Deloitte.

Safeguarding your enterprise from social engineering fraud risks

Forensic

Safeguarding your enterprise from social engineering fraud risks

What is social engineering fraud?

The recent case involving around 800 call center staff in India who duped foreign citizens of several million posing as income tax officials to extract money[1], has put the spotlight on one of the least discussed fraud schemes – social engineering.

Social engineering involves seeking information from unsuspecting victims and using it to dupe/defraud them. The cost effectiveness of this technique[2] makes it very popular across the world. It is usually assumed that only the gullible fall prey to such tactics and that personal data is primarily sought by fraudsters. However, in our experience, social engineering techniques can be deployed to extract organizational data too. If employees are untrained to respond to requests from fraudsters, it can put organizations at huge risk.

Typically, fraudsters manipulate some aspects of human behavior to persuade employees to share information. These include:

- **Desire to be helpful.** All employees, especially those in client-facing roles, are trained to be cordial and helpful to their customers. This desire to be helpful may lead to sharing of unauthorized information. Further, as organizations increasingly pride themselves on being quick to respond to customers, employees may overlook the need to verify requests for information for fear of delaying response to customers.
- **Tendency to trust.** Fraudsters tend to do extensive background research to create scenarios that will gain the trust of their victims. This includes providing accurate information about the subject to him/her to gain confidence and reduce suspicion. Most of us tend to trust individuals who appear to know significantly about our past behavior and personal details.
- **Personal greed.** Many successful social engineering attacks have been designed around personal greed where the individual is promised something valuable in return for such information. This can cloud judgement momentarily and make the victim a puppet in the hands of the fraudster.
- **Fear of indulging in unethical practices.** Fraudsters can take advantage of the fear/weariness that citizens have of facing government authorities such as those representing the tax department, municipality and the police. Building stories around tax defaults, non-payment of dues etc. is a common way to con individuals into parting with their money/ confidential data.

Examples of common social engineering techniques

Most social engineering scams follow a four-stage process:

- Information gathering (either prior to or during the interaction with the victim)
- Relationship development (during the interaction with the victim)
- Influence (attempting to convince the victim to buy the fraudster's story)
- Execution (instructing the victim to take certain action)

The three fictitious cases on the facing page illustrate some ways of how social engineering schemes can be developed.

Typical information sought by fraudsters that could put organizations at risk

- Phone numbers and email IDs of employees
- Employee IDs
- Salary details
- Work experience details
- Credit card details
- Passwords
- Financial details pertaining to business plans
- Vendor and contracts related data

[1] Sources : http://www.ndtv.com/india-news/maharashtra-police-detain-over-500-for-dupingus- citizens-1470385 ; http://localpress.co.in/2016/10/indias-biggest-raid-772-call-centreemployees-duped-us-citizens-rs-1-crore-everyday/

[2] Compared to the budgets required for a high end technology set-up to capture or decrypt sensitive information, social engineering primarily requires weaving a convincing story to get this information from the victim.

Case 1*

A large public sector company called Bare Limited faced a social engineering attack where fraudsters first registered a domain called www.bareltd.com that resembled the company's website www.bareltd.co.in. Further, the fraudsters created a fictitious email ID using the name of the company's finance manager Dev Patil. Mr. Patil's original email ID was dpatil@bareltd.co.in , whereas the ID created by the fraudsters was dpatil@bareltd.com. Fraudsters then hacked the company's IT systems to get information on clients and any billing-related communication. Using this knowledge, they sent emails from the fictitious ID to clients asking them to pay their dues to an alternate account, owing to some bank procedures being conducted at the old account. Clients and the company were both duped of several crores of rupees by the fraudsters and the fraud came to light only when the procurement team at Bare Limited questioned the clients over non-payment of dues, about three months after the incident took place.

Case 2*

When Radhika Mathur, the CFO of GoodLife Corp was asked by her CEO Brajesh Gupta to transfer Rs 200 crore urgently to a bank account in the Middle East, she did not question it. After all Mr. Gupta had sent her a "confidential" email mentioning how GoodLife Corp was in talks with an Iranian company for acquisition. In line with local laws in Iran, it was necessary to show that GoodLife Corp had adequate presence in the country and sufficient bank balance to proceed with the acquisition. He had provided her with the account details to enable the transaction and claimed that the law firm Grover and Kochhar as well as the company's bankers had just received the necessary clearances for this transaction. Hence immediate action was required from Radhika.

