The Ultimate Guide TO CYBERSECURITY FOR HOTELS

Tips and Best Practices

PANADVERT

The Ultimate Guide to Cybersecurity for Hotels

Tips and Best Practices

Author: Stelios Giannatos
Editor: Maria Dimitriou
Design: Athina Kalomoiri

Contents

Introduction

The hospitality industry is becoming i**ncreasingly dependent on technology to manage its operations and deliver services to its customers**. With the rise of digital systems and online platforms, hotels are now exposed to a range of cyber threats, including data breaches, hacking, and malware attacks. Cybersecurity is a growing concern for hotel owners, managers, and guests alike. As hotel owners and management are trying to provide their best services both online and offline, they need to manage many online platforms and track performance, which means that they are exposed to several risks and it is harder to stay secure.

Introduction

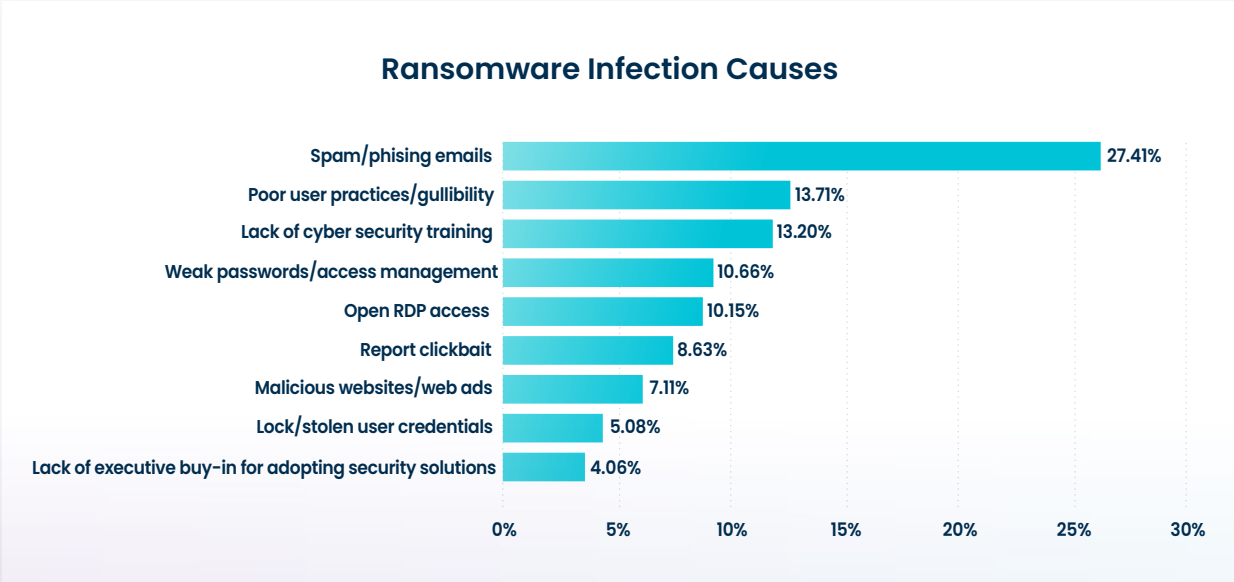
In this manual, we will provide you with in-depth explanations and analysis of each attack, including **social engineering, platform hijacking, session hijacking, network and Wi-Fi attacks, point-of-sale system vulnerabilities, phishing attacks, Wi-Fi eavesdropping and packet sniffing, keycard hacking, and cryptomining**. We will explore the risks and consequences of losing control, how attackers gain access to your data in seconds, and how hackers are exploiting USB sticks and charging cables.

In the first part of the manual, we will examine each of these attacks in detail, helping you understand their nature and scope. In the second part, we will provide you with best practices and tips on how to deal with and avoid these attacks. By following the guidelines outlined in this manual, you can safeguard your hotel's network and data, ensuring the privacy and security of your guests, your staff, and, ultimately, your business.

