

# VoIP Security

## Risks & Administrator Responsibilities

*Voice over Internet Protocol (VoIP) is an exciting new technology that gives you and your business unmatched options for communicating with your customers. However, like any other powerful system, VoIP comes with the potential for abuse unless it is deployed and maintained correctly. This document outlines some of the threats you may face, and your options and responsibilities for defending against them.*

## Common VoIP Threats

VoIP security threats can be grouped into four main categories: theft of service, toll fraud, deception, and vandalism.

### **Theft of Service**

You can pick up your VoIP phone and take it with you anywhere in the world – your calls will follow you. Unfortunately, this same ability can allow a criminal to steal your service unless you protect yourself. Theft of service can result in high phone bills, embarrassment, and even legal complications if the stolen service is used to commit a crime.

### **Toll Fraud**

Toll fraud is a variation on theft-of-service. Rather than simply stealing the use of your phone service, the criminal uses it to place high-cost calls resulting in their own profit. This type of fraud normally entails an offender setting up either a 900 number or an international long-distance number with very high rates. The criminal makes fraudulent calls to these numbers using your account, then you get the bill.

### **Deception**

Deception can take many forms. A criminal may listen in on your calls, redirect them, or even record, alter, and re-play them in order to gain business information or influence an event.

### **Vandalism**

Criminals can modify call routing, change voice menus, delete messages, or simply disrupt service.



## ***How to Protect Yourself***

Even though there are many possible ways your VoIP service can be attacked, you can easily protect yourself by implementing some simple steps: choose good passwords, protect your settings, and monitor your usage.

### **Choose Good Passwords**

Your Voice Portal and Web Portal passwords are the keys to your VoIP system. Anyone that has one or more of them may be able to exploit or damage your phone service. Choosing secure passwords is essential. Your passwords should be unique to each phone/user, and should never be an obvious pattern. Passwords should never be written down. Ideally passwords should be changed at least once per quarter. They should be changed immediately if you suspect that your service may have been compromised.

### **Protect your Settings**

Never share your passwords or phone settings with anyone but a Front Range Internet, Inc. employee. If you use a soft phone, never leave it unattended in a public place, and never set up a soft phone account on a shared computer. Make sure to change your passwords any time an employee leaves your company.

### **Monitor your Usage**

The faster you find out about and report a VoIP compromise the better outcome you'll experience. Check your monthly bill or go to <http://myfrii.com> to monitor your usage. Call 1-800-935-6527 to report any unusual calls or charges.

## ***Your Responsibilities***

You are ultimately responsible for your VoIP usage – even if the usage is the result of fraudulent activity. It is critical that you follow the security guidelines in this document to minimize your risk. It is especially vital that you report any unusual activity as soon as possible.

For assistance with these protection steps, or for advice, please contact a VoIP provisioning expert by calling 1-800-935-6527.

Thank you, and remember to think safe!

