safe | hotels

HOTEL HACKS

Physical Cybersecurity Tips

Cybercrime is a significant risk for hotels, and recent years have seen high-profile cyberattacks against some of the world's biggest hospitality brands. While there are no guarantees where cybersecurity is concerned, cyber threats can be guarded against by both guests and hotels.

The latest edition of the Safehotels Global Hotel Security Standard© Manual (implemented by hotels participating in the Safehotels Certification program) includes a new section relating to the physical aspects of cyber security.

This booklet contains awareness and action tips to help travellers, and hotel general managers, prevent Hotel Hacks.

1 Policy and procedures

A comprehensive cybersecurity policy, based on an initial risk and threat assessment specific to the hotel, is the foundation of a hotel's cybersecurity program: the stronger and more 'live' the policy, including regular reviews and updates, the better a hotel can guard against cyber threats. Policies need to be written in terms that senior management and front-line staff can understand, not just the IT Manager or those fluent in 'geek speak'.

Many gateway breaches of cybersecurity originate from human interaction and physical threats. In a hotel this can be via a phishing email to an employee; unauthorised individuals having access to IT server rooms and cabinets; physical data collecting devices placed on reception desk computer terminals or in-room guest TVs; breach of cyber-networked CCTV and building facilities management systems; spoof WIFI connections in hotel public areas or executive lounges; and failure to update systems software or change default passwords.

- ✔ **Check that cybersecurity policy and procedures are in place, and that the policy is 'live', regularly reviewed and updated.**
- ✔ **Does the IT Manager responsible for cybersecurity in the hotel understand the policy and can they communicate it clearly to non-IT management, employees and in response to guest enquiries?**
- ✔ **Do all customer-facing employees have at least basic awareness of the cyber policy and know how to manage guest enquiries or requests about cybersecurity?**

safe | hotels

2 Safeguard Guest Data on Check in

Card catching / skimming devices allow criminals to harvest details from guest payment cards and personal information from reception desk terminals. The device will continue to capture data as long as it is attached to the terminal port cable or portable point of sale device. Someone then needs to physically remove the device to retrieve the captured data – in the same way as they would take a USB stick from a lap top or fixed computer terminal.

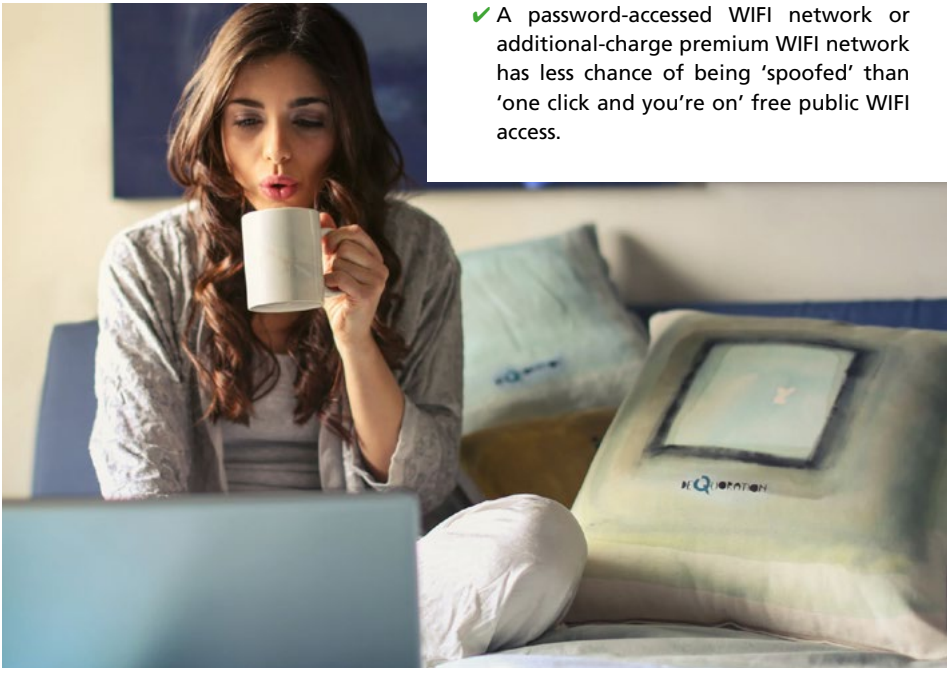
- ✔ Check employees know what data catching devices look like and the different types and methods used.
- ✔ Check employees are trained to check their computer or point of sale devices for suspicious devices. Insist that front office reception staff check terminals at the start of every shift.
- ✔ Encourage a 'challenge culture': employees should feel confident challenging someone accessing ports on computers or point of sale terminals. Is this individual really 'from IT'?