To get things into perspective

Hotels hold **vast amounts of sensitive customer data**, such as **credit card** details, **passport information**, and **personal contact information**. Cybercriminals seek to steal this information to commit fraud, identity theft, or sell the data on the dark web. Cybersecurity is essential in protecting customer information and avoiding financial and reputational damage to the hotel. Cybercriminals nowadays have a plethora of cyber-weapons they can use to launch an attack both to a client of a hotel or the hotel itself.

Based on data provided by cybersecurity institutes, the US Government and Microsoft's Digital Defense Report from 2022, **the volume of password attacks has risen to an estimated 921 attacks every second – a 74% increase in just one year**. With the latest Graphics Cards, an 8-digit password that includes uppercase and lowercase letters, symbols and numbers, can be brute forced in under 2 hours (depending on the hashing algorithm).



Phishing is by far the most popular way of attacking people in the digital world

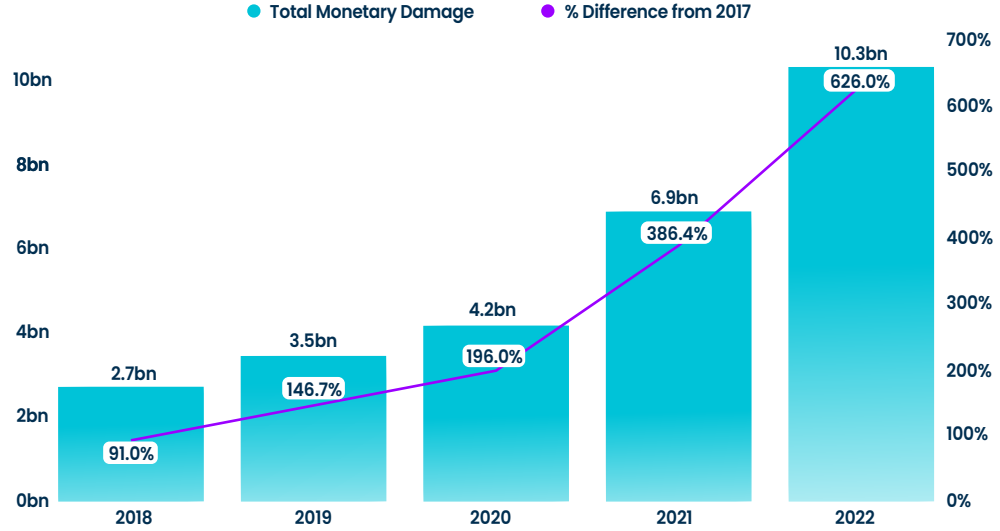
As the data suggests, and many more sources can point out, phishing is by far the most popular way of attacking people in the digital world. The reasons behind this are several; the attacks can be done on a massive scale really fast; the attack directly aims for the wallet and payment methods; the hackers understand that at the end of the day it is all about the numbers, if enough people are exposed to the attack; and, eventually, someone is going get caught in the trap.

