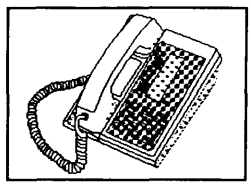
8-1992

Avoiding Telephone Fraud; Technology Alert, August 1992

Rosemary Zirille

AVOIDING TELEPHONE FRAUD

By Rosemary Zirille



AUGUST 1992

Ms. Zirille, a voice communications coordinator at Crowe Chizek & Co., an accounting firm in South Bend, Indiana discusses her firm's experience in avoiding telephone fraud.

Within one month after the installation of a new voice processing system within the firm, we were the victims of telephone fraud. We had installed both the voice processing system and all telephone systems in accordance with recommendations and instructions from the various vendors. And, while we were fortunate enough to detect and stop the illegal penetration quickly, the results could have proven disastrous.

As part of normal monitoring of the telephone systems in the firm, it was determined that an unusually high activity of outgoing calls were taking place tying up all of the outgoing telephone lines. About that same time, Crowe Chizek was notified by AT&T Network Corporate Security that hacker activity was taking place on our telephone system. At that time, our new voice processing system had been in place for one month. It was discovered that there were an excessive number of calls going through our system that were directed to Spanish speaking countries in South America. Being a midwest-based accounting firm, the quantity of calls destined for South America was highly irregular. After contacting the local police department and FBI, we then began acquiring additional information from AT&T and Octel to further secure our systems. We made several significant software changes to the telephone system and further restricted any type of off-net calling (dialing into the system, getting dial tone and dialing another number). We immediately removed the 809 area code from our system to disallow any calling to South America as a stop-gap effort to curtail the illegal activity (we have since discovered other methods to block only the illegal activity).

AT&T provided the detail from our telephone bills to the FBI for further dissecting. The FBI is attempting to check the locations of the phone numbers that placed the calls. Our experience is not unusual. A quick check of a few of our larger clients indicated that they too were victims of telephone fraud without even being aware of the abuse.

Since that time, we have learned a lot about telephone abuse and many better ways to prevent such an occurrence. The following is a list of recommendations and tips we have developed in order to safeguard our systems and our employees.

General Security

1. Shred information with telephone numbers or any corporate directory listings, rather than throwing them in the trash. This includes items such as fax sheets, electronic mail id's and voice mail passwords or lists.

   "Dumpster Divers" scour trash bins to obtain discarded company information that may include remote call authorization codes and other proprietary information.

2. Inform all employees that the person on the other end of a conversation may not be who he says he is. Many people misrepresent themselves as vendors and ask a lot of questions about your company and/or equipment that should not be given out.

   Normally, this is a thief who is trying to learn more about the employee's phone system in order to defraud the company, and pose as a legitimate contact.

3. If your wallet is stolen, be sure you report ALL the cards you have, especially your Telephone Credit Card, whether it be AT&T, Sprint, MCI, or Indiana Bell. This is a sure way to incur a large phone bill that **YOU** will be responsible for!!

4. Don't let a caller fool you, when they ask you for "Extension 9000". By transferring this call, you are providing them with a "free call" to the outside world. (9 gets you an outside line, and 0 gets you an operator).

5. If you receive a call back at the switchboard with your display indicating "ic", this is indicating an intercept call. If a number of these calls are received and result in hang ups upon answer or "sorry wrong number" explanations, you can be reasonably certain that unauthorized use of the system is being attempted (AT&T system).

6. When you are at a pay phone in an airport, bus , or train terminal, beware of those around you. There are hackers out there with tape recorders that will pick up the sounds from the telephone as you're dialing, which allows them to figure out your calling card number. They also are known to video tape as you dial the credit card number on the phone.

   Try to use those phones that are set up in a circular manner, rather than those lined up along a wall.

7. Be sure your call disconnects after you have completed the call. Many times, the card number stays in "memory" and the next person can make a call on "your" card. Pick up and listen for the dialtone.

8. Credit card scams - when a company calls you to verify your credit card number, don't verbally give it to them.

Voice Mail Security

1. If you receive any obscene calls in your voice mail box, notify your System Manager immediately.

2. If you find that you are unable to access the voice mailbox using <u>your</u> password, notify your System Manager.

3. If you are unable to access the voice mail system due to lines being busy or anything else, contact your System Manager.

4. For those voice mail users, we recommend using the maximum number of digits the system allows for your password. These passwords should not be written down anywhere, especially on your phone or posted to your terminal, nor should you use speed dialing with your password in it.

5. Passwords should be carefully selected so that they are not obvious (i.e. birthdate, social security number, phone number, part of your extension, same digits as 111111). Change your password frequently.

6. Utilize any security feature that is available on your mailbox.