TPx Voice Assurance & Anti-Fraud Policy

Version Effective on Jan 1. 2024

This document provides an overview of how TPx configures and manages your voice services to protect against unauthorized use and what you, as the customer, can do to help.

Customer Equipment Security

Customers are responsible for ensuring their equipment and configuration follow best practices which include strong pins/passcodes/passwords and disabling unused accounts and services. Systems which are periodically reviewed are less likely to be exploited by hackers. Customers who rely on 3rd party vendors other than TPx to manage their phone equipment should ask their vendor to verify the common sources of exploits are secured.

The following is an abbreviated list of common exploits to customer equipment:

- Set strong passwords for all admin accounts
- Enable account lockouts after X login attempts
- Enable account codes for international calling
- Enable password/passcode/pin policies
- Increase password/passcode difficulty to 6 or more letters/numbers
- Restrict admin access to specific networks/PCs
- Disable international calling on all extensions
- Disable international calling during afterhours/weekends
- Disable casual dialing/calling (1010+ dial-around)
- Disable secondary dial tone
- Disable outbound calling through the voicemail system
- Disable return call through the voicemail system
- Remove unused accounts over 90 days old

TPx Equipment Security

TPx may deploy equipment on the customer site which may serve multiple needs. TPx equipment will be configured in a manner which restricts access to a maintained Access Control List(s) (ACL) of authorized IP Addresses. ACLs not only restrict remote access to the device but also who may signal phone calls to the device using VoIP. TPx periodically updates ACLs based on the deployment of new and removal of old equipment.

TPx Voice Services Security

TPx voice services are designed by Engineering to be secure by default. Customers may desire for a more functional service which also increases the risk of fraud.

The following is a list of default settings TPx deploys for UCx and SmartVoice services.

- Passcode Policy – Enforces strength of voicemail passcodes
- Password Policy – Enforces strength of web portal passwords
- Outgoing Calling Plan – International calling is disabled by default
- Outgoing Redirect Plan – Forwarding to international number is disabled by default
- Enterprise Administrators – Customers must request an administrator to be created
- Group Administrators – Customers must request an administrator to be created
- User Account – Customers must pay for user accounts – Remove when not required
- Call Forwarding – Forwarding calls to international destinations is monitored
- Voicemail Callback – Disabled system wide – Cannot callback originator of voicemail
- Voice Portal Calling – Disabled by default – Service turned on only for desired accounts
- Group Call Capacity – Limits total number of concurrent calls based on number of users
- User Call Capacity – Limits number of concurrent calls a single user can make
- Device SIP Credentials – Randomly computer generated user and password

Unused Administrator Accounts

TPx periodically monitors UCx/SV systems for unused administrator accounts. These accounts may be disabled or deleted from the system.

Poorly Named Administrator Accounts

TPx periodically monitors UCx/SV systems for poorly named administrator accounts. These accounts may be disabled or deleted from the system. Poorly named accounts contain the words “TPx”, “Demo”, “Test” and “Trial”. Administrator accounts containing such names are typically temporary in nature and pose a risk to the customer if not removed.

Incorrectly Permissioned Administrator Account

TPx periodically monitors UCx/SV systems for administrator accounts which do not conform to preset permission guidelines. Accounts found with incorrect permissions will have permissions reset. Accounts with incorrect permissions pose a risk to the customer as the account may be able to perform higher level administrator tasks such as adding/remove user accounts.

Auditing Administrator Changes

TPx monitors changes may by administrators in real-time. This allows TPx to detect when an administrator is making too many changes or when specific changes increase the risk of generating fraudulent calls. These administrator accounts are flagged and an internal case is created for review by the Voice Assurance team.

The following are examples of changes which will trigger an alarm:

- System/Enterprise/Group/Department administrator creation / modification
- Modification to Outgoing Calling Plan
- Call Forward Always/No Answer/Busy/Not Reachable set to an international destination
- Voicemail Transfer to international destination

High-Risk International Countries

TPx blocks customers from calling high-risk international countries by default. A list of high-risk international countries is identified in Figure-1 of this document. Customers who have a business need to call these countries may either request access during service onboarding or open a TPx Service Case and request access. The customer will be required to sign the waiver in Figure-1 allowing specific phone numbers to call specific countries. This process insures the customer knowingly accepts the additional risk and costs associated with calling these countries. Customers should limit access to these countries to only specific phone numbers who need to make the phone calls. Opening access to their entire organization poses a significant risk.

Post Call Behavior Analysis

TPx monitors phone calls made by customers to track historical usage and detect possible fraudulent behavior. Most customers place phone calls during standard business hours, so calls made afterhours will have a higher risk of being fraudulent. TPx has also compiled a list of phone number which have been used by hackers and have a very high risk of fraud.

