

Gateway Telnet Communication's Fraud Guidelines

Fraud Guidelines

There are several ways that telecommunication services may be fraudulently accessed, but it is possible to take steps to minimize fraud exposure on your network. While we at Gateway Telnet hope this never happens to you, we have developed some simple tips to help you minimize your exposure to fraud and to help get to the bottom of the situation if you discover fraudulent activities.

You acknowledge that it is your responsibility to take whatever actions you deem necessary to make your computer and voice network and circuits adequately secure from unauthorized access. You further acknowledge that we only provide telecommunications services and certain equipment to you and that we are not responsible for the security of your network and circuits from third parties, or for any damages that may result from any unauthorized access to your network. We urge you to seek independent advice with respect to products, equipment (including configurations), and services available to make your computer network and circuits more secure from third parties.

If you suspect you may be the victim of fraud, call Gateway Telnet's service department at 818 775-1234 Monday through Friday, from 8:30 AM to 5:00 PM PDT as soon as possible.

The following are strongly recommended steps that, if taken, will help protect your network from hackers. Failure to implement these reasonable steps may expose your phone system to a greater likelihood of exposure to fraud. In addition you should consult your telephone system vendor for additional guidance.

A. Private Branch Exchange (PBX) Security

A PBX is a telephone system that serves a particular business or office. If the PBX system is not maintained and secured it can be compromised allowing remote hackers to originate long distance and international calls undetected to the business.

1. Change the generic code (administration security code) and or existing code. A generic code is the default administration security code set within a PBX/phone system. This code allows administrators to control the "on and off" features which provides remote access within the PBX/phone systems. Obtaining generic codes for specific makes and models of PBX/phone systems are made available in the internet, therefore exposure exists, with hackers obtaining these codes.
2. Understand the configuration of your PBX/phone systems and eliminate remote access and/ or disable access system. This is most important on IP PBXs in which SIP trunks and open ports for the Public Internet exist.
3. Check for errors and changes in the configurations of your PBX, firewall and router or call processing,
4. Install a firewall and anti-virus software.
5. Check for inbound data spikes.

6. Set up call accounting software or station message detail to monitor abnormal call activities. Set thresholds to alarm on abnormal call activities during business hours and off hours.
7. Block all international countries to include Canada and Caribbean if not normally called directly on your PBX/phone system. A list of the international country codes is provided in this Fraud Guideline.
8. If you do not accept third party billing, block this in your PBX/phone system.
9. Block casual calling on your PBX/phone system. Casual calling allows callers to place long distance calls using another carrier identification code (CIC). The caller dials 1010, CIC and the destination number. The caller will receive a third party bill from the third party carrier. Fraudsters often use this method of dialing.
10. Disable or change the password for Direct Inward System Access - **DISA** .This feature allows a caller to dial into the system, enter an authorization code and get an outbound line. The codes are often not difficult to crack. A hacker can then use this feature to make long distance calls at the company's expense. The DISA application will provide dial tone. If the password parameter is "no-password" the calls can complete.
11. Add long distance or international account codes.
12. Invest in a call accounting software.
13. Run periodic security audits to check for vulnerabilities.
14. Set a specific threshold for attempts to enter system and program the PBX to terminate access when threshold is exceeded.
15. Discard listings and/ or directories with PBX access numbers by shredding the information.
16. Share system information with only authorized individuals within the company.
17. Review the features that are available on the system and disable those features that are not required.
18. Disable, if possible, all forms of automated trunk to trunk (straight through dialing). Straight through dialing allows you to make telephone calls through your mailbox or telephone system when you are at an offsite location. If this feature is used, it is important that you generate and monitor reports to ensure your mailboxes are not being abused.

B. Voice Mail System

1. Change the generic code (administration security code) and/ or existing code. A generic code is the default administration security code set within a voicemail system. This code allows administrators to have control of turning on and off features within the voice mail systems. Obtaining generic codes for specific makes and models of voice mail systems are made available in the internet, therefore exposure exist with hackers obtaining these codes.

2. Set voicemail passwords to hard codes consisting of 6 characters to 10 characters. You must not use extensions and or soft codes 1111 and 1234. The more complex the security codes the harder it is to compromise.
3. Change user security codes at least every 90 days.
4. Understand the configuration of your voicemail system and disallow all features which allow remote access into your voicemail equipment to place outbound long distance and international calls. Hackers who have compromised a voicemail box will preprogram the fraud destination number(s). After they have done this, they use the transfer feature, pager feature and/or zero out features to place their fraud calls.
5. Block 011 international outbound calls and calls to the Caribbean countries.
6. Block 1010 casual calling and third party calls within your voicemail system.
7. Disable unused voice mail boxes especially in unoccupied areas.
8. Do not share your voice mail security codes or have them posted.