Over four transactions Ms. Mathur quickly transferred Rs 200 crore, to an account in the name of Mr. Hassan Hosseini at Bank Majidi. When Ms. Mathur called Mr. Gupta to inform him of the transfer, he drew a blank and Ms. Mathur realized she had inadvertently allowed the company to be defrauded. The "confidential" email received from Mr. Gupta was fake. On closer scrutiny, it came from a personal email ID, not his official one.

Case 3*

Ranjita Kumar had been the Secretary to the Managing Director of Lal Pharmaceuticals, Mr. Karan Lal for ten years now. She was considered very trustworthy and Mr. Lal often sought her views on the business. One day, she got a call from Mr. Lal's personal phone, with the caller asking her for the account number pertaining to the employee welfare fund. The caller claimed to be Dharmesh Dutt, the HR head, who had accompanied Mr. Lal during a visit to their facilities in Ahmedabad. The latter, he claimed, had just finished a session with newly promoted managers and wanted to reward them financially for their ideas on collaboration and growth. Dharmesh also claimed he had a bad cold and sore throat and apologized to Ms. Kumar for sounding hoarse.

Ms. Kumar proceeded to give him not just the employee welfare fund account number, but also requested him to take a message for Mr. Lal on his new personal credit card details.

Imagine her shock when Dharmesh walked into the office half an hour later. When questioned, Dharmesh said Mr. Lal had wanted to visit Ahmedabad but not for a tour of their facility. It was to explore partnership options with some of the local businesses. He had changed the plan of interacting with new managers only the previous evening and told Dharmesh that it would be better if the new recruits flew down to the Mumbai head office next week for discussions. Thankfully, Ms. Kumar gained composure and informed Mr. Lal about her being conned. The police was informed and both accounts – the employee welfare fund and Mr. Lal's credit card, were blocked in time.

Avoiding social engineering fraud risks

In our experience, one of the effective ways to safeguard organizations from being impacted by social engineering fraud risks is by creating awareness among employees on data confidentiality and responding appropriately to fraudsters.

Some specific measures include the following:

- Develop a robust data classification regime that restricts data access to very few employees. Large organizations often restrict access to data around financial information, employee information, business plans and client details and any requests are internally screened and approved by a senior person. This way social engineering schemes cannot make much headway as confidential data remains unavailable to the vast majority of employees.
- Focused training programs – Organizations can segregate their employees into different user groups based on the information they are privy to such as those in the procurement function, finance and accounts staff, customer relationship team, sales team etc. Depending on the level of information these employees hold, focused training programs can be organized to help them recognize potential social engineering requests and avoid them. Further, any known instances of social engineering attacks can be shared throughout the organization to warn employees against responding to such requests. A leading best practice is to have the IT security team share this information alongside recommended actions.
- Conduct third-party audits on employees to ascertain preparedness to tackle social engineering scenarios.
- Institute a call back policy, wherever

*Note: All these cases, names and companies are entirely fictitious in nature and have been based on Deloitte's aggregated knowledge of social engineering fraud.

possible especially for customer support staff. This means asking the fraudster for his/her information on the initial call. This gives an opportunity for the organization to verify the credentials of the caller before sharing the necessary information.

- Subscribing to suitable and up-to-date protection tools which can block links to known malicious sites can prevent access at an enterprise level.
- Creating an 'Always Alert' culture – Social engineering attacks can be thwarted if employees are alerted to the possibility of such scams in advance and asked to keep watch. Some of the steps organizations take to build an 'always alert' culture is to recognize/reward employees who have demonstrated presence of mind to avert large scale social engineering scams, frequently running a campaign sensitizing employees to the risk of social engineering, and encouraging employees to speak up and admit if they have fallen prey to such a scam.

Organizations in India have lost several hundred crores by falling prey to social engineering schemes. Given the quantum of losses, organizations can no longer afford to relegate social engineering to the bottom of the fraud risk pile.

Contacts

For more information, please contact

Rohit Mahajan
APAC Leader
Partner and Head - Forensic
Financial Advisory, Deloitte India
T: +91 22 6185 5180
mahajan@deloitte.com

Jayant Saran
Partner
Forensic – Financial Advisory
Deloitte India
T: +91 124 679 3607
jsaran@deloitte.com

Sebastian Edassery
Director
Forensic - Financial Advisory
Deloitte India
Tel: +91 80 6627 6157
edasserys@deloitte.com

Deloitte.