

Protecting Your Voice Mail System

Why would anyone want to listen to my boring messages anyway? Organizations go to great lengths to protect their computer systems, but don't always take the same precautions with their voice mail systems.

Voice mail security is more than preventing "hackers" from eavesdropping on someone's messages. It means protecting your system against fraudulent long distance charges, corporate espionage, and malicious system intrusions. By recognizing the different types of hackers and the trails they leave, you can protect your system and possibly even catch the culprit.

The best known hacker is a joy rider, who simply enjoys the challenge of breaking into a voice mail system. But other types of hackers have more nefarious motives.

Some break into systems to steal confidential company information or sales leads; this type of hacker usually works for a business competitor, and breaks into specific mailboxes. Others, like former employees, may break into mailboxes to leave nasty messages, or try to wreak havoc on your system for revenge.

Another type of hacker wants to use your system to set up an illegal business, like credit card fraud or selling drugs. These hackers try to access system administration controls in order to set up ranges of mailboxes outside of existing system parameters. They are often sophisticated, and can easily become entrenched before they're noticed.

Finally, there's the toll fraud hacker, whose only interest is dial tone. He or she will use your voice mail system to access your outgoing lines. The long distance calls made by such a hacker could result in thousands of dollars in fraudulent charges before the hacker is caught.

Prevention is your most effective weapon against voice mail hackers. In fact, almost all can be deterred with a combination of common-sense policies and procedures that involve better system design and administration, subscriber education, and effective company voice mail policies and guidelines.

System level security

Intelligent system design and maintenance can go a long way towards preventing most security breaches.

Probably the most important way to prevent hackers is regular and diligent system checks. Establish procedures and make reviewing system and network reports to identify hackers a regular part of system management - and don't think it's okay to skip a week!

Take advantage of your system

Voice mail manufacturers have many security features already built into their systems. Check to see which features your system has - and implement them today.

- Easy-to-change subscriber passwords.
- Automatic random password creation for new mailboxes. Otherwise, use random, six-digit -or longer passwords for new subscribers.
- A flexible password structure that allows the degree of security you need (for example, 10-to 20-digit passwords for system access).
- Reports on system activity and password access for unused mailboxes and multiple incorrect password attempts.
- Regular system backups, in case you need to recover data.
- Built-in/adjustable limits on the number of password attempts - we recommend limiting the number of consecutive unsuccessful log-in attempts to three or less. Some systems will even automatically "lock" a mailbox after a certain number of wrong password attempts.
- Ability to change system default password on installation.
- Ability to reset a subscriber's password to lock out a hacker.

Set up your system properly

- Locate your voice mail system in a room with controlled access.
- Make sure system access passwords and passwords for special applications aren't trivial or easy to guess.

Limit access to your system

- Control the number of mailboxes hackers can access. Don't create mailboxes before you need them, and never set up mailboxes with passwords that match the mailbox number.
- Establish multiple access levels for subscribers, system managers, system programmers. Require passwords for each level of access.
- Customize each subscriber's level of access through class of service.
- Manage your long distance capabilities: disallow or restrict calls to long distance numbers through the voice mail system. Don't allow any access to outside lines through an automated attendant or if you have 800 number access to voice mail.
- Limit voice mail ports to internal calling or restrict out-bound calls to certain numbers

Use system reports and network information to deter and find hackers

- Monitor system reports to identify:
 - Bad-password disconnects.
 - Mailboxes that aren't being used and delete them - but check with the assigned subscriber first!
 - Unusual after-hours system activity.
- Run full system reports regularly - and go beyond the range of mailboxes you've established to detect hackers who may have set up new mailboxes.
- Monitor access to your system's dial-up maintenance port.
- If you use an 800 number, or have ANI (Automatic Number Identification), check long distance reports to make sure you're not receiving excessive calls from the same phone number.

Company security

We recommend that every organization develop security guidelines that fit with its culture and management style. How guidelines are implemented is up to individual organizations, but TMIA strongly recommends these steps to deter or catch security breaches.

Train your employees

- Develop voice mail security policies and distribute them to all employees.
- Include security policies as part of your voice mail training classes.
- Make sure operators and receptionists are security conscious and won't transfer callers to an outside line.

Common-sense policies

- Establish well-controlled procedures for resetting passwords.
- Limit features like outcalling, message delivery, guest mailboxes, and access to the PBX via the voice mail system to specific company requirements and monitor the use of such features.
- Change system access passwords regularly and only issue them to authorized personnel (two or three at most).
- Consider the pros and cons of having subscribers regularly change their passwords. If subscribers change passwords monthly, they will sometimes end up with passwords that are easy to guess, like the current month. In some cases, your system might be more secure if subscribers establish passwords that are very difficult to guess and stick with them.

Everyone contributes to system security

The more educated and aware each subscriber is, the more secure your entire system will be. Here are some tips for subscribers:

- Guard your password - it's as important as your bank card PIN!
 - Change your assigned password the first time you log into the system.
 - Never program your password into speed-dial keys on your phone.
 - Never write down your password or give your password to others.
- Use long passwords - at least six digits.
- Report any unusual messages or mailbox activity to your system administrator.
- Don't make your password obvious, such as your department, your birthday, your nickname, or your child's name!

If you suspect a hacker has gotten into your system...

1. Change all system access and passwords immediately. Ask subscribers to change their passwords, too.
2. Check system reports for unusual activity, especially after hours. Hackers tend to remain on the system longer than subscribers.
3. ANI is very useful for tracing hackers. Check reports for calls to the system from numbers not associated with your business or personnel.
4. If you think a hacker is using your outside lines, immediately restrict PBX access and check your long distance records.