TOLL FRAUD POLICIES AND PREVENTION

What is Toll Fraud?

Toll Fraud is the theft of long-distance service. It's the unauthorized use of phone lines, services or equipment to make long distance calls. When businesses fail to maintain system security or have vendor-based support that's vulnerable to third-party access, fraud can occur. Hackers can gain entry to business voicemail and phone systems, placing international and domestic calls charged to your company – and leaving your business responsible for all phone charges.

Unfortunately, PBX system owners aren't typically aware of fraudulent activity until the bill arrives with unauthorized phone calls charged to the company. In addition, hackers may listen in on company phone calls or voicemail, accessing sensitive company information without detection. For these reasons and more, it's important to understand fraud, know how it occurs, and take action to secure your business phone and voicemail systems.

How Does Toll Fraud Occur?

There are numerous ways fraud occurs, but getting remote access to your voicemail and PBX phone systems by third parties are classic examples. Hackers may gain entry to your business phone system through the maintenance port of your PBX, through voicemail, through remote voicemail access, or via the DISA (Direct Inward System Access) PBX feature.

Since PBX systems are usually powered by software, misconfigurations in your system can leave your company vulnerable to hacker attacks. And because PBX administrators generally use the maintenance port to manage their company system, once hackers get control of this port they're in charge of the system. This means they can do a lot of costly damage -- from changing passwords to closing down your entire PBX system.

Fraud Prevention is Key

What can you do to stop fraud? The most effective way to eliminate fraud and its associated costs is through prevention. When businesses own their phone system, it's essential to be proactive by taking preventive measures that secure the system and help eliminate fraud. Some measures involve simple observation, like recognizing unusual phone activity or seeing unfamiliar numbers on your bills (especially international numbers). Other measures are more technical and involve shoring up system security.

As a telecommunications service provider, although we're not responsible for your network security or any fraud costs, we hope you don't have the misfortune to be a victim of fraud. For this reason, we recommend you take a few minutes to read through the following prevention information because it may protect your company from unauthorized access to your network and equipment that results in fraud. We strongly suggest implementing the strategies below to help ensure your network and equipment security.

Overview

1. Understand the dangers and high-cost of phone fraud and hacking. As the owner of your phone system, you are liable for all fraudulent usage and associated toll charges, not your service provider.

2. Know that one of the easiest ways to minimize toll fraud is utilizing call blocking.

3. Create an after-hours plan for quickly notifying the correct employees if hacking is suspected.

4. If you don't use remote notification, auto-attendant, out-paging capabilities, call-forwarding, or other such features, disable these options.

5. Don't use obvious passwords such as date-of-birth or numbers with repeatable patterns.

6. Check your mailbox greeting message regularly to ensure that it's yours.

7. Use authorization codes or complex passwords that are regularly changed; limit access and calling range after business hours.

8. Teach security procedures to employees using your PBX and stress the importance of compliance to these procedures.

9. Consult with your telephone system and voicemail vendors for additional guidance to prevent fraud.

Security Tips for TDM PBXs

1. Change the default (generic) security code, known as the administration security code that was set up by the vendor for your PBX system. The generic codes listed for specific PBX phone system makes and models can be easily found on Internet. Keep any default passwords confidential.

2. Password cracking software is routinely used by hackers to crack passwords. To help prevent intrusion, use random, complicated passwords and never reuse passwords. They should contain at least eight digits, numbers, letters, upper and lower case, and symbols.

3. Regularly update your company codes and passwords. Implement a schedule of mandatory authorization code and password changes.

4. Know your PBX/phone system configuration so you can spot irregularities. Don't share system information with unauthorized company personnel.

5. Quickly deactivate extensions, passwords, codes, and access rights for former employees and job positions.

6. Disable or change the default password for Direct Inward System Access (DISA) which allows callers to dial into the system, enter a code and get an outbound line. If the password parameter is "no-password", the DISA feature will provide dial tone, and calls will complete without a code.

7. Securely store or shred lists of PBX access numbers.

8. Establish a non-negotiable threshold for PBX system access attempts. Once the threshold is exceeded, require users to get administrator permission for access.

9. Install reputable anti-virus software and ensure your firewall is appropriately configured and is on at all times.

10. Schedule security audits. Routinely look for changes or errors in PBX configuration, call processing, router, and firewall.

11. Implement call blocking. Review Nextera's International Call Blocking policy. Add additional call blocking for domestic, Canadian, and Caribbean if calling to those areas not needed.

12. Require national and international long-distance calling account codes.

13. Monitor your PBX system with vigilance. Once you know your network's traffic patterns during peak usage, you'll recognize irregularities that indicate network intrusion.

14. Invest in call accounting software or security surveillance/monitoring software equipped with triggers. Establish threshold triggers that will set off alarms that notify you when security has been breached or unusual surges in traffic occur.

Security Tips for IP PBXs

1. Change the default (generic) security code, known as the administration security code that was set up by the vendor for your PBX system. The generic codes listed for specific PBX phone system makes and models can be easily found on Internet. Keep any default passwords confidential.

2. Password cracking software is routinely used by hackers to crack passwords. To prevent intrusion, use random, complicated passwords and never reuse passwords. They should contain at least eight digits, numbers, letters, upper and lower case, and symbols.

3. Regularly update your company codes and passwords. Implement a schedule of mandatory authorization code and password changes.

