Shaw Business

Voice Mail Fraud

If you don't change the default password on your voice mailbox, you, or your company, could be in for a big – and expensive – surprise. The Federal Communications Commission (FCC) has become aware of a form of fraud that allows hackers to use a consumer's or business's voice mail system and the default password to accept collect calls without the knowledge or permission of the consumer.

The Scam Works Like This:

A hacker calls into a voice mail system and searches for voice mailboxes that still have the default passwords active or have passwords with easily-guessed combinations, like 1-2-3-4. (Hackers know common default passwords and are able to try out the common ones until they can break into the phone system.) The hacker then uses the password to access the phone system and to make international calls. The hacker does this by first changing the voice mailbox's outgoing greeting to something like "Yes, yes, yes, yes, yes, operator, I will accept the charges." Then, the hacker places a collect call to the number they've just hacked. When the (automated) operator (which is usually programmed to "listen for" key words and phrases like "yes" or "I will accept the charges") hears the outgoing "yes, yes, yes, yes, yes, operator, I will accept the charges" message, the collect call is connected. The hacker then uses this connection for long periods of time to make other international calls.
There is also another twist to this scam. A hacker breaks into voice mailboxes that have remote notification systems that forward calls or messages to the mailbox owner. The hacker programs the remote notification service to forward to an international number. The hacker is then able to make international calls.

What to Beware of:

- Hackers usually break into voice mail systems during holiday periods or weekends, when callers will not be calling; thus, the changing of the outgoing message goes unnoticed.
- Hackers are typically based internationally, with calls frequently originating in and/or routed through the Philippines or Saudi Arabia.
- Businesses that are victimized usually find out about the hacking when their phone company calls to report unusual activity or exceptionally high phone bills. (The fraud usually occurs on business voice mailbox systems, but consumers with residential voice mail also could also become targets.)
- Consumers who are victimized may find out about the hacking when they receive unusually high phone bills.

What You Should Do to Prevent This Risk:

To avoid falling prey to this scam, the FCC recommends voice mail users do the following:

- always change the default password from the one provided by the voice mail vendor;
- choose a complex voice mail password of at least six digits, making it more difficult for a hacker to detect;
- change your voice mail password frequently;
- don't use obvious passwords such as an address, birth date, phone number, or repeating or successive numbers, *i.e.* 000000, 123456;
- check your recorded announcement regularly to ensure the greeting is indeed yours. Hackers tend to attack voice mailboxes at the start of weekends or holidays;
- consider blocking international calls, if possible; and
- consider disabling the remote notification, auto-attendant, call-forwarding, and out-paging capabilities of voice mail if these features are not used.