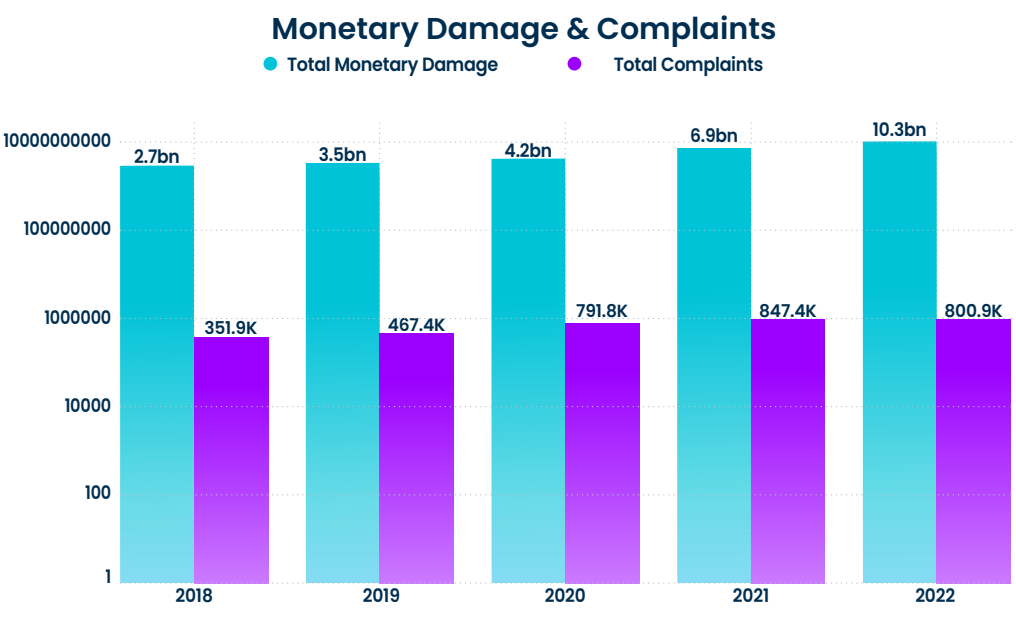
Imagine that a phishing email attack has a success rate of 1%. If the attack reaches one million individuals, the successful attacks would be ten thousand. These attackers tend to scam from a few bucks to a few hundred bucks. Multiplying this, amounts ten thousand times and they have a big sum of stolen money.

Hotels need to protect customer information against phishing

To get things into perspective

In these two graphs, the monetary losses, the percentage increase of losses compared to 2017, and the number of complaints in terms of cyber crime reported by Internet Crime Complaint Center (a division of FBI) are presented:





Hacking and cybercrime have drastically increased as is evident from the aforementioned. The increase **from 2012 to 2022 is a stunning 1,671%**. This means that, **in 10 years**, cybercrime has increased **17 times**, compared to the 2002- 2012 decade, where a 977% increase - which is still quite significant - was recorded.

General Best Practices

Business security and individual security are two vastly different things. When securing a business, the focus is to make a system that works in a secure manner and in a scalable way, while when securing a person, there is some room for manual work for enhanced protection. The best practices and recommendations that are listed below apply to both categories. There are situations where special attention is required though.

General Best Practices

The most important thing that applies to almost every situation, as seen in many cases, is that 20% of action results in 80% of results. Small but important changes have significant and meaningful impact. If we have to say a few things that every business should invest in are the ones following, in no particular order.

Train your staff or raise awareness through physical or digital means

Raising awareness

Even if you cannot afford to have training for your staff, raising awareness through simple means, like providing an informative brochure or some online articles, could be sufficient.

Raising awareness can also be very beneficial for your guests as well, since many incidents can be avoided. This can be done either through physical or digital means:

Physical

- Provide informative brochures at the reception or at a dedicated place within the guest rooms where literature is kept.
- Have the front desk personnel relay some general info to the guests during check-in as well as at check-out and guide them to learn more through the physical brochures or through digital means as mentioned below.

General Best Practices

Digital

- Have a dedicated section at the hotel's website where guests can find information and useful links for further reading about cyber threats and how to keep safe during their stay.
- Include some general information or some external links to relevant articles in the electronic communication with the guests (e.g. in the reservation confirmation email, check-in email, after-check-out email, recurring newsletter etc.).
- Have a dedicated QR code clearly visible at the reception, inside the guest rooms and in places throughout the hotel (e.g. next to wall stickers that mention the hotel Wi-Fi, in or next to the elevators etc.). Guests will be able to very easily scan these QR codes with their phones and they will lead them to the dedicated web page of the hotel mentioned earlier or a relevant web page.
- Before guests are able to connect to the hotel's Wi-Fi there is usually a web page that requires them to input some kind of password, e.g. their room number and last name. At this stage, before they are granted access to the hotel Wi-Fi, some general short warning guidelines and links to read more could be added so that at least the guests keep cybersecurity at the back of their minds.

