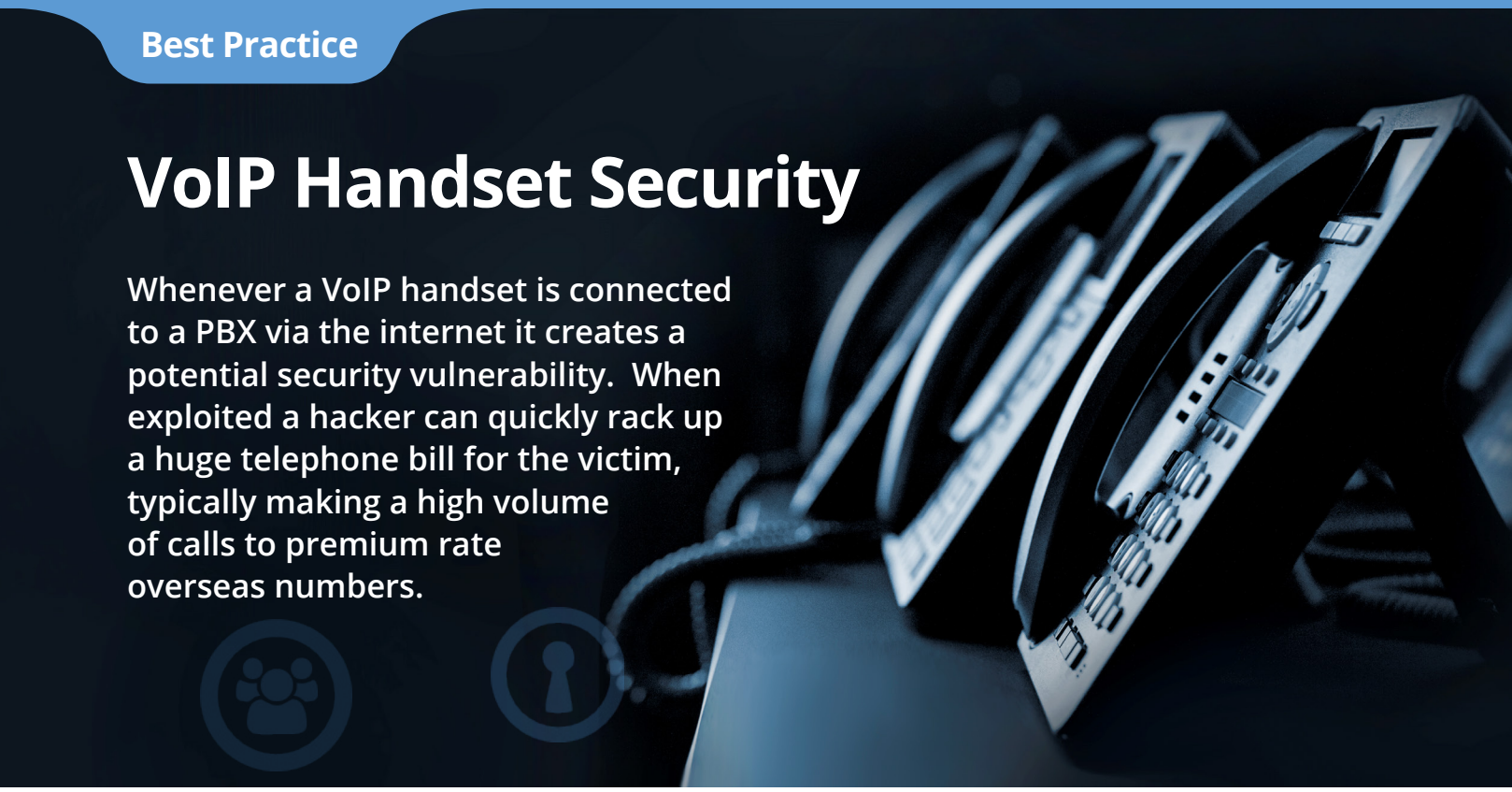
SPITFIRE®
VOICE • INTERNET • WAN

Telecoms and IP Engineering
Solutions for Business since 1988

Best Practice

VoIP Handset Security



Whenever a VoIP handset is connected to a PBX via the internet it creates a potential security vulnerability. When exploited a hacker can quickly rack up a huge telephone bill for the victim, typically making a high volume of calls to premium rate overseas numbers.

What are the vulnerabilities?

- The internet router is poorly configured or unable to prevent malicious attacks
- Remote access to the handset for support provides a back door
- Default passwords in use
- Unused interfaces not disabled
- Outdated, vulnerable firmware
- Unused handsets connected to the network

Spitfire's solution

When Spitfire designs and deploys Cloud telephony solutions, security considerations are paramount. Where possible, Spitfire 'voice-only' circuits are used. While using internet access technologies, these circuits connect the customer site directly to Spitfire's voice network yet provide no access to the internet, thus eliminating many of the vulnerabilities outlined above.

Where converged voice and data circuits or non-Spitfire internet connections are used, security best practice is followed throughout. Read on to understand some of the steps you should take to prevent telephony fraud.

SPITFIRE®
VOICE • INTERNET • WAN

Steps to securing your handset

Where it is not possible to utilise a private Spitfire 'voice-only' circuit the following actions should be taken.

Utilise a business class router or firewall

The router or firewall should be capable of identifying and dropping malicious inbound packets. This feature is often referred to as stateful inspection.

Domestic broadband routers often have minimal security capability.

Configure your router or firewall for security

Your telephone service or Cloud PBX should not require open inbound ports or port forward in order to work. Some routers will allow an inbound connection when an outbound connection is made (in order to allow return traffic). While this may be normal functionality in many cases it is not required for VoIP and will create a vulnerability.

Port forwards are sometimes used to provide remote support for handsets. To mitigate against both of these challenges an access control list should be created to only allow inbound traffic from the Cloud PBX and support provider's IP addresses.

Manage your handset

Handsets are often deployed straight out of the box in default configuration. A few simple steps will address the vulnerabilities that this brings.

Firstly, update the firmware to the latest version to protect against any vulnerabilities that the handset vendor has already addressed. Next change the passwords. Handsets often have multiple interfaces and passwords. For example there may be a web management interface or an API interface as well as the SIP interface. Each of these interfaces will have different credentials.

All interfaces should be disabled if they are not needed and the passwords should be changed using strong passwords.

Where a VoIP handset is no longer in use, ensure it is factory reset, removing all passwords before being disconnected.

Every network and VoIP deployment is different so the above are recommendations only and cannot provide any guarantees in relation to completely preventing telephony fraud.