using that identity to acquire information or convince a target to take a specific action.

In calls to contact centers, pretexters use publicly available information to "spoof" IVR systems or agents into performing acts that could compromise the privacy or identity of a real customer. The pretexter might use an email or home address

to gain access. Passwords aren't usually a problem – they're easy to guess if you know the names of the real customer's pets or outside interests. If the password has been obtained by phishing, this is even easier. Once they've "spoofed" the IVR system or agent your customer's data is compromised.

Pretexters also use telephone-based tools like ANI (automatic number identification) Spoofing to enhance the new identity. In ANI Spoofing, the pretexter changes the number that appears on the called party's phone display from his or her own number to that of a: Basically, pretexters can change their number to anyone else's. To do that, they use Caller ID Spoofing technologies that are cheap and easy to acquire.

Social engineering attacks are powerful because they take advantage of our very human desire to be polite and helpful. To counteract that power, companies need a combination of practices, processes, applications and services designed to stop social engineering attacks before they begin – before they reach the most vulnerable link in the chain – the human.

Preventing Social Engineering Attacks – The Best Breach is No Breach at All

Preventing attacks by social engineers should be a high priority for every company of every size. No company, or even individual, is immune from unscrupulous individuals looking for inside information, ways to inject malware, or monetary gain through identity theft. To keep social engineers out of your company and your systems, we recommend a three-step plan:

#1 Education – Teach employees the importance of protecting company and personal information. Make employees and customers aware of social engineering tactics and how they can be used to manipulate people into providing information they shouldn't. Let customers know how they can validate an email or SMS message related to their account so they are better able to identify phishing messages they receive.

#2 Audits – Many companies currently perform PCI compliance or other types of security audits that address malware and hacking attacks. Adding an audit that targets social engineering weaknesses makes perfect sense. Choose an auditor that has the knowledge and experience that is required to do the job without crossing any legal and/or ethical lines. Some companies opt to comply with state and federal privacy regulations using third party, hosted services.

- **PCI Hosting** – Keeping customer care and self-service software up to date (usually newer versions have patches that close security holes) and maintaining an environment that is PCI compliant can be expensive and difficult. An alternative for many companies is to utilize services from a PCI compliant hosting company. A hosting company that is PCI compliant will ensure that all software is up to date (and all security patches have been implemented) and that the environment remains secure through regular audits. PCI compliant hosting is a simple way to insure the integrity and cost effectiveness of a company's customer care and self-service application environment.

#3 Technology – Stopping elicitation or pretexting attacks before they reach a human being is the best method of prevention. But, when that isn't possible, stopping these attacks immediately is essential. Among the most effective tools in social engineering attack prevention are:

- **Caller ID/Automatic Number Identification (ANI) Detection** – Services like Aspect's ANI Verifier analyze the phone number of incoming calls to determine if the Caller ID/ANI is spoofed. If the number has been spoofed, the call is rejected and never reaches the called party. The ANI Verifier stops pretext attacks before they can reach a contact center agent or employee.
- **Biometrics** – Biometrics solutions, which commonly include voice biometrics but may also include facial or fingerprint data (e.g., Apple TouchID), make it possible for companies to stop pretext or elicitation attacks before the attacker can use deception tactics on an employee or contact center agent, and can effectively secure data available via self-service applications. It also significantly lowers the effort required by customers to gain secure access to accounts and information. In the past, this technology was relatively expensive and difficult to deploy. However, newer service approaches and API-based implementation make it a simple and cost-effective way for companies of all sizes to reliably authenticate customer identities.
- **Location Intelligence** – Location-based intelligence allows companies to verify the exact location of a customer based on their mobile device or even their landline. This information can be used to help verify individual interactions or across channels. If, for example, several transactions are performed (over the phone, SMS, mobile web or smartphone app) from multiple geographies in a short time period, more stringent security could be required. Companies can also use location-based services to verify the location of a credit card transaction matches the location of the customer.
- **Dynamic Security Questions** – Companies will continue to use information customers know as a step in the authentication process based on level of risk. Opting for a solution that uses dynamically generated security questions based on information in personal records, such as a verifying a recent purchase or credit card payment, are difficult for thieves to predict and hack.

The technologies listed above each individually can help protect companies from attacks by social engineers, even those who have procured customer passwords. However, when used together these technologies provide rigorous multi-factor authentication, and form a robust and difficult to penetrate bastion against elicitation and pretext attacks.

Equally important, is the opportunity companies have to make a positive impact on the customer experience and the bottom line. Using the technologies described enables customers to verify their identities faster and with fewer frustrations. At the same time, costs are reduced by minimizing the time agents spend on authentication.

Conclusion

Social engineering is a very real part of every company and every individual employee. It's the way we get our children to clean their rooms, but it's also the way that unscrupulous individuals acquire private information, distribute malware, and steal identities. Their "successes" are apparent in the more than 700 million company or customer records that were compromised in 2014 alone.

Companies should take steps now to protect themselves, their employees, their customers, and their partners from social engineering attacks. Steps that include employee education and social engineering audits combined with automated software and services that can:

- Detect spoofed Caller IDs
- Authenticate callers based on their unique voice-print
- Pinpoint the location of communications
- Maintain a secure and PCI compliant transaction and application environment
- Dynamically generate security questions

Education, audits, and automation combine to build the new "social engineering firewall" – a firewall that hampers the human hacker, and protects companies and their information.

Corporate Headquarters East
300 Apollo Drive
Chelmsford, MA 01824
+(1) 978 250 7900 office
+(1) 978 244 7410 fax

Corporate Headquarters West
2325 E. Camelback Road,
Suite 700
Phoenix, AZ 85016
+(1) 602 282 1500 office
+(1) 602 956 2294 fax

Europe & Africa Headquarters
2 The Square, Stockley Park
Uxbridge
Middlesex UB11 1AD
+(44) 20 8589 1000 office
+(44) 20 8589 1001 fax

Asia Pacific & Middle East Headquarters
8 Cross Street
25-01/02 PWC Building
Singapore 048424
+(65) 6590 0388 office
+(65) 6324 1003 fax

About Aspect

Aspect's fully-integrated solution unifies the three most important facets of modern customer engagement strategy: customer interaction management, workforce optimization, and back-office. Through a full suite of cloud, hosted and hybrid deployment options, we help the world's most demanding contact centers and back offices seamlessly align their people, processes and touch points to deliver remarkable customer experiences. For more information, visit **www.aspect.com**.