# PBX Fraud Information

**Increasingly, hackers are gaining access to corporate phone and/or voice mail systems. These individuals place long distance and international calls through major telecom networks using local systems. Your business could be a victim of this type of fraud and would be responsible for all phone charges. Many business customers have not kept existing systems secure, or, have other vendor-based support that could pose a security threat. As the owner of your phone system it is important that you take measures to ensure proper security. We have created this document to help you protect your business from fraud.**

## Telephone Hackers Hit Where It Hurts: Your Wallet

Telephone hacking is unauthorized or fraudulent activity through a telephone system and can potentially cost businesses significant amounts of money and resources. Usually the owner of the PBX isn't aware it's happening until an enormous bill from their toll provider arrives or malicious events start occurring via their phone system. Unfortunately the owner of the telephone system is responsible for toll charges, not the provider.

## Why do these activities occur?

Telephone hackers can infiltrate vulnerable PBX systems to make international and long distance calls, listen to voice mail, or monitor conversations. Victims of hacked PBX systems unknowingly allow the hackers to "sell" the use of their telephone system to others or provide the hackers with an opportunity to maliciously reprogram the system.

## How do they do it?

Typically hackers gain unauthorized access through the PBX's maintenance port, voice mail (if voice mail can be accessed remotely) or the Direct Inward System Access (DISA) feature of a PBX. Some hackers call in on toll free lines intended for customer use; some use stolen calling cards; and some will even impersonate someone else to social engineer their way into your system.

Most PBXs today are software driven and, when configured improperly, can allow hackers to access the system remotely. PBX administrators usually manage the system using a PBX maintenance port by interconnecting from their remote service centers via a modem. By controlling this PBX maintenance port, hackers can change the call routing configuration, alter passwords, add or delete extensions, or shut down a PBX, all of which adversely impact business operations.

# PBX Fraud Information

Some voicemail systems can be accessed remotely and programmed to make outbound voice calls. The hacker will search for voice mailboxes that still have active default passwords or have passwords with easy sequence combinations; i.e., 123456. Hackers use the outbound calling feature to forward calls to a "phantom" mail box that will give a dial tone. This allows them to make domestic or international calls from anywhere on your business account at your expense. Hackers can also gain access to your mailbox to listen to your messages, change your greeting or delete your messages.

DISA is a feature enabling remote users access to an outside line via a PBX with authorization codes. This is a very useful feature for employees who are on the road a lot or who frequently make long distance calls or international conference calls after business hours. By gaining access to this feature, hackers can access an outside line and make domestic or international toll calls at the expense of your business.

## How will you know if hackers are/have been in your System?

You may notice lights on phone lines that are lit up without anyone using the phone system. You may also be notified by your toll provider that there is suspicious/unusual usage associated with your phone numbers. Unfortunately though, you may only find out you have been hacked when you receive a bill for international calls made from one or more of your lines that were not dialed by anyone in your company.

## What can you do about it?

As the owner of a telephone system, it is your responsibility to secure your system to prevent unauthorized access. Having a properly secured telephone system is the best way to prevent telephone hacking and mitigate the potential damage and resulting costs to your business. The following are some industry best practice guidelines that, if followed, could help reduce the risk of telephone hacking. You may have to consult your equipment vendor to assist in securing your system security efforts.

# Best Practices for Securing Your PBX System

## Education

1. Familiarize yourself with the dangers of telephone hacking and the financial exposure you have to your toll provider. Remember, it is you as the owner of the telephone system who is liable for fraudulent usage and associated toll charges, not your toll provider.
2. Educate staff that utilize your PBX on security procedures and ensure they have an appreciation for the importance of adhering to set procedures.
3. Establish after-hours contact protocol so that appropriate personnel can be notified in a timely manner.
4. Take time to evaluate your current settings and disable any features that are not in use.

## Authorization Code/Password

1. Do not use any preconfigured default codes and passwords. Be sure to change those default settings as soon as possible after the PBX is installed and update them regularly.
2. Choosing complex, random passwords of at least six to eight digits, will make it more difficult for a hacker to detect.
3. Don't use obvious passwords such as address, birth date, phone number, or repeating or successive numbers, i.e. 000000, 123456. Don't use sequential, ascending or descending numbers or any part of the telephone number for your passwords.
4. Force password and authorization code changes for employees periodically.
5. Ensure that only trusted system administrators know the administrator password and be sure to change passwords quickly after any staffing changes. Eliminate the advertising or publication of default passwords.
6. Do not keep extensions active for former personnel or positions. If there are staff changes cancel the associated extension, including any associated features, access rights (i.e. LD/IDD) and codes and passwords.