Provide information and useful links for further reading about cyber threats and how to keep safe during their stay

General Best Practices

Getting training for management and staff

Most phishing attacks, spam email **attacks**, scams, social engineering attacks, unauthorised access breaches, network Wi-Fi attacks and many more can **be avoided by having special training in the field of IT and cybersecurity**. We know training is hard on a larger scale, can be expensive and sometimes not even worth it in cases where job positions constantly change; but it really **does go a long way when a business has staff knowledgeable about the dangers of cybercrime**.

The best recommendation would be to start from the top of the business hierarchy. Personnel with higher access levels should always have cybersecurity in mind. It is like giving your front-door's keys to strangers when one is not considering cybersecurity as a threat. For individual training, online lessons on a platform like Udemy or Coursera is enough. Even minimal action is a lot better than no action at all. For example, **making a password audit** for starters can be of great benefit.

A Password Manager

Having a password manager goes a long way. It is nearly impossible to keep track of all your passwords and also comply with the best practices of password management without using a password manager. **There are many online and offline solutions**. For businesses and individuals that are knowledgeable in terms of IT infrastructures, it is highly recommended to use an offline or self-hosted password management system.

One of the best solutions for businesses and individuals alike is Bitwarden. Bitwarden provides a convenient online solution and a self-hosted option for those that value privacy and are willing to go the extra mile for a combination of security and privacy. Another amazing option, mostly aimed towards the more tech savvy people is KeePass XC, an office-only solution that provides the maximum security.

it is highly recommended to use an offline or self-hosted password management system

The best recommendation would be to start from the top of the business hierarchy. Personnel with higher access levels should always have cybersecurity in mind.

Note that **the setup for all the recommendations is really important**. **It does not matter** if you use the latest and **greatest encryption standards** and a password manager **if you reuse the same password**, have a password with small length, do not have a secure infrastructure etc. For example, self-hosting Bitwarden offers both convenience and protection but if there are misconfigurations, they are in a worse situation than before. **A prime example of misconfiguration in self-hosting is not using encryption in your network**. Typically, with self-hosted tools the organisation would create a VPN network using encryption in combination with a solution like Cloudflare, in order to have authorised personnel only have access to the internal network of the company. Finally, encryption for the local connections of the network with a solution like Let's Encrypt, which is free and open-source, is required.

General Best Practices

If there is a lack of encryption or unauthorised access is granted, the entire structure will collapse while you have also taken a huge risk by having your entire organisation's passwords in one place. **KeePassXC**, which is not self-hosted, does not offer the convenience of other applications, but it is the **best solution in terms of security**. However, if you use a weak master password, the encrypted database is going to be cracked no matter what.

In terms of online password managers, besides Bitward, **we also recommend Dashlane and 1Password**, since none of the three have ever publicly been tied to a security breach. These options provide both security and convenience because they work completely online and, most commonly, only require the use of a browser plugin to function.

if you use a weak master password, the encrypted database is going to be cracked no matter what

A very important note: The major browsers' built-in password managers should be turned off. In the section "How Hackers Are Exploiting USB Sticks & Charging Cables" the most commonly used way of obtaining password that will be described is via the browser's auto-fill and autosave feature. In general, it is recommended turning this feature off for all browsers, even in the case of not using a password manager.

Use an Antivirus

To prevent malware from causing damage to your system it is **strongly recommended to use antivirus programs**, which can recognize, quarantine, or delete hazardous programs.

It is common practice for antivirus software to hash a program and check on a list of malicious hashes. If the program is considered malicious, no more operations are required and it is flagged as malicious.

