VirtualPBX®

VoIP Phones Security Checklist

VoIP phones are powerful communication tools, designed to function on a secure network. They are not intended for deployment on the open internet. Specifically, every VoIP phone contains credentials that allows the phone to place calls, often anywhere in the world.

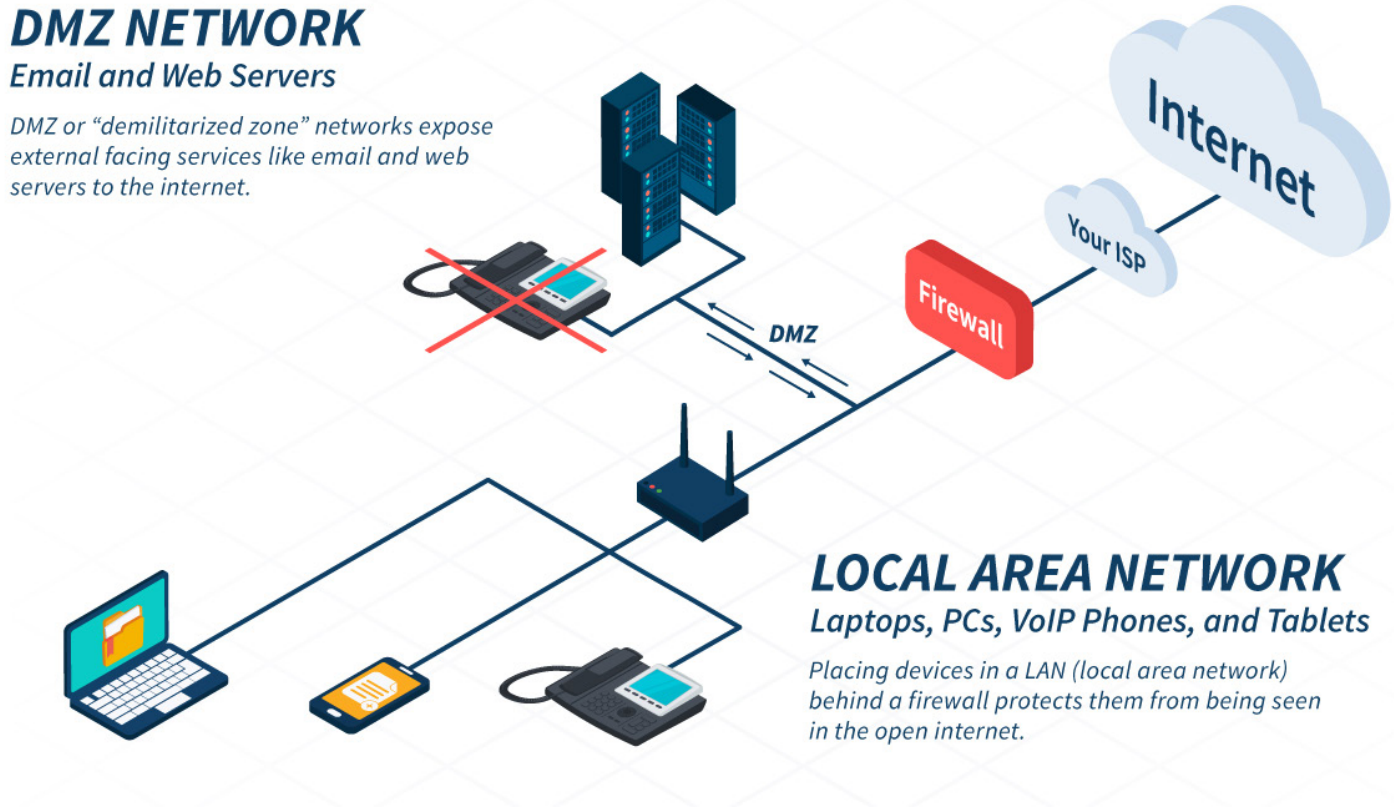
Protecting your VoIP credentials, just like all of relevant business and personal information, is vital to the overall safety and success of your organization.

Securely Deploying Phones on Your Network

A key to protecting VoIP devices from hackers is deploying the phone safely and securely on your network – ensuring the phone is not accessible by anyone on the internet directly.

Most networks can segment a portion of their devices in a DMZ, or "demilitarized zone." Services and devices in a DMZ, such as an email server, can be accessed from the internet.

Deploying a phone on a network's DMZ exposes it to attacks from anyone on the internet. Attackers can compromise the credentials stored on the device, placing unwanted and often expensive calls, or worse.



VirtualPBX.com | 1275 Lincoln Ave, Suite 7, San Jose, CA 95125 | Toll Free: 888.825.0800 | Fax: 888.998.3535

1998-2020. VirtualPBX.com, Inc. All rights reserved. Virtual PBX, TrueACD, and ProSIP are ® trademarks of VirtualPBX.com, Inc.

Protecting your VoIP Phone

Remember to never expose any device that contains usernames and passwords to the internet. Following the security protocols outlined by your IT department, you'll be doing your part to keep your VoIP phone safe and avoid costly attacks on your company.

Security Checklist

To keep your personal log-in credentials and company information both secured and safe, make sure you follow these steps:

- ❑ Establish your firewall and/or VPN connections in line with your company's security protocols.
- ❑ Ensure your router settings are in line with VoIP standards. Some steps may require you contact your ISP:
    - ❑ DISABLE SIP ALG if it is enabled. Not all routers have this setting; if the setting is not found, it is possible that your router does not allow you to disable it and you may need to replace your router.
    - ❑ Make sure NAT is enabled – please be aware that if there is more than one router in the path, there could be 'DUAL NATTING.' If this is the case, you may need to put the second router in BRIDGE mode. You may need to contact your Internet Service Provider to assist.
    - ❑ DISABLE Universal Plug'N'Play (UPnP).
    - ❑ Enable QoS (Quality of Service) if available.
    - ❑ You may also need to open the following ports on your router/firewall:
        - ❑ Port 5060 TCP and UDP (this is for the SIP call messaging)
        - ❑ Ports 16348-32768 UDP (this is for all RTP and audio streams)
- ❑ By default, VirtualPBX provides complex login credentials on VoIP devices, and these credentials very rarely need to be re-entered. If you must change those credentials, always exercise sound password strength and protection practices.
- ❑ Going to be out of town on vacation? Turn your VoIP phone off.

We're Here to Help!

VirtualPBX works hard to help protect your organization. **If you ever have a question or concern, we are here to help.** Simply give our team a call at 888.825.0800, reach us in chat at virtualpbx.com, or send us an email at support@virtualpbx.com. Our team is available 24/7.

1998-2020. VirtualPBX.com, Inc. All rights reserved. Virtual PBX, TrueACD, and ProSIP are ® trademarks of VirtualPBX.com, Inc.