Alternative TECHNOLOGIES

1050 Heinz Avenue, Berkeley, California 94710 • (510) 848-4411 • www.alternativetechs.com

STOP HACKING: Best Practices for Mitigating Risk of Telecom Fraud in On-premise Phone Systems

What is telecom fraud?

The most common type of telecom fraud is when unscrupulous people access your phone lines and place long distance calls, usually to other countries, which are billed to your account. There are often auto-dialers involved, and dozens of calls go through at once, racking up hundreds or thousands of dollars in charges very quickly. The bad news is that carriers will hold you responsible for payment.

How is telecom fraud committed?

The criminals are generally far away and are remotely accessing your phone service, whether digital or analog lines. To do that, they have to gain access to your phone system's programming and make changes that will allow calls to be placed that do not originate in your office. This is frequently termed "hacking."

What can be done to prevent telecom fraud?

If you want to protect a physical building against break-ins, you may install a tall fence and locked gate, put locks on all the doors and windows, and install an alarm. Similarly, the best way to protect your phone lines is to put up strong defenses at every layer of possible entry, which includes access to your office's computer network, routers, phone system (PBX), and phones. Additionally, there are steps you can request your carrier to take that will further protect against potential fraud. Of course, as with physical break-ins, a determined burglar may still breach your defenses, but there's no point in making it easy by leaving your doors and windows open.

* * *

The following pages provide concrete steps that your organization can take to mitigate the risk of telecom fraud. Starting with your carrier, then your own employees and IT professionals, and finally your telephone system itself – each of these pieces play a role in protecting your organization from telecom fraud.

What to request from your carrier

- Block international and collect calls.
- Block 900 and other toll numbers and casual calling (calling card or PIN long distance).
- Require account codes for long distance.
- If you have an 800 number, ask if your carrier can block calls from overseas to the 800 number.
- Request that your carrier block calls from known toll-fraud centers (carriers have lists of countries with highest frequency involvement in toll-fraud schemes).
- Ask for alerts for unusual activity.
- Discuss whether it's worth live-monitoring of phone activity on the circuit.

Steps to take within your organization

- Educate your staff on the real financial risk that is posed by lax telephone security.
- Work with your IT person to create protocols to maintain the security of your computer network and phone system.
- Limit access to your network and phone system. Keep information about the system secure. Use strong and unique security codes for admin access to your phone system. Don't use the same code for multiple purposes around the office.
- Require unique security codes for all voicemail boxes.
- Have a standard way of dealing with a departing employee's voicemail and network access immediately upon their departure.
- Change passwords immediately after a staff change.
- If you have phones for non-employees (volunteers, guests, clients), limit the types of calls that can be made from those extensions.
- Don't set up mailboxes for extensions unless they are monitored daily.
- Eliminate unnecessary mailboxes.
- Educate your staff about "social engineering" hackers who try to talk their way into getting information about your system.
- Do not share information about your system with unauthorized people.
- Be sure that your phone system is secured behind a recommended internet firewall.
- Schedule regular phone system checks and software upgrades.
- Keep your phone system and network equipment room locked.
- Verify each technician's identity before allowing access to your phone system or network equipment.
- Consult with your phone system vendor (that's us, Alternative Technologies!) about what features are available in your system that might pose a vulnerability, and disable all features that you don't need.
- *For number-only passcodes, follow these guidelines:*
  - Nothing incremental or sequential: 1234, 9876, 2468.
  - No all-same characters: 0000, 1111.
  - Do not match to extension or direct number.
  - As long and as varied and as unpredictable as possible.
  - Change regularly (at least every 90 days).
  - Never use default codes that come pre-configured with any service.

What to request from your IT professional

- Install a recommended internet firewall, properly configured.
- Limit outside access to computers on your network through the firewall.
- Remote phones should connect to the main phone system via a secure route.
- Ask your IT person to run periodic security audits to check for vulnerabilities.
- Talk to your IT person about the security of passwords for accessing your network, including guest passwords for your wireless network.
- Talk to your IT person about best practices for network security.
- Remember, the phone system control unit (PBX) is a computer on your network and should be kept as secure as your other computers.

What Alternative Technologies can do for your organization

NOTE: Some of these are actions we do at the time of installation, or may have done on subsequent visits if your system is older. Some items you will need to request from us. We are happy to discuss any of these actions with you.

- Set up secure codes for PBX maintenance/admin access (no manufacturer defaults, no easily-predictable codes).
- Limit access to maintenance/admin ports.
- Prevent or restrict outbound calling from the voicemail.
- Eliminate unused extensions and unused voicemail boxes.
- Block all outbound calling to particular area codes and country codes (particular extensions can be set up to override the restrictions and permit calls).
- Disable call-forwarding off-premise if it is not used; if it is, limit to specific numbers.
- Block casual calling (the use of alternate long-distance companies, like calling cards).
- If hacking is suspected: review history of modifications to the system.
- To monitor traffic: we can install call-accounting software for your phone system.

* * *

Since 1989, Alternative Technologies has been helping nonprofits and local businesses use technology to support their missions. Our areas of expertise:

- **Cloud Services**
- **IT Consulting**
- **Telephone Systems**
- **Cloud Phone Service**
- **Voice & Data Cabling**

Contact us anytime with your technology questions.

510-848-4411
info@alternativetechs.com