Real-time Call Behavior Analysis

TPx monitors phone calls being made by customers to detect possible fraudulent behavior. A user is monitored for not only the number of calls placed but also the international destinations of the calls. Calls are allowed/disallowed by preset thresholds which are managed by TPx.

Toll Free Traffic Pumping

TPx monitors for Toll Free traffic pumping and will block it when detected. Traffic pumping is a type of attack used by hackers who will call a single or multiple Toll Free numbers repeatedly. The purpose of traffic pumping is to adversely affect a customer’s ability to answer legitimate calls or to cause the customer financial harm.

Hangups/Silence/Telemarketing

These types of calls may be lawful, so TPx will not take any proactive action to block these.

Customers may open a Service Request to block specific phone numbers, but the offending caller may switch phone numbers and reach the customer again. In extreme cases, the phone number can be removed from the user.

Call Annoyance/Harassment

Customers experiencing annoying or harassing calls must first open a case with local law enforcement. TPx can be involved once the customer has a case number by calling 1-866-839-8545 (option 5) during business hours. The Legal/compliance team will take the inbound request and forward the request to the Voice Assurance team to determine if specific originating phone numbers can be blocked.

RoboCalling

RoboCalling is an automated system which dials a large number of phone numbers. Once a call is connected, an automated message is played and/or the call is transferred to an agent who typically tries to sell you something.

Customers wishing to use the RoboCalling service may open a Service Request to be signed up for RoboCall blocking. This service will route inbound calls through a service which interrogates the calling number against a national RoboCalling database of offenders.

Do Not Originate (DNO)

DNO are phone numbers which should not be used to place calls to customers. The following is a list of DNO numbers which can be blocked:

- Inbound Toll Free numbers
- Extensions
- Poorly formed numbers (81-861-4600)
- The number zero

Customers wishing to use the DNO service may open a Service Request to be signed up for DNO blocking. This service will route inbound calls through a service which interrogates the calling number against a DNO database.

Locking Out a Hacker

TPx systems are designed to identify any account that has been compromised by hackers and will automatically take action to secure the account. This process will lockout a hacker who may have obtained account credentials through brute force or social engineering. As this process also lock out the legitimate user, TPx will open a service request to track the action and the repair department will contact the customer to restore the user's service.

Supplemental Information:

https://www.fcc.gov/sites/default/files/stop_unwanted_robocalls_and_texts.pdf

Figure 1 – International Unblock Worksheet

Enable International Calling					Initial			
Enable High Risk International Destinations Identified below					Initial			
High Risk Destinations			High Risk Destinations			High Risk Destinations		
Select	Name	Code	Select	Name	Code	Select	Name	Code
	Afghanistan	93		Georgia	995		Nigeria	234
	Albania	355		Guinea	224		Niue	683
	Algeria	213		Guinea-Bissau	245		Papua New Guinea	675
	Angola	244		Inmarsat (Atlantic Ocean-East)	871		Rwanda	250
	Anguilla	1264					Saint Helena	290
	Ascension Island	247		Inmarsat (Atlantic Ocean-West)	874		Sao Tome and Principe	239
	Azerbaijan	994					Senegal	221
	Belarus	375		Inmarsat (Indian	873		Serbia	381
	Benin	229		Inmarsat (Pacific Ocean)	872		Seychelles	248
	Bosnia and Herzegovina	387		International Networks	882		Slovenia	386
	Botswana	267		Ivory Coast	225		Solomon Islands	677
	Burkina Faso	226		Kiribati	686		Somalia	252
	Burundi	257		Latvia	371		Sudan	249
	Cameroon	237		Lesotho	266		Swaziland	268
	Cape Verde	238		Liberia	231		Tanzania	255
	Central African Republic	236		Macedonia	389		Togolese Republic	228
	Chad	235		Madagascar	261		Tokelau	690
	Comoros	269		Malawi	265		Tunisia	216
	Congo	242		Maldives	960		Tuvalu	688
	Cook Islands	682		Mali	223		Uganda	256
	Cote D'Ivoire	225		Mauritania	222		Uzbekistan	998
	Croatia	385		Mauritius	230		Wallis and Futuna	681
	Democratic Republic of the Congo	243		Mayotte	262		Zambia	260
				Monaco	377		Zimbabwe	263
	Diego Garcia	246		Montenego	382			
	Djibouti	253		Morocco	212			
	Estonia	372		Mozambique	258			
	Equatorial Guinea	240		Myanmar	95			
	Ethiopia	251		Namibia	264			
	Gabonese Republic	241		Naura Islands	674			
	Gambia	220		Niger	227			

By signing this form, Customer agrees that it is responsible for all authorized and unauthorized international usage charges made based on the above choices, beginning on the date this authorization is signed.

Date: ______________________________

Customer Name: ______________________________

Title: ______________________________

Signature: ______________________________

Name (Printed): ______________________________