8YY (Toll Free) Traffic Pumping

8YY Traffic Pumping – This is a different fraud type that may actually be misconstrued as a [Telephony Denial of Service](#) (TDoS) attack. Companies that run contact centers for services or support of their customers subsidize your call by providing a toll free number. They pay a higher rate than you would for the call, but do so for your convenience. The fraudster sets up a revenue sharing agreement with one or more service providers routing the 8YY calls, and then generates a large volume of traffic. In many cases, they will target an Interactive Voice Response (IVR) system, because fraudsters can keep hitting prompts without dealing with a human that would hang up the call.

1. Set up disconnect supervision on the IVR, auto attendant and voicemail. The caller should not be able to loop around in the IVR by pressing certain prompts. This is the key in avoiding long duration calls.

VoIP SIP Security Recommendations

- 1) Do not accept SIP authentication requests from all IP addresses. Use the “permit=” and “deny=” lines in sip.conf to only allow a reasonable subset of IP addresses to reach each listed extension/user in your sip.conf file. Even if you accept inbound calls from “anywhere” (via [default]) don’t let users reach authenticated elements.
- 2) Set “alwaysauthreject=yes” in your sip.conf file. The default is “no”, which allows extension information leakage. Setting this to “yes” will reject bad authentication requests on valid usernames with the same rejection information as with invalid usernames, denying remote attackers the ability to detect existing extensions with brute-force guessing attacks.
- 3) Use STRONG passwords for SIP entities. Don’t just concatenate two words together and suffix it with “1”. Use symbols, numbers, and a mix of upper and lowercase letters at least 12 digits long.

- 4) Block your AMI manager ports. Use “permit=” and “deny=” lines in manager.conf to reduce inbound connections to known hosts only. Use strong passwords, at least 12 characters with a complex mix of symbols, numbers, and letters.
- 5) Allow only one or two calls at a time per SIP entity, where possible. This limits your exposure when legitimate password holders on the system lose control of their passphrase.
- 6) Make your SIP usernames different from the extensions. While it is convenient to have extension “1234” map to SIP entry “1234” which is also SIP user “1234”, this is an easy target for attackers to guess SIP authentication names. Use the MAC address of the device, or some sort of combination of a common phrase + extension MD5 hash (example: from a shell prompt, try “md5 -s ThePassword5000”)
- 7) Ensure your [default] context is secure. Don’t allow unauthenticated callers to reach any contexts that allow toll calls. Permit only a limited number of active calls through your default context (use the “GROUP” function as a counter.) Prohibit unauthenticated calls entirely (if you don’t want them) by setting “allowguest=no” in the [general] part of sip.conf.

C. Physical Security

1. Keep phone rooms secured and locked.
2. Validate credentials for all technicians who visit your sites. Fraud perpetrators can gain access to unsecured phone rooms. A device can be clipped on to your line(s) to place fraud calls.
3. Develop a security plan with your shared tenants and building management to secure your phone room.

D. Social Engineering

“Social Engineering” may be used, where a caller manipulates someone into performing an action or divulging confidential information. When the types of calls described below are received, report the call to Gateway Telnet Fraud and Security Compliance Department at (866) 839-8545.

A fraud perpetrator may call into a business establishment pretending to be a technician for a phone company. The perpetrator will manipulate the party into pressing certain digits on the telephone keypad, allowing the perpetrator to place free long distance calls. The party will be charged for the long distance calls.

Do not transfer callers to 900, 800, and 700. This is a fraud scam. Dialing 9, will provide the caller with an outside line and “00”, will send the caller to the long distance operator. Any completed call placed will be charged to the business that transferred the caller to 900, 800, or 700.

E. Modem Hijacking

Modem Hijacking may be used to make fraudulent long distance calls from your computer that is billed to your phone number. Possible steps to help prevent modem hijacking include:

1. Turn off your computer and modem when they are not in use.
2. Unplug phone connections from the modem when a modem is not in use.
3. Raise the volume level of your modem, so that you are aware of a redial.
4. Be aware when visiting sites of questionable content, or avoid such sites entirely. A number of sites download surreptitiously onto consumers' hard drives.
5. Monitor your child's use of the Internet. Consider using blocking software to keep children from questionable sites – adult, gambling, etc.
6. Do not download from an un-trusted web site.
7. Close pop-up windows by selecting the, "X" button in the upper right hand corner, rather than any other embedded icons.
8. Keep your operating system current with patches and updates.
9. Ensure that Internet dial-up access numbers are on your local telephone plan and delete unknown access numbers.
10. Consider installing anti-virus software and update regularly.
11. Disable ActiveX.
12. Install software to help prevent fraudulent activity. Web sites where anti-virus or trial version of anti-virus software has been made available include:
 - www.symantec.com
 - www.mcafee.com

F. International Country Codes List to Block Directly within the PBX.**International Country Code List**

<u>Code</u>	<u>Country</u>
20	Egypt
211	South Sudan
212	Morocco
213	Algeria
216	Tunisia
218	Libya
220	Gambia
221	Senegal
222	Mauritania
223	Mali
224	Guinea
225	Ivory Coast
226	Burkina Faso
227	Niger
228	Togo
229	Benin
230	Mauritius
231	Liberia
232	Sierra Leone
233	Ghana
234	Nigeria
235	Chad
236	Central African Republic
237	Cameroon
238	Cape Verde
239	São Tome
240	Equatorial Guinea and Principe
241	Gabon
242	Republic of the Congo
243	Democratic Republic of the Congo
244	Angola
245	Guinea-Bissau
246	British Indian Ocean Territory
247	Ascension Island
248	Seychelles
249	Sudan
250	Rwanda
251	Ethiopia
252	Somalia