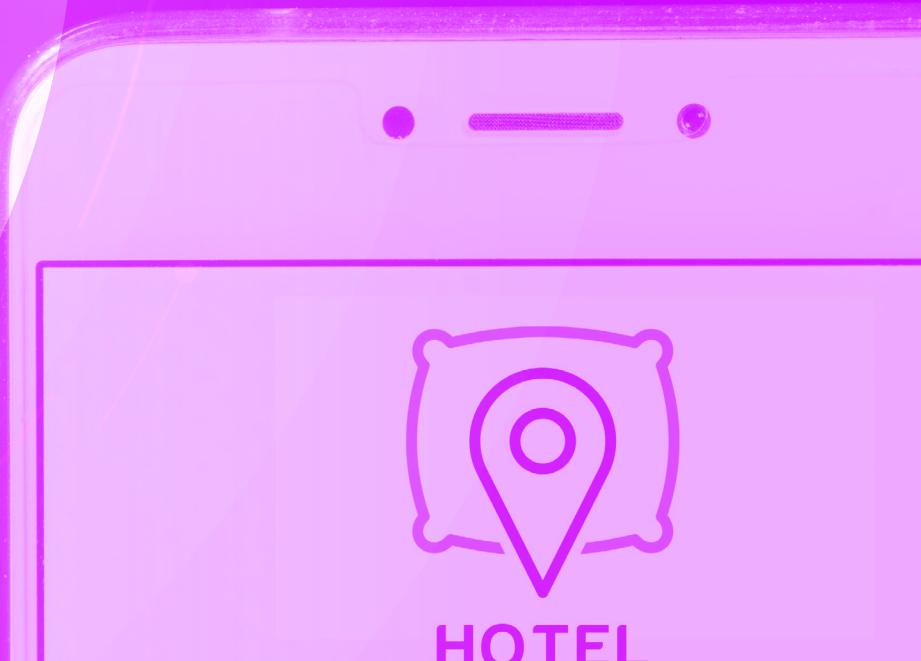
In the early days of the internet, antivirus programs would use only this method to determine if a software is malicious. For example, Microsoft released the first edition of Microsoft word. The hash of the official program is calculated. If a user has the original, but with a single bite different. The antivirus software back in the day would mark the program as malicious. Nowadays there are many more methods for an antivirus to detect if a software is malicious beyond hashing, but it is still a prominent method for saving resources. Contemporary antivirus software also continually updates itself in order to provide protection against the most recent viruses and malware.

A great platform for checking malicious programs based on the hash is VirusTotal. The hash of the program/website will be calculated and checked on lists of hashes from many antivirus companies. A paid alternative would be intezer. The best options for an antivirus software for download would be Kaspersi and Bitdefender.

Hotels and Hackers

Exploring the threats to the business

Hotels are exposed to a wide range of cyber assaults aimed at their internet platforms, systems, and client data. **These assaults can have** severe effects, like **financial loss, reputational harm, and legal liability.** In this section, we will explore the many forms of assaults that hotels may face, and the dangers and repercussions that come with it.



1 SOCIAL ENGINEERING

Social engineering is described as deceiving and manipulating a victim in order to take advantage of their position. For hotels, this may mean elevated access. A very prominent example in the hotel industry and in the digital world is what is called **pretexting, which happens when an individual presents themselves as a staff member**, typically as a front desk employee, and asks guests for sensitive information or access to valuable resources. For instance, a scammer may ask for a guest's credit card information in order to validate their stay or in order to supposedly fix a payment issue. The phone number might as well be from within the hotel so that it is harder to trace and more convincing to the guest.

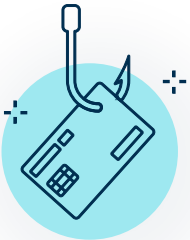
Hotels are exposed to a wide range of cyber assaults

Another example may be to ask if they have used the hotel's vault, and, after obtaining this information they will try to find a matching keycard or steal a staff keycard, in order to access the room of the individual. Other useful information for someone with such power might be when the room of a guest is empty; this way, a scammer might inform the staff that some issues with the equipment in the room were detected and gain unauthorised access in order to steal valuables and other belongings.

