PBX Fraud Educational Information for PBX Customers

Telephone Hackers Hit Where It Hurts: Your Wallet

Telephone hacking is unauthorized or fraudulent activities that can affect your telephone system, and potentially cost your business significant amounts of money and resources if they occur. Unfortunately most of the times the owner of the PBX isn't aware of the "hacking" until an enormous bill from their toll provider arrives or malicious events start occurring via their phone system.

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.

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

Some voicemail systems can be accessed remotely and programmed to make outbound voice calls. Hackers make use of this feature to forward calls to a "phantom" mail box that will give a dial tone, allowing them to make calls from anywhere, on your business account. 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 to access 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 need to access international call conference after business hours. By gaining access to this feature, hackers can make access on an outside line and make tolled calls at the cost of your business.

What can you do about it?

Having a properly secured telephone system is the best way to prevent telephone hacking and mitigate the potential damage and cost that could be incurred by your business as a result. The following are some industry best practice guidelines that, if followed could help reduce the risk of telephone hacking.

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.
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 timely.
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 default codes and passwords that come preconfigured. Be sure to change those settings as soon as possible after the PBX is installed and update them regularly.
2. Choose random, lengthy passwords.
3. Force password and authorization code changes for employees periodically.
4. Ensure that only trusted system administrators know the administrator password and be sure to change passwords as soon as possible after any staffing changes.
5. Do not keep extension 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.

Voice Mail

1. Disable the external call forwarding feature in voice mail, unless it is absolutely required.
2. Remove any inactive mailboxes.

Toll Call

1. Restrict access to international or long distance destinations to which your company does not require access. Restrictions should include 1-900 calls.

Extensions

1. When an extension is no longer required, it should be canceled, along with associated features and access rights such as LD/IDD.

Ongoing Monitoring

1. Familiarize yourself with your business' 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 Information on Fraud Protection

Provided courtesy of PAETEC

Preventing Phone Fraud at Your Home or Business

- Don't accept collect calls from people you don't know. By accepting a call, you have agreed to pay the phone charges.
- Block third-number billing to your phone number. Third-number billing allows you to bill calls you make from other phones to your phone number, but it is also a potential source of phone fraud. If you have a calling card, it's a good idea to block all third-number calls.
- Watch out for individuals claiming to be law enforcement or telephone companies who ask you to accept collect calls or third-party calls as part of an investigation or telephone repair/analysis project. Legitimate law enforcement and telephone officials will never ask you to accept collect calls or third-number charges. If anyone asks for sensitive information as part of an "investigation," be wary. Don't provide any information and report the activity to the alleged agency or company. Either use the telephone number printed on your statement or look up the inquiring agency number in the telephone book.

Preventing PBX & Voice Mail Fraud

A PBX, or Private Branch Exchange, is a telephone switch usually located on your premises. It provides communications between individual users and the public switched telephone network. A PBX is often paired with a voice mail messaging system.

A PBX or voice mail hack occurs when hackers discover a hole in the security of the telephone system. The hackers take advantage of that hole by generating calls that they have no intention of paying for. Instead, calls are billed to the organization using the PBX or voice mail system.

What can you do to protect your business?

- Contact your equipment vendor immediately and have a proactive discussion on PBX and voice mail security.
- Deactivate unused features and mailboxes.
- Change default passwords for users and administrators and increase the length of passwords. Restrict login attempts.
- Restrict message notification or out-dialing on voice mail boxes.
- Block operator services or international access as appropriate.
- Block casual dialing from the PBX: 101XXXX and 1010XXX.
- Add verified account codes for international dialing.
- Review the call detail on monthly invoices and report anything suspicious.
- Invest in call accounting software or station message detail recording to review internal extensions for abnormal activity.
- Do not allow remote access until confident it is secure.

Do you have VoIP equipment?
If your customer premises equipment is improperly configured, it is possible that unregulated inbound SIP traffic will pass through your IP network/PBX and out of your SIP trunk group. This can allow Internet-based hackers access to local dial tone from the IP PBX/SIP trunk group without your knowledge.

- Contact your equipment vendor about running a security audit of your IP and voice mail systems.
- Check the status of your firewall and/or other call processing software for errors or manipulation of setup.
- Verify the configuration of your IP PBX to ensure that WAN traffic is isolated from SIP Trunk solution.
- Block Internet WAN traffic from accessing the gateway via SIP (Port 5060) for TCP and UDP.

Social Engineering

In the communications industry, a Social Engineer uses his or her conversational skills to trick an unsuspecting victim into providing access to dial-tone or other information. Once dial-tone is received on the fraudster's end, calls can be made anywhere, for any length of time. The victim, usually a business owner, is left holding the bill.

Social Engineering happens in a variety of ways:

- A caller posing as an employee of the "telephone company" calls into the receptionist at ABC Company. He asks the receptionist for assistance in testing the line. He may ask to

dial 9, 0, #, and then hit the "connect" key on the telephone set. The 9 will allow him to get an outside line, the 0 will take him to the Operator, and from there he can call any destination, billing back to ABC Company. He may also ask to be connected to extension 90(X) and attempt to get an outside line that way.

