CORPORATE SECURITY

SOCIAL ENGINEERING

It's not high-tech, but it's high dollar loss!

Social Engineering, as it is known within the Telecommunications Industry, is the art of utilizing interpersonal conversational skills to convince unsuspecting victims into forwarding fraudulent telephone calls through corporate America's telephone systems. The fraudulent schemes which have been in use by telephone service thieves for years, have in recent months shown a drastic increase among corporate customers.

These "social engineers" can be hackers, prison inmates or call/sell operators and the terminating locations can be domestic or international telephone numbers. The following are four of the more popular schemes currently utilized by these social engineers: (*keep in mind– there are an infinite number of ways that these thieves can talk a victim out of a dialtone)

SCHEME ONE

A caller will place a call into a company receptionist, generally via the company's 800 number, requesting to be connected to the customer service department. When the customer service representative answers, the callers gets the representative's name and then indicates that the receptionist has put his call to the wrong department. The caller then asks to be returned to the receptionist and when connected, assumes the identity of the employee previously called. The caller requests the receptionist's assistance in getting an outside line. Upon connection to an outside line, the caller places a fraudulent long distance call.

SCHEME TWO ***MOST COMMON***

A caller contacts a company receptionist posing as a telephone technician and requests assistance in checking for problems with the company's telephone lines. The caller requests that the receptionist dial 910333 (or 910XXX– depending on the carrier). This is the casual calling feature that allows the call to go out over a chosen carrier. If forwarded, the "9" provides the caller with an outside line and the 10333 allows the caller to either charge the call directly to the company through Sprint, or allows him to use a stolen telephone credit card. The caller can also utilize this scenario and ask to be transferred to extension 90xx which connects him to a long distance operator who then facilitates a long distance call. Another variation of this scheme is to ask to be connected to extension 9011. This allows the caller to get an outside line ("9"), then "011" allows the caller to direct dial to international locations.

It is not uncommon for telephone thieves to pose as executives of their respective companies and attempt to dupe unsuspecting employees, or a receptionist, into placing calls for them through the company's PBX.

SCHEME THREE

In this scheme, a caller from a foreign country calls a company which provides FAXBACK services for its customers. The caller then requests that a fax be forwarded to a foreign location. When the fax is sent, the call is manipulated so that it does not disconnect, resulting in a long duration international call. The caller perpetrating this fraud is paid a percentage payment in advance by the foreign carrier, based on calling volume generated by the scheme. The payment made to the caller is made prior to the foreign carrier receiving complaints about the illegal activity.

SCHEME FOUR

This scheme involves fraudulent companies and persons in foreign countries that page employees of companies in the United States, who in turn, call the international number on their pager. When the call is answered, the person in the foreign country acts as though he is very busy accepting calls, and asks the caller to hold. The scheme is designed to keep the caller on hold for as long as possible to raise the calling volume again. The company or individual in the foreign country again receives a percentage payment for the increased call volume from the foreign carrier.

The above four schemes are very basic and can be used in multiple variations, depending on what the thief is attempting to accomplish. **The one common characteristic in each of these schemes is that they are very effective!**

Unlike other forms of customer premise equipment fraud, the answer to prevention is not more hardware or software. The only way to stop this fraud is having well-educated employees who are familiar with these types of fraud schemes and refuse to be manipulated by these social engineers!
Discuss this with all employees who answer incoming calls. Have a plan of action in place if one of these thieves does call.

EMPLOYEE EDUCATION IS THE ONLY PREVENTION!