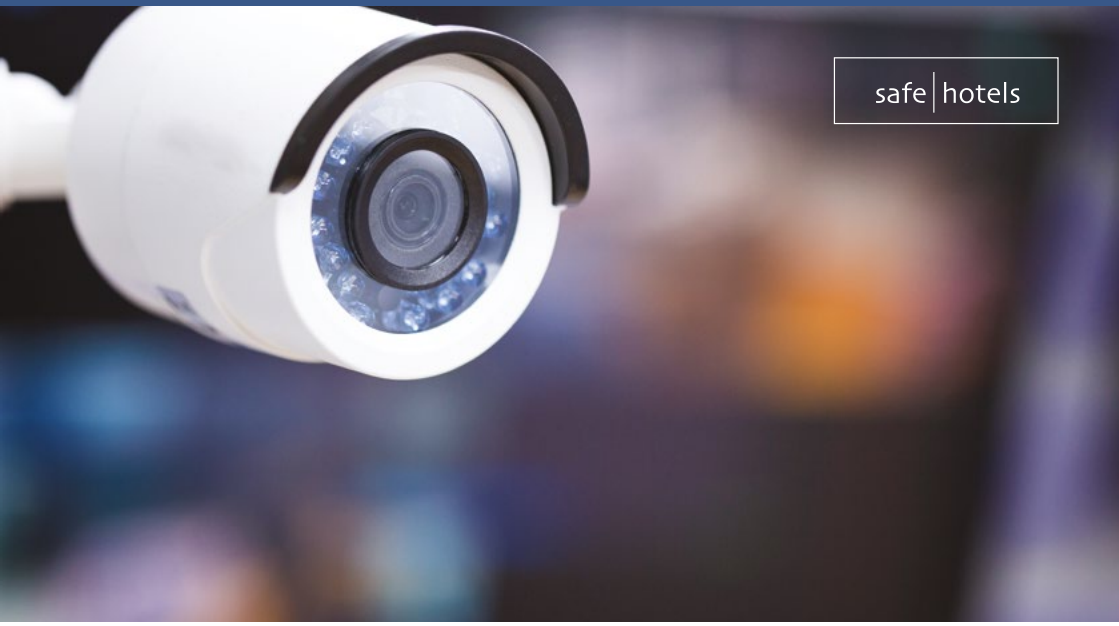
safe | hotels

3 WIFI Connectivity

Most hotel guests want free and instant access hotel WIFI connectivity and more and more hotels are providing this. The reality is the more open and instant access to a WIFI network, the less secure it is. The hotel click-through WIFI terms and conditions of use do not guarantee secure connections: guests usually bear any risk from accessing the WIFI connection. Knowing this, criminals put up 'spoof' WIFI connections in hotel public areas and executive lounges with WIFI addresses similar to the genuine hotel WIFI connection. The guest thinks they are on a secure hotel network when in fact they have entered a criminal's network connection.

- ✔ As a guest, use a VPN when accessing WIFI in a hotel. If the hotel network does not allow a VPN connection, or you are in a country that does not allow VPN, think twice about what type of access you could be exposing your connection to and the type of activity you want to open up when connected. The responsibility and consequences for deciding to access hotel WIFI is usually with the user rather than the provider.
- ✔ As a hotel, check daily if public areas have spoof WIFI connections showing.
- ✔ A password-accessed WIFI network or additional-charge premium WIFI network has less chance of being 'spoofed' than 'one click and you're on' free public WIFI access.





4 | CCTV, Guest Room and Building Facility Management Cyber Security

Remote access is a popular feature for CCTV systems used in hotels because it allows remote viewing, and in some cases remote control, of cameras via the internet. CCTV installers are also able to conduct servicing using remote access via the internet. Without correct security features, remote access hotel CCTV can be subject to malware and ransomware. This means the images of every guest, employee or security function within the hotel could be compromised if cyber security protocols are not in place. Equally, the same applies for remote access building management systems that control the utilities, mechanical and electrical functioning of a hotel.

- ✔ CCTV systems and cameras are sold with remote access enabled by default, and with weak or default password security. Check these are disabled if there is no requirement for remote internet access. If remote access is in use, ensure firewalls, filters and strong passwords, changed from default installation settings, are used.
- ✔ Check both the IT Manager and Security manager understand the network capability set up of the CCTV system and do not leave it 'blindly' to the CCTV installer.
- ✔ Check access to CCTV servers and portable devices, such as USB ports into the system, are secured and restricted.
- ✔ Make sure the hotel has conducted a penetration test on remote-activated security and building management services to see if they can be accessed or taken control of.

About Safehotels

Safehotels operates the Global Hotel Security Standard© – the world's leading safety and security certification standard for the hotel industry. It shows guests and travel buyers that your hotel has been independently assessed to meet more than 270 safety and security standards.

We provide the support, expertise and on-the-ground assessment to help your hotel achieve, and remain compliant with, the Global Hotel Security Standard©.

Safehotels is headquartered in Gothenburg, Sweden, and is present in 16 service hubs in Europe, Africa, Asia and North America.

safe | hotels

People
Integrity
Passion

For expert advice on how you can reduce your physical cyber security risks – and protect your guests and staff with improved hotel safety and security overall – contact **anna@safehotels.com** or visit **safehotels.com**