Business Phone System Security Guide

Protect your VoIP phone system from toll fraud, eavesdropping, and denial-of-service attacks — SIP security, encryption, access control, and compliance.

6	20+	Guide	Free
SECURITY TOPICS	SECURITY CONTROLS	BEST PRACTICE FRAMEWORK	DOWNLOAD NO STRINGS

About This Guide

This guide provides practical, actionable advice for UK businesses. Work through each section to build a comprehensive understanding of the topic. Use the information to make informed decisions and implement best practices.

1 VoIP Security Threats

Understanding the threat landscape is the first step in protecting your phone system from attack.

VoIP systems face a range of threats that traditional phone systems did not. Because VoIP runs over your data network and the internet, it inherits all the **security risks of IP-based communication** plus telephony-specific attack vectors.

- **Toll fraud:** Attackers compromise your VoIP system to make expensive international or premium-rate calls at your expense. UK businesses lose an estimated **£1.2 billion annually** to toll fraud. A compromised system can rack up thousands of pounds in charges overnight.
- **Eavesdropping:** Without encryption, VoIP calls can be intercepted and recorded by anyone with access to the network path. This is trivially easy on unencrypted WiFi networks or compromised switches.
- **Denial of Service (DoS):** Flooding your VoIP system with SIP requests or RTP packets can make it unavailable, preventing all inbound and outbound calls. Targeted DoS attacks on VoIP are increasingly common.
- **Vishing (Voice Phishing):** Attackers use your VoIP system or spoofed caller ID to impersonate your organisation and trick customers, partners, or employees into revealing sensitive information.
- **Man-in-the-Middle (MitM):** Without TLS for signalling and SRTP for media, attackers can intercept and modify call setup, redirecting calls or injecting audio into conversations.
- **Registration hijacking:** Attackers steal SIP credentials to register their own devices as extensions on your system, enabling toll fraud, eavesdropping, and caller ID spoofing.

Real-World Impact

A London law firm lost £32,000 in a single weekend when attackers compromised their VoIP system and routed calls through premium-rate numbers in West Africa. The first indication was the Monday morning phone bill. Preventative security is far cheaper than remediation.

2 SIP Trunk Security

Your SIP trunk is the gateway between your phone system and the public telephone network. Secure it rigorously.

SIP trunks are the most common target for VoIP attacks because they provide direct access to the PSTN for making calls. **Securing your SIP trunk configuration** is your most important defensive measure.

- **Use IP-based access control:** Restrict SIP trunk access to specific IP addresses or ranges. Only your VoIP platform and authorised devices should be able to send SIP traffic through the trunk.
- **Enable SIP authentication:** Require strong username and password authentication for all SIP registrations. Use randomly generated credentials with at least 20 characters — never use default or simple passwords.
- **Enable TLS for SIP signalling:** TLS (Transport Layer Security) encrypts the SIP signalling channel, preventing credentials from being intercepted in transit. Use TLS 1.2 or higher.
- **Implement rate limiting:** Configure your SBC or firewall to limit the number of SIP INVITE requests per second from any single source. This mitigates brute-force registration attacks and SIP flooding.
- **Disable unused SIP methods:** If your system does not use SIP SUBSCRIBE, PUBLISH, or MESSAGE methods, block them at the firewall to reduce the attack surface.
- **Use a Session Border Controller (SBC):** An SBC sits between your phone system and the internet, providing topology hiding, protocol normalisation, and security enforcement for all SIP traffic.

Provider-Side Security

Ask your SIP trunk provider what security measures they implement on their side: fraud detection, call spending alerts, automatic barring of suspicious destinations, and IP-based access control lists. A good provider adds a critical second layer of defence.

3 Toll Fraud Prevention

Toll fraud is the most financially damaging VoIP attack. Layer your defences to prevent it.

Toll fraud prevention requires **multiple layers of protection**. No single measure is sufficient on its own. Implement all of the following controls:

- **Set call spending limits:** Configure daily and weekly call spending caps with your SIP trunk provider. If charges exceed the cap, calls are blocked automatically. Set the cap well above normal usage but low enough to limit fraud damage.
- **Bar premium-rate and international destinations:** Block calls to premium-rate numbers (09xx), international destinations you do not need, and high-cost satellite numbers by default. Whitelist only required international destinations.
- **Restrict out-of-hours calling:** If your business does not make calls outside business hours, configure time-based restrictions to block or alert on any calls made during these periods.
- **Monitor call patterns:** Set up alerts for unusual calling patterns — calls to new international destinations, calls at unusual hours, high call volumes, or abnormally long calls.
- **Secure voicemail systems:** Attackers can use voicemail systems to make outbound calls via DISA (Direct Inward System Access) features. Disable DISA unless absolutely required, and enforce strong voicemail PINs.
- **Audit extension permissions regularly:** Review which extensions have permissions to make international and premium-rate calls. Restrict by default and only enable for users who need it.
- **Enable fraud alerts from your provider:** Most SIP trunk providers offer free fraud alerting services that notify you of suspicious activity. Ensure these are enabled and that alerts reach someone who can act on them immediately.

