Fraud Protection

Everfast Fiber Networks LLC (“Everfast,” “our,” “we”) has in place an advanced toll fraud management system that enables it to:

- Monitor all of our network usage
- Identify suspicious network activity (based on abnormal call patterns, atypical call activity, hot lists, and subscriber information)
- Receive automatic alerts
- Distinguish fraudulent from honest customer usage
- Investigate and manage cases dynamically and easily
- Resolve cases intelligently with options ranging from automated disabling of the number to configuration changes
- Document fraud cases

While no system is 100% fool-proof, our fraud management system has been proven to minimize toll fraud experienced by our customers.

We continue to track suspected fraudulent usage and will block international calls (with or without customer permission) if we determine that fraud is occurring. However, not all fraud is obvious, and some fraudulent calls may be completed without being detected.

We provide international toll fraud monitoring as a courtesy to our long-distance customers and to protect our network. We are not required to do so.

FAQs

If my phone system is hacked, who is responsible for paying the charges?

The owner of the phone system, not your phone or long-distance provider, is responsible for all charges incurred due to a security failure in your system and resulting fraudulent calling.

Why doesn’t the carrier write off these charges?

As an individual or business end user, you control access to your system. Your telecommunications provider does not. Therefore, you are responsible for all charges incurred. Each carrier must pay a portion of the call that they handle. When a call is placed to an international location the domestic carrier must pay the foreign carrier regardless of whether the call was fraudulent.

Who is responsible for stopping the fraudulent calls?

It is the customer's responsibility to identify and stop fraudulent calls given that only they can differentiate legitimate calls from fraudulent ones.

Filing a Complaint with the FCC

Businesses or consumers who become victims of fraud can file a complaint with the FCC. There is no charge for filing a complaint. You can file your complaint using an online complaint form found at www.fcc.gov/complaints.

Voicemail Fraud from the FCC

https://www.fcc.gov/guides/voice-mail-fraud

Important PBX Long Distance Toll Fraud Risk Prevention

If your business uses a PBX system, it may be at risk of being hacked and allowing others to fraudulently gain access to your business's phone and voice mail system. Through security holes, hackers place long distance and international calls using your local system. If you fall victim to such circumstances, your business is responsible for all associated phone charges. As the owner of your phone system, we suggest you take measures to ensure proper security to best prevent the occurrence of hacking. Use this document to better understand how this hacking occurs and what measures we suggest to secure your phone system.

Unauthorized or fraudulent hacking through your phone system can potentially cost your business significant amounts of money. PBX owners are often not aware of any security holes until they receive an invoice from their telecommunication provider for an amount in excess of what it expected. Unfortunately, these toll charges are the responsibility of the business customer and not the responsibility of the telecommunication provider.

Primary Gaps

The primary form of fraud most frequently seen allows hackers to use a consumer's or business's voice mail system and the default password to accept collect calls without the knowledge or permission of the consumer or business. Telephone hackers can also infiltrate systems through the Direct Inward Dial System Access (DISA) feature of your PBX.

How Does the Scam Work?

Hackers are able to infiltrate a voice mail system and search for voice mailboxes that still have the default passwords active or have passwords with easily-guessed combinations, like 1-2-3-4. Hackers know common default passwords and can try them until they can engineer their way into your phone system. The hacker then uses the password to access the phone system and to make international calls.

The hacker does this by first changing the voice mailbox's outgoing greeting to something like "Yes, yes, yes, yes, yes, operator, I will accept the charges." Then, the hacker places a collect call to the number they've just hacked. When the (automated) operator (which is usually programmed to "listen for" key words and phrases like "yes" or "I will accept the charges") hears the outgoing "yes, yes, yes, yes, yes, operator, I will accept the charges" message, the collect call is connected. The hacker then uses this connection for long periods of time to make other international calls.

There is also another twist to this scam. A hacker breaks into voice mailboxes that have remote notification systems that forward calls or messages to the mailbox owner. The hacker programs the remote notification service to forward to an international number. The hacker is then able to make international calls.

PBX systems can be configured improperly and with poor security which can allow hackers to gain access to the system remotely. This is normally managed through the PBX maintenance port from remote service centers. By taking control of the port, hackers can change call routing, modify passwords, remove, and add extensions or completely shut down your PBX all of which are a great risk to your organization.

Some voicemail systems can be programmed to make outbound calls. By searching for default mailboxes, a hacker then finds easy sequences to target as mentioned above. Hackers then use the outbound calling feature to a voice mail box that will give them dial tone. This allows the hacker to make calls from anywhere on your account at your toll expense.

What to Beware of:

Hackers usually break into voice mail systems during holiday periods or weekends, or evenings when callers will not be calling; thus, changing the outgoing message goes unnoticed. Businesses that are victimized usually find out about the hacking when their telecommunications provider calls to report unusual activity or exceptionally high toll charges.

What You Should Do to Prevent Toll Fraud Risk:

Because the PBX owner is responsible for the security of their system and responsible for all charges associated with toll fraud, we recommend the following to avoid falling prey to these types of scam:

- Educate key staff that utilize your system on proper security measures to prevent fraud.
- Always change the default password provided by the voice mail vendor and change this password frequently;

- Choose a complex voice mail password of at least six digits, making it more difficult for a hacker to detect;
- Remove inactive mailboxes. When an extension is no longer required, it should be canceled along with access rights.
- Don’t use obvious passwords such as an address, birth date, phone number, or repeating or successive numbers, i.e. 000000, 123456;
- Check your recorded announcement regularly to ensure the greeting is indeed yours. Hackers tend to attack voice mailboxes at the start of weekends or holidays;
- Consider blocking international calls, if possible
- Consider disabling the remote notification, auto-attendant, call-forwarding, and out-paging capabilities of voice mail if these features are not used.

If you believe your system has been hacked, call Everfast and report the incident to the police.

Last updated: April 2024