4. Know your PBX/phone system configuration so you can spot irregularities. Don't share system information with unauthorized company personnel.

5. Quickly deactivate extensions, passwords, codes, and access rights for former employees and job positions.

6. Disable or change the password for Direct Inward System Access (DISA) which allows callers to dial into the system, enter a code and get an outbound line. Default codes are not difficult to crack and if the password parameter is "no-password", the DISA feature will provide dial tone, and calls will complete without a code.

7. Securely store or shred any PBX access number lists.

8. Implement break-in evasion algorithms supported by some IP PBXs to lock out extension or user accounts after a specified number of failed authentication attempts.

9. Harden your base operating system by disabling services on your PBX system that aren't necessary. For example, disabling unneeded services on an OS X system minimizes unauthorized access to your PBX system through an unused component.

10. Be proactive with patch management. Manufacturers often discover vulnerabilities to hardware and software after it's released. Update your system with all patches released by hardware and software manufacturers in a timely manner to ensure system security.

11. A web interface on VoIP handsets can permit easy access to PBX extension login credentials, creating the potential for another SIP device login to your PBX system with the same extension credentials. To help ensure security, completely disable the web interface after your handset has been manually provisioned.

12. Discourage hackers from using your extension to route third-party calls by limiting the number of active SIP sessions for each extension. If more than several sessions are open at once, your system is vulnerable and inviting to hackers.

13. To ensure phones can't be remotely accessed by external users, implement private IP numbering schemes for your IP-PBX and all handsets.

14. Use dedicated servers for your PBX system to reduce vulnerabilities that can occur when PBX servers are shared with web servers. Private PBX servers eliminate the opportunity for hackers who use web applications to attack or access your PBX.

15. Deploy a host-based network intrusion detection system that allows host administrators to discover network security breaches and resolve issues before they can escalate.

16. Install reputable anti-virus software and ensure your firewall is appropriately configured and on at all times.

17. Schedule security audits. Routinely look for changes or errors in PBX configuration, call processing, router, and firewall.

18. Implement call blocking. Review Nextera's International Call Blocking policy. Add additional call blocking for domestic, Canadian, and Caribbean if calling to those areas not needed.

19. Require national and international long-distance calling account codes.

20. Monitor your PBX system with vigilance. Once you know your network's traffic patterns during peak usage, you'll recognize irregularities that indicate network intrusion.

21. Invest in call accounting software or security surveillance/monitoring software equipped with triggers. Establish threshold triggers that will set off alarms that notify you when security has been breached or unusual surges in traffic occur.

Security Tips for Voicemail Systems

1. Change the default (generic) security code, known as the administration security code set up by the vendor for your PBX system. The generic codes listed for the specific voicemail system makes and models can be easily found on Internet.

2. Use random, complex voicemail passwords containing at least eight digits. Don't share your voicemail passwords with anyone, especially unauthorized personnel.

3. Regularly update your company codes and passwords. Implement a schedule of mandatory authorization code and password changes.

4. Understand the configuration of your voicemail system and disallow all features which allow remote access. Hackers who compromise a voicemail box will reprogram to a fraud destination number(s). They then use the feature, pager feature and/or zero out feature to place their fraudulent calls.

5. Delete voicemail boxes no longer in use.

6. Routinely check your voicemail greeting to ensure the message is yours, particularly before the weekend and holidays. Hacking often occurs during after-work hours and out-of-office days.

7. Implement call blocking. Review Nextera's International Call Blocking policy. Add additional call blocking for domestic, Canadian, and Caribbean if calling to those areas not needed.

Tips for Physical Security

In addition to ensuring technical security, it's also helpful to take steps that include physically securing your phone and voicemail systems.

1. Prevent intrusion by securing your phone room. Use either a lock or security system and work with your building manager to implement a security plan.

2. Know the technicians who visit your business and validate their credentials before sharing any information.

3. Employ general security measures that also protect you from phone fraud such as supervision of building access during weekends and holidays; monitoring employee use of building keys; and maintaining building security by using lighting, video cameras, and other security measures as needed.

Tips to Avoid Social Manipulation through Impersonation

Beware of anyone who pretends to be a technician from a phone company. How do you know? Use the information provided below to avoid fraud that's perpetrated by imposters who attempt to gain system access through manipulation.

1. If you aren't familiar with an individual who says they're from Nextera Communications (or any other phone company), quickly place a call to Nextera to verify their identity.

2. Unless the technician's identity has been thoroughly validated, don't share any company password or code information.

3. If an unverified representative of Nextera asks you to press certain digits on the phone keypad, refuse to do so. Certain digits and patterns allow hackers to place free long-distance calls, which would result in charges to your business.

4. Don't transfer callers to 900, 800, and 700 numbers because it's likely a fraud.

Tips for Modem Security

Modem hijacking may be used to make long distance calls from your computer that can be fraudulently billed to your phone number. Minimize modem hijacking by following the suggestions below.

1. Disable ActiveX.

2. Install anti-virus software and update regularly.

3. To be aware of all modem redials, turn up the modem volume.

4. When your modem's not in use, unplug it.

5. Only download content and software from trusted websites. If you aren't sure, don't download. Avoid sites that contain offensive or questionable content. This includes gambling, pornography, sites offering free movies, etc.

6. Don't allow pop-ups on your computer.

7. When you're not using your modem or computer, turn it off instead of setting it to sleep or hibernation.

8. Delete any unknown Internet dial-up numbers from your system.