1.1. The case of Hilton

A very famous social engineering case was with Hilton Hotels in 2014, which involved a hacker group that compromised the computer systems of the major hotel chain. They sent out spear-phishing attacks - a kind of phishing attack that aims to infiltrate high profile targets by using malicious links in emails - with sophisticated emails that made the senders and source look legitimate. After the malicious software was installed on the devices of the Hilton hotels, they were able to steal sensitive data including credit card information.

Malicious links in e-mails & installment of malicious software



Spear-phishing attacks & credit card theft

1 SOCIAL ENGINEERING

1.2. How to steer clear of Social Engineering

Social Engineering is one of those types of attacks where having gotten **proper cybersecurity training can be incredibly useful**. As it was seen in the graph "Ransomware Infection Cases", **13.71% of the total cases occur due to poor user practices, 13.2% due to lack of cyber security training, and 4.06% due to lack of executive buy-in for adopting security solutions.**

In general, the most important aspect of protection is understanding what the vulnerabilities are. When knowing how an attack works and what the attacker thinks, we can take the appropriate countermeasures. In the case of Social Engineering, the attacker most of the time does either of two things; they want to be the exception to a situation or they want to blend in very well. This involves being very familiar with how company policies and operations are.

The best way to avoid falling victim to Social Engineering attacks, especially in a business environment, is to have **strict and well thought-out policies. We can never assume anything about anyone.** Some form of authentication should be needed in order to access private information regarding the customers in cases of impersonation. **In more sophisticated attacks, an organised system should be in place.** In addition, it is crucial to have specific operations in place for certain situations and rules to be taken seriously by all employees. This way, anything out of the ordinary will stand out.

All hotel guests should also be informed and reminded about what the operations of the hotel are, how they are being conducted, and that no sensitive information is going to be requested from them via phone. This is a very good first step, so that **all issues** regarding visitors are going to take place **face-to-face at the front desk**. In the case the hotel needs to contact guests via online platforms, it is recommended that this conversation take place **either through the online travel agency**, for example booking.com if the reservation took place from there, or either contact the guest **directly via an email address that belongs to the hotel** and has the domain name of the hotel in the email address. For instance, if you make a hotel reservation through a website that is hilton.com, you should expect a message from *someusername@hilton.com* that proves that the user name corresponds to an actual employee of the hotel.

All hotel guests should also be informed and reminded about what the operations of the hotel are, how they are being conducted, and that no sensitive information is going to be requested from them via phone.

2 PLATFORM HIJACKING

2.1. The risks and consequences of losing control

Platform hijacking is when a bad actor obtains access to computer systems, software programs and network connections. For example, in the hotel's property management system (PMS), **a criminal has real-time access to a customer's sensitive information**. This data can be divided into two categories:

1. Personal Information

- First and last name
- Address
- Contact details
- Nationality and ethnicity
- ID or Passport information
- Email address
- Phone number

2. Reservation details

- Arrival and departure dates
- Room type
- Room rate
- Any special requests
- Billing information
- Financial background
- Loyalty program information
- Dietary restrictions
- Room location preferences
- Communication history
- Preferences for promotional emails and offers
- Reservations for restaurants, spas, and other amenities within the hotel

2 PLATFORM HIJACKING

2.1. The risks and consequences of losing control [Continued]

Cyber hijacking also includes the loss of access to a business platform/profile and the **unauthorised access of a malicious actor**. These platforms, including the property management system mentioned above, are the following:

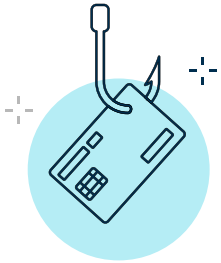
- Instagram Account
- Facebook Account
- LinkedIn Account
- Pinterest Account
- Ad platforms
- Content Management System
- Website back-end server access
- Google accounts
- Internal analytics tools
- Booking Engine
- Domain registrar

The Content Management System is **a platform like Wordpress**, which allows the publication and management of different types of content on a website, **which is the backbone of the online image of any property**. For hotels, however, a website plays an even more significant role; it is what creates trust for the client and reflects the professionalism and the entire philosophy and ideology behind the property.

