TELNET

TelNet Worldwide

Tips for Preventing Telecom Fraud

Telecom fraud occurs when hackers discover a hole in the security of a telephone system and 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 that was compromised. Your business could fall victim to this type of fraud and would be responsible for significant phone charges generated, even though you did not make the calls. Learning about fraud, taking proactive steps to secure your systems and adopting preventative measures across your organization can help you avoid the risks most businesses face.

Watch for fraud and those who would take advantage of your service.

Hackers have highly sophisticated methods to gain access and use your service as their own, allowing them to rack up significant toll charges for which you would be responsible. As the owner of your phone system, it is your responsibility to take proper measures to secure your system and implement preventative practices. Here are a few ways to brace your business:

- ❑ **Be proactive**; discuss PBX and voicemail security with your equipment vendor and service provider.
- ❑ **Be aware and leery of unknown people asking your cooperation in testing the telephone line**. They are likely 'phishing' for technical information they can use. Probe the caller for information such as employee ID, supervisor's name, and a call back number. Most times telecom technicians can conduct tests without the customer's assistance. Occasionally if you have initiated a service order, change or other call into TelNet customer care, one of our service technicians may ask for your assistance in testing. Just be sure you know who is on the line for you.
- ❑ **Never transfer a call from a caller you're unsure of to an unknown number outside your PBX;** if you are unsure of the person's identity requesting the transfer, arrange a call back to that person's line.
- ❑ **Be alert to the overt signs of PBX abuse** such as repeated calls of short duration, unexplained increases in incoming or outgoing calls, sudden increases in 800 usage or changes in after-hours calling patterns. You may also see phone lines lit up when no one is using the phone system.
- ❑ **Educate employees** about the dangers of phone fraud and what they can do to help prevent it.
- ❑ **Contact TelNet immediately at 1.800.508.1254 to report any suspect activity.**

Call management tips

- ❑ **Block services you don't need that have a high risk of misuse** including 1-900 calling, operator services, international access and casual dialing (101XXXX and 1010XXX) as appropriate.
- ❑ **If you need international service, add account codes** for international dialing.
- ❑ **Carefully review the call detail** on monthly invoices and report anything suspicious.
- ❑ **Cancel/remove extensions that are no longer required**, along with their associated features and access rights such as outbound toll and international dialing.

Notes regarding international service blocking:
if TelNet or another provider blocks international calls, calls to certain locations outside the U.S. that are within the North American Numbering Plan (i.e. they have an area code and are dialed like any other toll call,) may not be blocked. Locations include Canada, Puerto Rico, US Virgin Islands and other Caribbean countries. Fraud to these countries is on the rise, and the best way to prevent them is a secure system and strong passwords.

Also note that if TelNet or another provider blocks international calls, your business may still fall victim to fraud and will be responsible for usage charges should fraud occur.

Securing your passwords/authorization codes

Managing and securing passwords and authorization codes is a critical practice in preventing fraud. To bolster your password protection:

- ❑ **Delete all authorization codes that were programmed into your PBX for testing or servicing.**
- ❑ **Change default passwords** often for users and administrators.
- ❑ **Increase the length of passwords and require a mix** of upper/lower case letters, non-sequential numerals and special characters.
- ❑ **Select random codes** – don't use phone numbers, employee IDs, birthdays, addresses or other common numeric sequences.
- ❑ **Restrict number of login attempts** before requiring a password reset.
- ❑ **Assign codes on a need-to-know basis**, advising employees to treat codes as they would credit card numbers.
- ❑ **Require employees to change passwords frequently.**
- ❑ **Promptly delete unassigned access codes**, especially those used by former employees.
- ❑ **Shred any directories and business cards that list PBX access numbers** before placing them in the trash.

TELNET

Securing your phone system

- ❑ **Tailor access to your PBX to the needs of your business.** Block access to international numbers your company does not call, or consider using "time-of-day" routing features to restrict international calls to daytime hours only.
- ❑ **Don't allow unlimited attempts to enter your system;** program your PBX to disallow access after the third invalid access attempt.
- ❑ **Deactivate unused features and voice mailboxes,** especially features related to remote access and forwarding calls.
- ❑ **Restrict equipment room access**: your PBX system should be kept in a secured location to which only authorized users have access. Verify any technician's identity that requests access to your PBX equipment.

Remote Access

A prime entry point for hackers is equipment or phone system configured for remote access. If practical, eliminate remote access to your PBX and replace it with telephone credit/calling cards for authorized personnel. If remote access is important, these additional suggestions may help you minimize your risk to fraud:

- ❑ **Limit the number of employees** who use remote access.
- ❑ **Use an unpublished number for remote access lines** instead of 800 numbers.
- ❑ **Consider programming your PBX to wait at least five rings before answering a call;** a delayed call response can provide added security.
- ❑ **Use a voice recording or silent prompt instead of a tone** as your remote access prompt; using a steady tone leaves your system vulnerable to automatic dialing programs.
- ❑ **Do not allow remote access until confident it is secure**.

Voice Mail

Voice mail is another popular hacker inroad. In addition to other fraud prevention practices, these tips may help secure your voice mail:

- ❑ **Disable the external call forwarding feature** in voice mail, unless it is required.
- ❑ **Check your recorded announcement regularly** to ensure the greeting is yours. Hackers tend to attack voice mailboxes at the start of weekends or holidays.
- ❑ **Restrict message notification or out-dialing** on voice mail boxes.

Additional tips to secure your Voice over IP or SIP Services

If your on-premise 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 voicemail 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 the SIP Trunk solution.
- ❑ **Block Internet WAN traffic from accessing the gateway** via SIP (e.g., Port 5060) for TCP and UDP.

How does TelNet help customers prevent fraud?

TelNet continues to invest in technology and processes to prevent fraud. Here are just a few ways we are helping keep our customers secure:

- **Monitoring our network and facilities 24/7** for early indication of any issues.
- **Using 'best practices'** in fraud prevention.
- **Notifying our customers** of suspect usage.
- **Providing information** and suggestions to customers so they can actively minimize their risks of fraud.
- **Cooperating with other carriers and law enforcement agencies** to investigate and prosecute hackers.
- **Saving money by detecting and blocking fraudulent calls**.

Make fraud prevention a priority.