## DISA

1. Limit the DISA access number and authorization codes to only employees that have a real need for such a feature.
2. If possible, ensure the first few digits of the access number for DISA are different from the voice line.

# Best Practices for Securing Your PBX System

## Voice Mail

1. Disable the external call forwarding feature in voice mail, unless it is absolutely required.
2. Remove any inactive mailboxes.
3. 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.
4. Consider disabling the remote notification, auto-attendant, call-forwarding and out-dialing capabilities from voicemail if these features are not used.

## Toll Calls

1. Consider restricting international or long distance destinations to which your company does not require access. Restrictions should also include 1-900 calls and 1010 casual dialing within the PBX/Voice Mail system. While you can request this of your phone company, you should also set these restrictions up in your phone system.
2. Regarding international blocking: it is important to understand that if your provider blocks international calls, this will not block calls to certain locations outside the U.S. but still within the "North American Numbering Plan" (i.e. they have an area code and are dialed like any other toll call. These locations include Canada, Puerto Rico, US Virgin Islands and other Caribbean countries such as Jamaica and the Bahamas. Fraud to these countries is on the rise, and the best way to prevent them is a secure system and strong passwords. For a current list of NPAs in the North American numbering plan, visit www.nanpa.com/area_codes

## Extensions

1. When an extension is no longer required, it should be canceled, along with associated features and access rights such as outbound toll and international dialing.

## Ongoing Monitoring

1. Familiarize yourself with your company's call patterns and monitor them regularly.
2. Look for any suspicious call activity after hours, including weekends and public holidays.

## Equipment Room Access

1. The PBX system should be kept in a secured location to which only authorized users have access.
2. Verify any technicians' identity that requests access to your PBX equipment.

# Additional FAQS

### When I get hacked, who is going to pay for the calls?

Your business, not your Long Distance Carrier, is responsible for all charges incurred on your system due to fraud (including toll fraud), abuse, or misuse of services, whether known or unknown, and whether or not your Long Distance provider takes any actions to stop or block Toll Fraud. **The responsibility for the security of your PBX system is yours** and you should take steps to protect your assets.

### Why don't the carriers write off these charges?

Today, fraudulent calls are placed over many different inter-exchange carriers (IXCs); each carrier must pay that portion of the call handled by them. When the call is placed to an international location the domestic carrier must pay the foreign carrier regardless of the fraud. You, the end user, control access to your PBX system, not your telecommunication provider, so you are responsible for the charges incurred.

### Why is identifying or stopping the fraudulent calls the customer's responsibility?

Only the customer can differentiate legitimate calls from fraudulent ones. The carriers do not have access or permission to work on your PBX, the vehicle that hackers use most to conduct their activities.

### How will the hacker find my system?

Criminals pay for a PBX maintenance port number and password. Hackers "scan" using auto-dialers to find systems equipped with modems. Your company's telephone directory listing or your toll free service advertising make you
known to the hacker.

### How do I justify the expense of corrective action when we have not suffered a loss?

Past performance is not an accurate indicator of present threats. The equipment and the motivation to perpetrate this criminal activity did not exist years ago. Educate your managers about the pitfalls of not protecting your corporate assets and enlist their support by implementing a corporate policy on unauthorized access as your first step.

### How do hackers know which PBX type and brand of Voice Mail we own?

Hackers identify the type of PBX by the Login procedure used for each system. They know the pass codes for each vendor PBX. Hackers also recognize the various Voice Mail and Phonemail systems by the default digitized voice recordings.

# Additional FAQS

### We are a small business, why should hacker activity concern me?

Hackers use auto-dialers to search entire area codes to find systems to hack, they do not care who or where their victims are located. No one is safe and smaller companies may be less able to absorb the average loss ranging from $10,000 to $100,000.00 plus dollars per incident.

### What can we do to protect ourselves from these crooks and con artists?

As with your personal life, the better informed you are the better protected you are from the risks. Stay on top of the current threats, establish and follow a policy on security, secure your system configuration, setup a team approach to security and service, and work with your equipment vendor. Do not let management or your business be taken by surprise. This is one disaster that is very predictable and equally preventable. Remember that you will be a victim and that you, and only you, control the severity of these attacks. It is much easier to prevent an attack than to recover your system from hackers.

---

**TDS Reminder:** Businesses with privately owned voice systems are responsible to ensure the devices are properly secured before activation AND are responsible for all charges incurred through the system. It is recommended to contact your Voice Mail or PBX vendor to have your system evaluated by a professional and take the necessary steps to prevent against possible fraud.