An example of hijacking in this case is bad actors having access to the hotel's website, meaning they are able to edit the content and make changes, while the property owners, management, and developers are locked out.

Most bad actors in this situation would blackmail the owners for some sort of payment in order to reclaim access to their accounts.

Bad actors having access to the hotel's website



Blackmailing with some sort of payment in order to reclaim access to their accounts

2 PLATFORM HIJACKING

2.1. The risks and consequences of losing control [Continued]

But what if the hackers are determined to destroy the hotel's reputation? In that case, they could start uploading malicious files, trying to infect potential customers and potentially redirect traffic to a website where they are completely in charge, in order to steal even more information from potential clients, like credit card information from a fake booking engine.

If a hacker in a similar situation **has access to the social media** platforms of the hotel, they **can do** some really **serious damage to the brand name of the hotel**. The idea of losing the hotel's entire fanbase alone can be frightening, particularly when one considers the potential consequences of a rogue individual controlling the hotel's Facebook or Instagram accounts and publishing inappropriate content. The resulting damage to the brand, therefore, could be significant. This applies to all social media platforms mentioned above.

Hackers upload malicious files, trying to infect potential customers

In the case of a breach in the domain name registrar, the consequences are even more severe. Your registrar serves as the most significant and vulnerable point of failure. In the event that your registrar is compromised by hackers, they can gain full control over your domain name, allowing them to redirect it to any destination of their choosing. Furthermore, they even have the ability to transfer ownership of your domain name to an unauthorised third party, which can result in far-reaching consequences for your organisation.

To put this in perspective, let's say in a hypothetical scenario that the domain *facebook.com* is hacked in the way described above. The hackers would be able to transfer the domain to a different platform and have access to all email addresses and aliases. They would also have full access to change anything and everything they would like regarding the website, since the registrar certifies the ownership of a domain name. If someone had access to this, then, it is like they own the domain, which, in the case of our hypothetical scenario, the hackers would literally own facebook.com.

In the case of Facebook, the domain is under the RegistrarSafe or RegistrarSEC registrar, which are ICANN-accredited registrars based in Delaware, and are wholly-owned subsidiaries of Meta Platforms. This tends to be the case with many big enterprises, so this makes our example just a point of reference for the amount of damage a breach like that would cause. It is unlikely for huge players in the digital world to experience such a breach, however.

With that being said, not every company can afford to have this solution and may be forced to make do with retail registrar sellers like GoDaddy and Namecheap, so the best thing one can do is to secure their business' domain as much as possible by using a strong password and two-factor authentication.

2 PLATFORM HIJACKING

2.2. How to protect your business from platform hijacking

The most effective way of protecting an online account from platform hijacking is to have a strong password and use multi-authentication. Security is a trade-off with convenience in most cases. There are situations when a user sacrifices small portions of convenience and gains a lot of security but there are also the opposite cases. One should start from the cases where little to no convenience is sacrificed and then start exploring the more advanced options available.

The method used as the most common best practice for this kind of attack is to use a password manager. This, surprisingly, is actually one of the cases where both security and convenience are enhanced, especially in a business environment, where there are many passwords and accounts connected to multiple users. Having a password manager is essential and helps the users manage their accounts more easily. Of course all this depends on the password manager, as was analysed earlier.

The next step would be to add a **multi-factor authentication method**, usually referred to as **two-factor authenticator or 2FA**. The most effective method of multi-factor authentication is by far **hardware authentication**, which involves having a **physical key, like a Yubikey**, to use with RFID or via USB. This ensures that the person logging in to your account also has physical access to this key, which they likely have on their person all the time. We can understand, thus, that this makes it really hard to log in to their account without actually being the owner of the account.

