Nsight® TELSERVICES

# Protect Your Business *from* Toll Fraud

**> Worldwide, phone equipment hacking is consistently one of the main reported computer crimes.**

**> Businesses who are the victims of international calling fraud can incur.**

**> Toll fraud can negatively impact productivity and profits.**

### WHAT IS TOLL FRAUD?

Toll fraud refers to a hacker breaking into and accessing a company's telecommunications system and then making long distance calls or selling long distance and/or international telephone time to third parties. Hackers can also listen to voicemail, monitor conversations, and reprogram the company's phone system.

### WHY DO HACKERS TAKE OVER A PHONE SYSTEM?

When a phone system is unsecure, hackers can gain access to trunk lines and begin generating as many calls as possible to high-rate international premium services (the equivalent of 900 numbers in the U.S.), where customers are assessed a per-minute fee on their phone bill for the services. The hackers use the calls to generate revenue.

### HOW DO THEY GAIN ACCESS?

According to the FCC, the hacker calls into a voicemail system and searches for voicemail boxes that still have active default passwords or have passwords with easily guessed combinations, like 1-2-3-4. Hackers are typically highly skilled phone engineers who know common default passwords and are able to try out the most common passwords until they can break into the phone system. A hacker can systematically work through a company's phone extensions and pass codes with the aid of dialing software. After uncovering a password, the hacker can access the phone system, change the voicemail's outgoing greeting and use the connection for long periods of time to make international calls.

In addition, a hacker can break into voicemail boxes that have remote notification systems that forward calls or messages to the mailbox owner. The hacker programs the remote notification service to forward an international number. The hacker is then able to make international calls.

### IS YOUR PHONE EQUIPMENT VULNERABLE?

It's most common for hackers to gain unauthorized access through the phone system's maintenance port or the voicemail system. If your voicemail boxes still have active default passwords or passwords with easy sequence combinations such as 1-2-3-4, you're at risk.

Unfortunately, businesses usually don't find out they have been the victim of hacking until their phone company calls to report unusual activity or an exceptionally high phone bill. As the phone equipment owner, you are responsible for all phone charges, including fraudulent activity.

### TAKE ACTION TO PROTECT YOUR COMPANY

Hackers look for potential vulnerabilities to exploit, making it imperative that companies put effective counter measures in place.

### WHAT TO BE AWARE OF:

- Hackers usually break into voicemail systems during holiday periods or weekends, when callers will not be calling. So if a hacker changes the outgoing message, it goes unnoticed.
- Hackers are typically based internationally, with calls frequently originating in and/or routed through the Philippines or Saudi Arabia.
- Businesses that are victimized usually find out about the hacking when their phone company calls to report unusual activity.

### NSIGHT TELSERVICES IS YOUR PARTNER

As your committed telecommunications partner, Nsight Telservices is committed to assisting customers in identifying suspicious calling patterns that may affect your operations and finances. For early detection, Nsight's Network Management Center (NMC) continuously monitors outbound international and domestic anomalies, trends and activity directed to and from known fraudulent areas and notifies customers of unusual activity. The NMC team also partners with members of the Communications Fraud Control Association, the Internet Crime Complaint Center and the Federal Communications Commission to monitor for fraudulent activity and changes in criminal behavior.

It's impossible to completely eliminate the risk of toll fraud, however, early detection and quick response can minimize the financial impact to your company. Nsight Telservices reserves the right to take the action(s) it deems necessary to reduce or eliminate fraud, however, as the telecommunications equipment owner, you remain solely responsible for taking any action necessary to reduce or eliminate fraud.

**Call Nsight Telservices (877) 463-8532 for more information or to schedule an appointment to review what protective steps would be the most beneficial and appropriate for your business.**

## How To Reduce Risk

**To avoid falling prey to an international calling scam, the Federal Communications Commission (FCC) recommends the following:**

### > BE KNOWLEDGEABLE

- Know what your financial responsibilities are if your company is the victim of hacking. If you are the owner of the phone system, you are liable for any fraudulent usage and associated charges.
- Educate all team members who use the phone system on taking the proper security measures.
- Establish a plan for how to respond to toll fraud.