- A caller calls into ABC Company and requests Customer Service. When Customer Service answers, he takes the name of that person and then says he was transferred to the wrong department. He asks to go back to the receptionist, and pretends to be the Customer Service representative asking for help getting an outside line. Once he gets the outside line, he places a fraudulent call, which is then billed back to ABC Company.
- Social Engineers can manipulate representatives of ABC Company into providing PIN numbers for calling cards, extension numbers, names, password information, telephone system information, or any information that would enable them to make a free phone call. This includes the ability to talk or trick a victim into accepting third-party billed or collect calls.

What can you do?

- EDUCATE! Tell everyone in your organization and then spread the word externally. Educating employees is the number one deterrent against successful Social Engineering.
- REPORT! Tell your Communications Manager and your Communications Carrier what has happened. In nearly all cases, the calls originate from a payphone or unknown numbers. Although the fraudster is often impossible to find, Carriers are pooling information in an effort to combat fraud and prosecute the perpetrators.
- PREVENT! Make changes in your telephone system that may prevent access to well known fraud destinations. You can request an international block from your carrier or certain country code blocks from your telephone equipment vendor. Operator Services can be blocked at the local carrier level to avoid unauthorized charges made through the Operator Service Provider.

Call your vendor and inquire about the security of your current system: Is there access from the outside world into your system or voicemail? Are all systems password protected? Have default passwords been changed? Are features not in use turned off, such as out dialing? Are all vacant voice mailboxes deleted? Read your telephone bills! Inquire about suspect activity to international countries or calls placed outside normal business hours.

Internet Dialer Fraud, Modem Hijacking, or Internet Modem Switch Fraud

Internet dialer fraud, also known as modem hijacking or Internet modem switch fraud, occurs when a "Dialer" software program is downloaded without your knowledge from an Internet site to your computer. Such a dialer is designed to disconnect your current Internet connection and dial out to a different, reprogrammed number. Often the numbers dialed from your computer are expensive long distance, international, or 900 numbers.

Several things may occur if an attempt to establish a connection is made:

- A dialer box pops up on your screen and indicates that it is dialing when you did not direct it to.
- Your computer makes an audible noise like it is trying to reconnect.
- The current site you are browsing doesn't respond to your commands and freezes up.

If you are a victim of Internet dialing fraud or modem hijacking, the FTC offers a complaint form at www.ftc.gov, or contact the FTC toll-free at 1-877-HELP (1-877-382-4357

begin_of_the_skype_highlighting 1-877-382-4357 FREE end_of_the_skype_highlighting). The FTC works with consumers to prevent fraudulent practices and will enter the information into a secure online database that is available to law enforcement agencies in the United States and abroad.

You may be able to prevent this type of fraud by taking these steps:

- Have international and 1010 dial around blocks placed onto your phone line if you do not normally need to dial these types of calls. These blocks may not be available in all areas.
- Remove your telephone line from your modem when you are not actively using your computer. Shut off your computer when it is not in use.
- Increase the security settings on your operating system software and install a firewall.
- Be cautious when surfing the Internet or closing pop-up boxes especially if it indicates "no credit card is needed" or a product or service is "free".
- Install and run up-to-date anti-virus software and spyware removal tools.

Preventing Calling Card Fraud

- Make sure no one is watching you enter your calling card number or listening as you give your number to an operator. If a "shoulder surfer" sees or hears you enter your card number and PIN (Personal Identification Number) on a pay phone, you may become the next victim of fraud. Block the view of the keypad and speak directly into the phone. When possible, use a phone that reads your card automatically.
- Do not use your calling card as an identification card. Use your driver's license or some other form of ID.
- Memorize your calling card and PIN number. Select a PIN that you can easily remember. Ask that your PIN not be printed on your card.
- Beware of anyone who calls you requesting calling card verification. Telephone companies will NEVER call you to ask for your calling card number. Give out your card number ONLY when placing a call through an operator.
- If you do not make international calls, request a calling card for domestic use only.
- Report a lost or stolen card immediately. Notify your calling card provider the moment you suspect your calling card has been lost, stolen or otherwise compromised.

Don't Get Slammed

Slamming is used by some long distance companies to enlarge their customer base by switching the subscriber's long distance carrier without the subscriber's consent or knowledge.

The Federal Communications Commission (FCC) has taken action against companies known to use slamming as it is an illegal practice. The FCC order clearly outlines requirements for the content and format of Letters of Agency (LOAs) in an attempt to reduce or eliminate unauthorized Primary Inter-exchange Carrier (PIC) changes. All rules apply to both residential and business PIC change requests.

In order to prevent your service from being slammed, simply contact your local telephone company business office and ask for a PIC freeze. A PIC freeze indicates that no carrier selection changes can be made unless you notify them by phone or in writing. Only when a customer has authorized a change in carriers is a change allowed to be made to the account.

Cramming

Cramming is when a consumer's monthly bill has charges for services or products the consumer did not order or authorize. Charges may be as low as a few dollars a month or as high as $50 a month. These charges often appear on a consumer's bill without warning.

Consumers are encouraged to contact their telephone company if they discover charges they didn't authorize. Many fall victim to cramming by signing sweepstakes forms or after placing calls to certain toll-free numbers. In addition, customers often fail to closely examine their phone bill and therefore pay the charges unknowingly. Charges not challenged are likely to continue. Consumers should examine their phone bills closely and contact their phone company to have any unauthorized charges adjusted immediately. If a customer is unsure of the charges appearing on their bill, phone company representatives can explain what charges are mandated and what charges are applied due to billing arrangements.