voipstudio

White paper

# How to secure your cloud business phone system

# Understanding the risks

voipstudio

Cloud-based phone systems have transformed how businesses communicate, but with **increased connectivity also come new security challenges**.

**Small and mid-sized businesses are particularly vulnerable because attackers often assume they have fewer resources to invest in security.** However, with the right strategies, you can proactively safeguard your communications infrastructure and ensure customer trust.

## Key risks to watch out for

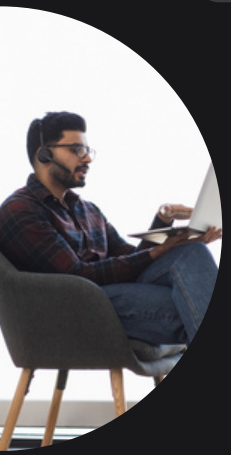
1. **Data breaches:** Sensitive customer and business data can be intercepted if systems aren't secured.
2. **VoIP fraud:** Criminals exploit vulnerabilities to make unauthorized international calls or reroute traffic, causing unexpected costs.
3. **Unauthorized access:** Weak authentication protocols make it easy for attackers to hijack accounts or intercept calls.
4. **Denial-of-Service attacks (DoS):** Malicious actors overload systems, rendering your phone services unusable.
5. **Phishing and social engineering:** Attackers target employees to gain access to admin credentials or sensitive information.

**43%**

Of cyberattacks target small and mid-sized businesses, with VoIP systems becoming a growing focus for hackers.

Source: Verizon DBIR

# Best practices for protection



Securing your cloud-based phone system doesn't have to be complex, but it does require a proactive approach. **The goal is to combine strong policies, robust authentication, and continuous monitoring.**

## Best security practices

- **Enable multi-factor authentication (MFA):** Add an extra layer of security to prevent unauthorized access to dashboards and accounts.
- **Use encrypted communications:** Systems like VoIPstudio offer end-to-end encryption for calls and messages to secure sensitive data in transit.
- **Set up access controls:** Restrict permissions based on roles to ensure only authorized team members can manage key settings.
- **Monitor and audit activity:** Regularly track login attempts, call patterns, and unusual account activity to identify risks early.

**99.2%**

Reduction in account compromise risk when using MFA compared to relying on passwords alone.

Microsoft Security

voipstudio

# Building a future-proof security strategy

voipstudio

Securing your VoIP system isn't a one-time task, it's an ongoing process. **Threats evolve constantly, and businesses need a forward-thinking security strategy that grows alongside technology and customer demands.**

### Integrate security into workflows

Embed security measures into onboarding, remote access, and day-to-day operations.

### Train employees continuously

Educate staff on phishing, password hygiene, and secure communication practices.

### Collaborate with trusted providers

Providers like VoIPstudio offer strong security certifications, transparent policies, and built-in protections.

### Plan for incident response

Prepare a detailed action plan for potential breaches to minimize downtime and reputational damage.

## 75%

Of organizations using cloud communications say provider-level security is critical for ongoing protection and compliance.

Source: Gartner

# The checklist: Assess your phone system security

voipstudio

## Step 1: Check for MFA & encryption

- [ ] Activate multi-factor authentication (MFA) for all admin dashboards and user accounts to block unauthorized access.
- [ ] Ensure your phone system uses end-to-end encryption for calls and messages to protect sensitive data from interception.

## Step 2: Set role-based access controls

- [ ] Assign permissions based on job roles so employees only access what they need.
- [ ] Use separate admin and user accounts to minimize the impact of compromised credentials.

## Step 3: Monitor activity

- [ ] Monitor live and historical analytics to spot unusual call patterns, failed login attempts, or suspicious account behavior.
- [ ] Review detailed audit logs regularly to spot anomalies before they escalate into breaches.

## Step 4: Train your team

- [ ] Run ongoing training sessions on phishing, secure password practices, and safe remote access.
- [ ] Run simulated attack exercises to test employee readiness and reinforce security awareness.

**95%**

Of security breaches are caused by human error. Ongoing training and proactive monitoring are your best defense.

Source: IBM

# Conclusion & Next steps

voipstudio

Securing your cloud business phone system also means safeguarding your customers, your reputation, and your business continuity. **As business and teams scale, the risk surface expands, making robust security practices non-negotiable.**

VoIPstudio equips you with enterprise-grade security features to keep your communications safe and compliant without adding complexity.

- **End-to-end encryption:** Protects calls, messages, and data from interception.
- **Multi-factor authentication (MFA):** Add an extra layer of login security.
- **Role-Based Access Control (RBAC):** Restrict permissions to only what's necessary.
- **Live wallboards:** Spot unusual call patterns and potential threats in real time.
- **Secure data centers:** Infrastructure with built-in redundancy and 24/7 monitoring.
- **Comprehensive logs:** Complete visibility into system activity to support compliance.

Unlock enterprise-class call center power at affordable prices

- Start a free 30-day trial
- Contact us