253	Djibouti
254	Kenya
255	Tanzania
256	Uganda
257	Burundi
258	Mozambique
260	Zambia
261	Madagascar
262	Réunion
263	Zimbabwe
264	Namibia
265	Malawi
266	Lesotho
267	Botswana
268	Swaziland
269	Comoros
27	South Africa
290	Saint Helena
291	Eritrea
297	Aruba
298	Faroe Islands
299	Greenland
30	Greece
31	Netherlands
32	Belgium
33	France
34	Spain
350	Gibraltar
351	Portugal
352	Luxembourg
353	Ireland
354	Iceland
355	Albania
356	Malta
357	Cyprus
358	Finland
359	Bulgaria
36	Hungary
370	Lithuania
371	Latvia
372	Estonia
373	Moldova
374	Armenia
375	Belarus
376	Andorra
377	Monaco
378	San Marino
379	Vatican City
380	Ukraine
381	Serbia

382 Montenegro
383 Kosovo
385 Croatia
386 Slovenia
387 Bosnia and Herzegovina
388 Discontinued
389 Macedonia
39 Italy
40 Romania
41 Switzerland
420 Czech Republic
421 Slovakia
422 unassigned
423 Liechtenstein
43 Austria
44 United Kingdom
45 Denmark
46 Sweden
47 Norway
48 Poland
49 Germany
500 Falkland Islands
501 Belize
502 Guatemala
503 El Salvador
504 Honduras
505 Nicaragua
506 Costa Rica
507 Panama
508 Saint-Pierre and Miquelon
509 Haiti
51 Peru
52 Mexico
53 Cuba
54 Argentina
55 Brazil
56 Chile
57 Colombia
58 Venezuela
590 Guadeloupe
591 Bolivia
592 Guyana
593 Ecuador
594 French Guiana
595 Paraguay
596 Martinique
597 Suriname
598 Uruguay
599 Netherlands Antilles
60 Malaysia

61	Australia
62	Indonesia
63	Philippines
64	New Zealand
65	Singapore
66	Thailand
670	East Timor
672	Australian External Territories
673	Brunei
674	Nauru
675	Papua New Guinea
676	Tonga
677	Solomon Islands
678	Vanuatu
679	Fiji
680	Palau
681	Wallis and Futuna
682	Cook Islands
683	Niue
685	Samoa
686	Kiribati
687	New Caledonia
688	Tuvalu
689	French Polynesia
690	Tokelau
691	Federated States of Micronesia
692	Marshall Islands
7	Russia/Kazakhstan/Abkhazia
81	Japan
82	South Korea
84	Vietnam
850	North Korea
852	Hong Kong
853	Macau
855	Cambodia
856	Laos
86	China
870	Inmarsat SNAC Service
878	Universal Personal Telecommunications Services
879	reserved
880	Bangladesh
881	Global Mobile Satellite System
882	International Networks
883	International Networks
886	Taiwan
888	Telecommunications for Disaster Relief by OCHA
889	unassigned
90	Turkey
91	India
92	Pakistan

93	Afghanistan
94	Sri Lanka
95	Myanmar
960	Maldives
961	Lebanon
962	Jordan
963	Syria
964	Iraq
965	Kuwait
966	Saudi Arabia
967	Yemen
968	Oman
970	Palestine
971	United Arab Emirates
972	Israel
973	Bahrain
974	Qatar
975	Bhutan
976	Mongolia
977	Nepal
979	International Premium Rate Service
98	Iran
991	International Telecommunications Public Correspondence Service
992	Tajikistan
993	Turkmenistan
994	Azerbaijan
995	Georgia
996	Kyrgyzstan
998	Uzbekistan

Caribbean Dialing Code List (1+)

1+	340	United States Virgin Islands
1+	670	Northern Mariana Islands
1+	671	Guam
1+	684	American Samoa
1+	787	Puerto Rico
1+	242	Bahamas
1+	246	Barbados
1+	264	Anguilla
1+	268	Antigua and Barbuda
1+	284	British Virgin Islands
1+	345	Cayman Islands
1+	441	Bermuda
1+	473	Grenada
1+	649	Turks and Caicos Islands
1+	664	Montserrat

1+	721	Sint Maarten
1+	758	Saint Lucia
1+	767	Dominica
1+	784	Saint Vincent and the Grenadines
1+	809	Dominican Republic
1+	829	Dominican Republic
1+	849	Dominican Republic
1+	868	Trinidad and Tobago
1+	869	Saint Kitts and Nevis
1+	876	Jamaica
1+	939	Puerto Rico