### > STRONG PASSWORDS ARE THE GREATEST DEFENSE

- Never write down authorization codes and passwords or program them into auto dialers.
- Do not use default pass codes; change the codes as soon as possible after the phone equipment is installed and update the codes regularly.
- Limit who has access to the administrator password; only trusted system administrators should know the administrator password. Change passwords immediately after any staffing changes.
- Enforce password expiration dates to ensure frequent password changes; update passwords every 90 days.
- Do not use the same password for all phones or voicemail boxes.
- Passwords should be lengthy (at least six digits), random and complex; include characters, numbers and letters.
- Don't use obvious passwords such as an address, birth date, phone number, repeating numbers (i.e. 000000) or sequential ascending or descending numbers (i.e. 123456 or 654321).

### > CHECK VOICEMAIL

- Check your outgoing announcement regularly to ensure it is your recorded greeting.
- Disable the external call-forwarding feature in voicemail, unless it is a necessity.
- Remove any inactive mailboxes or extensions.
- Do not publish the remote voicemail access phone number or default voicemail password for your company.

### > RESTRICT ACCESS

- Restrict or prohibit access to international destinations that your company does not require.
- Limit international calling to employees who need to place international calls.
- Require an authorization code before an international call can be placed.
- Consider restricting when international calls can be placed; exclude evenings and weekends, when the highest incidence of hacking occurs.
- Block all calls to the 809 area code, which is a popular calling destination for hackers and resellers.
- If possible, block all international calling.
- Restrict 1-900 calls.

### > PROTECT TELECOMMUNICATIONS EQUIPMENT

- Ensure switch room and wiring closets are secure and periodically change the locks.
- Any documentation and reports that reveal trunk access codes or password information should be secured.
- Change administrative log-on passwords and access codes a minimum of four times per year.
- Change or remove authorization codes when an authorized user, such as a technician, leaves the company.
- Configure your telecommunications system to provide maximum protection.
  - Pre-program international telephone numbers to be called.
  - Program the system to terminate access after the third invalid attempt to log into the voicemail account.
- Confirm that your phone equipment vendor is able to change maintenance access passwords. • Only allow authorized individuals to contact your phone equipment vendor and make changes to your account.

### > KNOW YOUR SYSTEM

- Consider disabling features you don't use, such as remote notification, auto-attendant, call-forwarding, and out-paging capabilities of voicemail.
- Periodically re-evaluate your current settings and disable features that are not in use.

### > COMMIT TO ON-GOING MONITORING

- Familiarize yourself with your company's call patterns. Watch for an increase in after-hour calls, international calls made to countries you don't do business with, multiple short duration inbound calls (particularly those that occur outside of the work day) and incoming calls from suspect areas where phone hacking frequently originates.
- Schedule daily usage reports to monitor usage charges.
- Regularly monitor voicemail, automated attendant and 800 call detail records. Watch for numerous incoming calls coming in on your 800 lines followed by a surge in long-duration outbound 800 calls.

## What To Do In The Event Of Toll Fraud

### > IF YOU SUSPECT FRAUDULENT ACTIVITY HAS OCCURRED:

- Call Nsight Telservices at (877) 463-8532; our team will block further fraud attempts.
- Be prepared to share any information you may have regarding the toll fraud.
- Note any modifications made to the telecommunications equipment in an attempt to stop the toll fraud.
- Nsight Telservices will begin an investigation to identify the source of the fraudulent activity.

### > IF NSIGHT TELSERVICES IDENTIFIES A POTENTIAL FRAUD:

- If feasible, Nsight Telservices will block the offending traffic as it transits our network in an attempt to limit exposure to fraudulent charges while we take steps to notify the customer; this includes calling the customer to ensure contact has been made.
- Nsight Telservices also has agreements in place with our upstream carriers; if an upstream carrier identifies high-fraud probability traffic before Nsight's NMC, the carrier has permission to block the traffic and then notify Nsight Telservices. Nsight will then contact the customer directly.
- Nsight Telservices will begin an investigation to identify the source of the fraudulent activity.

## Liability

- It is the exclusive responsibility of the customer to prevent the occurrence of fraud.
- The customer is financially responsible for any charges incurred due to fraudulent activity.

**Call Nsight Telservices (877) 463-8532 for more information or to schedule an appointment to review what protective steps would be the most beneficial and appropriate for your business.**