IntelePeer
The Cloud Communications Company

TIP SHEET

Avoiding VoIP Fraud

As long as telephone lines have existed, people have been finding ways to attack them. Now, with the emergence and growth of VoIP, those attacks are becoming more frequent, and in some cases, easier to pull off.

Whether attackers are looking to reroute calls, steal free minutes, or enact fraudulent schemes, you must take precautions to safeguard your and your customers' personal information and data. Because VoIP relies on Internet-based networks and interfaces, you must be more diligent than ever.

The following list of security best practices should get you well on your way to protecting your network.

Passwords

Any VoIP device with a configuration interface – phones, PBXs, IP phones, soft clients, workstations, and other networked devices – need strong passwords. Encourage employees to create unique passwords by avoiding simple or easily recognizable passwords.

VPN

Using an encrypted Virtual Private Network is a safe way for remote users (e.g. home workers) to access your network securely. Employees access the network using a specific password and traffic is encrypted to prevent would-be hackers from monitoring and capturing data.

Patches

As new system vulnerabilities are discovered – oftentimes weekly – it's becomes extremely important to run the newest operating system patches. Check regularly for software/firmware updates.

Unused Services

Attackers looking for weaknesses may be able to exploit unused services. For example, if the voicemail system isn't being used, disable it. This will help prevent unnoticed attacks.

Wi-Fi

Open wireless access presents its own set of vulnerabilities. Be sure to use secure encryption systems like WPA2 to keep unknown users off of the network and implement password best practices to ensure security (see above).

SMART PASSWORD TIPS

- Join two or more familiar words that tell a memorable story (e.g. itrimtrees, mydogskippy)
- Use numbers and letters together (e.g. 10derh3art, 5plus2equals7)
- Use an 8 character minimum. 12 or more is better.
- Avoid simple passwords like strings of numbers (1111, 1234) or personal numbers (home address, car registration)

Management Interfaces

Attackers can find "open" ports in your network, sometimes through a simple Google search. Secure all VoIP systems (PBX, phone, etc.) behind an SBC to prevent remote access or call rerouting from hackers.

Mobile VoIP

As VoIP use on smartphones becomes more common, so should security considerations. In the event of a lost or stolen phone, configuration of the phone's access PIN can prevent unwanted access to content. For additional security, implement encryption services for remote VoIP phones.

Lock Down the PBX

Because VoIP phones can register with a PBX from anywhere in the world, consider limiting registrations to within a specific office network, securing phones with passwords, IP addresses, or MAC (physical) address, or grant access to specified users.

TO PUT IT ANOTHER WAY... *Deny access by default and create exceptions for authorized users.*

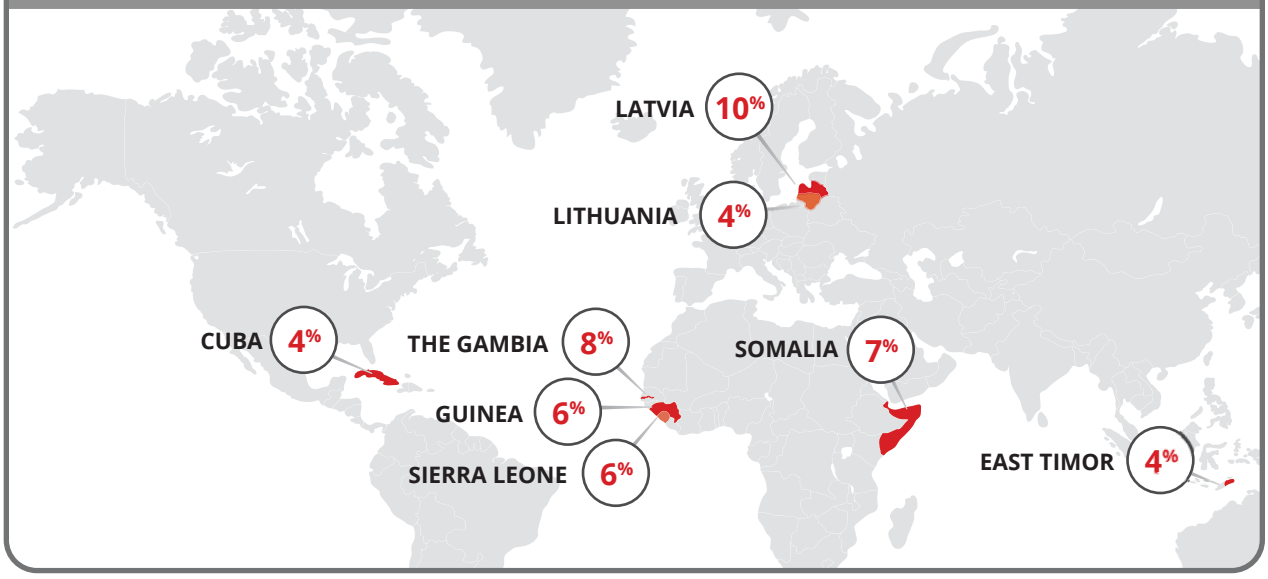
Call Limits

Asking the Internet telephony service provider (ITSP) to place limits on premium rate and international call destinations may help detect fraudulent activities. When patterns of fraud are detected, a notification is issued for authorization of additional spend.

Block International Numbers

Blocking outbound traffic to international numbers is one of the best ways to impose limitations on hackers, especially those using simple forms of toll fraud (such as late night staff making long calls to family members in other countries).

TOP COUNTRIES FOR TOLL FRAUD CALL TERMINATION



For more information, read our *VoIP Security Best Practices Guide*

OR, contact us to learn more about IntelePeer's secure solutions.

IntelePeer
The Cloud Communications Company