4 Encryption & SRTP

Encrypt both signalling and media to protect call privacy and prevent man-in-the-middle attacks.

VoIP encryption has two components: **signalling encryption (TLS)** and **media encryption (SRTP)**. Both must be enabled for comprehensive protection. Without encryption, anyone on the network path can capture and listen to your calls using freely available tools.

- **Enable TLS for SIP signalling:** TLS encrypts call setup messages including authentication credentials, caller ID, called number, and routing information. Use TLS 1.2 or higher with strong cipher suites.
- **Enable SRTP for voice media:** Secure Real-time Transport Protocol encrypts the actual voice audio stream. Without SRTP, captured RTP packets can be converted directly into an audio file of the conversation.
- **Use mutual TLS where supported:** Mutual TLS (mTLS) requires both the client and server to authenticate, providing stronger protection against impersonation than standard TLS.
- **Verify certificate management:** TLS certificates must be valid, issued by a trusted CA, and renewed before expiry. Expired certificates cause TLS failures and can revert to unencrypted communication silently.
- **Ensure end-to-end encryption:** Encryption from your phone to the VoIP provider is essential, but understand that calls transiting the PSTN are decrypted at the gateway. For truly sensitive conversations, consider platforms offering end-to-end encryption.
- **Verify handset and softphone support:** Not all desk phones support TLS and SRTP. Check that your deployed hardware supports the encryption standards your VoIP platform requires.

Performance Consideration

Encryption adds processing overhead. Ensure your firewall, SBC, and handsets can handle the additional CPU load without impacting call quality. Modern equipment handles this easily, but older hardware may struggle with large numbers of concurrent encrypted calls.

5 Access Control & Authentication

Restrict who can access and configure your VoIP system to prevent unauthorised changes and abuse.

VoIP system access control follows the same **principles as any IT system security**: least privilege, strong authentication, and comprehensive audit logging.

- **Admin portal access:** Restrict VoIP platform admin access to named individuals with unique accounts. Enable multi-factor authentication for all admin logins without exception.
- **Role-based access control:** Create separate roles for full admin, supervisor (call monitoring, reporting), and user (personal settings only). Do not give everyone admin access.
- **IP-based access restrictions:** Limit admin portal access to specific IP addresses or VPN connections. Do not allow admin access from any public IP address.
- **Strong SIP credentials:** Use randomly generated SIP authentication passwords with at least 20 characters including mixed case, numbers, and symbols. Never reuse credentials across extensions.
- **Voicemail PIN policy:** Require voicemail PINs of at least 6 digits. Block obvious PINs (000000, 123456, repeating digits). Enforce PIN changes every 90 days for users with sensitive voicemails.
- **Audit logging:** Enable comprehensive audit logging for all configuration changes, admin logins, and permission modifications. Review logs weekly for suspicious activity.
- **Deprovisioning process:** When staff leave, immediately disable their VoIP extension, revoke admin access, and change any shared credentials they had access to. Include VoIP in your standard leaver process.

6 Compliance: GDPR & PCI-DSS

VoIP systems process personal data and potentially payment card information. Ensure compliance with relevant regulations.

VoIP systems capture and store **significant amounts of personal data**: call recordings, voicemails, call logs, caller ID information, and potentially payment card details spoken during calls. Compliance with UK GDPR and, where applicable, PCI-DSS is mandatory.

UK GDPR Compliance

- **Inform callers about recording:** If you record calls, you must inform callers at the start of the call. An automated announcement at the auto-attendant stage satisfies this requirement.
- **Define retention periods:** Do not retain call recordings indefinitely. Define retention periods based on legal requirements (typically 6 months for quality, up to 7 years for FCA-regulated firms) and delete recordings after the retention period expires.
- **Honour Subject Access Requests:** You must be able to locate and provide call recordings and call data for a specific individual within 30 days of a SAR. Ensure your system supports searching by caller ID or extension.
- **Secure call recordings:** Recordings must be stored securely with access restricted to authorised personnel only. Encrypt recordings at rest and in transit.

PCI-DSS Compliance

- **Pause recording during card payments:** If agents take card payments over the phone, call recording must be paused during the payment to avoid capturing card numbers. Most VoIP platforms support manual or automatic pause/resume.
- **Use DTMF masking:** For IVR-based payments, implement DTMF masking to prevent card numbers entered via keypad from being captured in recordings or logs.
- **Segment the voice network:** If your VoIP system handles payment card data, it may be in scope for PCI-DSS. Segment voice traffic to minimise the PCI scope and reduce compliance burden.

Compliance Documentation

Document your VoIP compliance measures including call recording policy, retention schedule, access controls, and DSAR process. This documentation is essential for demonstrating accountability under UK GDPR and for PCI-DSS audits.