Fraud Control and Management

How does Tel2 deal with Fraud?

Toll fraud is a potential threat not just for Telcos but all businesses subscribing to a VoIP phone service. While we will quickly disable any suspected toll fraud attempt, like any online service, subscribers are responsible for securing their own systems.

- **SIP Registration**: uses a phone number and password to authenticate (or “register”) your phone onto our service. Always ensure strong passwords, never use passwords like ‘123’, ‘abc’ or ‘password’ as your passwords and finally always ensure your passwords safe storage.
- **SIP Peering**: This method of connection links your public WAN address and our proxy address (phone.tel2.co.uk). Administrators must always confine access to their customers public SIP port to trusted service providers via IP Tables or firewall rules.

Occasionally staff will in error misdial the leading prefix, which our systems identify as potential threat (e.g. Somalia is +252). We are generally quick to identify misdialled prefixes and after speaking directly with account holders will quickly unblock the account. Most customers are happy to put up with this minor inconvenience for the comfort of knowing we are actively monitoring call fraud attempts.

How Fraud works

(c) 2024 Support <support@tel2.co.uk> | 2024-05-07 17:18
URL: https://faq.tel2.co.uk/index.php?action=artikel&cat=0&id=52&artlang=en-us

Overseas calling

Most fraud attempts we see originate from hackers in locations like Russia, Israel and Estonia with the ultimate objective being to find a vulnerable Telco or customer account. Once a vulnerability is identified the end goal is to route calls via the compromised account to regions like Afghanistan, Somalia, Syria etc with the fraudsters magic triangle combining unstable countries with astronomical phone costs and of course a hacked phone number. This is serious business and there is no shortage of disputes between tier one carriers in particular and stunned customers out the door thousands of dollars with the carrier (tier one usually) stubbornly clinging to their strict terms and conditions.

Calling Card operators

On the other side of this fraud are the Calling cards operators offering cheap calling into those very same high cost destinations. Of course somewhere in the middle are our fraudulent hackers selling those very same stolen routes to the calling card middle men always willing to turn a “blind eye” to the truth.

How we block fraud attempts

We monitor every call to all the worlds global hotspots. If for example a call attempt is made to Somalia during the middle of the night, where you’ve never previously called that destination, we will immediately end the call and block all further calls attempts. Behind the scenes we also implement a range of measures to isolate the hacker and their associated proxies.

What should you do to prevent?

Registration: The resolution from your side is usually as simple as changing or providing strong passwords. If your account has been blocked by us for a suspected fraud attempt, we ask you to change your password.

SIP Peering: Administrators must limit all access to their WAN ip including most importantly SIP ports 5060 and port 80 to known service providers (such as us) and system admins.

What happens after we have blocked your account?

- We will notify you by email of the international toll block on your account
- Immediately the account will have been prevented from making overseas calls. As soon as you have reset the password, or hardened your firewall, we will reenable the account to allow overseas calling.
- See also Ghost Calling.

(c) 2024 Support <support@tel2.co.uk> | 2024-05-07 17:18
URL: https://faq.tel2.co.uk/index.php?action=artikel&cat=0&id=52&artlang=en-us

Unique solution ID: #1051
Author: Support
Last update: 2016-05-29 00:17

(c) 2024 Support <support@tel2.co.uk> | 2024-05-07 17:18
URL: https://faq.tel2.co.uk/index.php?action=artikel&cat=0&id=52&artlang=en-us