This, however, may not work in a business environment. For example, a hotel might have dedicated staff for managing their social media accounts, which would mean that the account needs to have one key for each person managing the social media and, additionally, one for the owner. This makes it very easy to lose a key or get locked out of an account, despite providing the most security conceptually.

The most effective way of protecting an online account from platform hijacking is to have a strong password and use multi-authentication.

2 PLATFORM HIJACKING

2.2. How to protect your business from platform hijacking [Continued]

The next best option is using an **authenticator application**. These applications are usually mobile apps. The best picks in terms of security alone, in no particular order, would be the following:

- Authy
- Google Authenticator
- Duo authenticator
- Aegis Authenticator
- OTP

With the last two options being open-source applications, it is important to keep in mind that back-up codes for each account are mandatory. If a user loses access to their phone, sometimes they may not be able to recover their two-factor authenticators and get locked out of their account. The other methods available for authentication are not considered secure, like authentication by SMS or via email.

It is recommended, therefore, that a password should be at least 16 characters in length, and should include uppercase/lowercase letters, numbers, and symbols.

In terms of **password strength**, attacks are more focused on phishing in recent years and making a user give out their credentials, instead of brute forcing the password. With that being said, dictionary attacks and brute force attacks are still very popular means of password cracking. As mentioned in the introduction, the latest graphics cards working in clusters can crack a strong 8-digit password in under 2 hours. It is recommended, therefore, that a password should be at least 16 characters in length, and should include uppercase/lowercase letters, numbers, and symbols. This will ensure that hijacking an account with brute force methods would be very difficult and time-consuming. In the case of phishing and social engineering, the only thing a user can do is to be informed and cautious when using their credentials.

3 SESSION HIJACKING

Session hijacking is the process of obtaining the **session cookies** of an individual to impersonate their browser. This usually happens by gaining access to the Operating System (OS) of the platform. But before deep-diving into the Cybersecurity aspect of cookies and how they can be used maliciously, let's start from square one.

3.1. What are cookies?

Cookies are data files that store information regarding browsing activity, preferences, login details and more. This information is stored on your device by the website you visit. There are many types of cookies, that are used for different purposes, as listed below:

1. **Session cookies:** The session cookie is a server-specific cookie that cannot be passed to any device other than the one that generated the cookie. The session cookie allows the browser to re-identify itself to the single, unique server to which the client had previously authenticated.
2. **Persistent cookies:** A persistent cookie is a file stored on a user's computer that remembers information, settings, preferences, or sign-in credentials that the user has previously saved. This saves time and creates a more convenient website experience. Web Servers set an expiration date on these cookies.
3. **First-party cookies:** These cookies are directly stored by the website (or domain) you visit. They allow website owners to collect analytics data, remember language settings, and perform other useful functions that provide a good user experience.
4. **Third-party cookies:** Third-party cookies are all the cookies on a website that are placed by any other site, such as an advertiser or social media site.
5. **Analytics cookies:** Analytics cookies or performance cookies are used to track website visitors and their user behaviour. This data is then used to improve the way the website works and, in turn, improve the user experience. Google Analytics cookies are one of the most common analytics cookies set by websites.
6. **Advertising cookies:** They allow advertisers to profile their target customers with unprecedented accuracy. At its core, an advertising cookie catalogues the behaviour of all users on a particular website.

Cookies are data files that store information regarding browsing activity, preferences, login details and more

The cookies hackers intend to steal in order to impersonate a user are the **session cookies**. By stealing them, they can even by-pass multi-factor authentication and log in altogether to all platforms you have previously logged on. After getting these cookies they could straight up replace their own browser cookies - if the stolen ones are not encrypted - and successfully manage to by-pass any sort of security a site possesses.

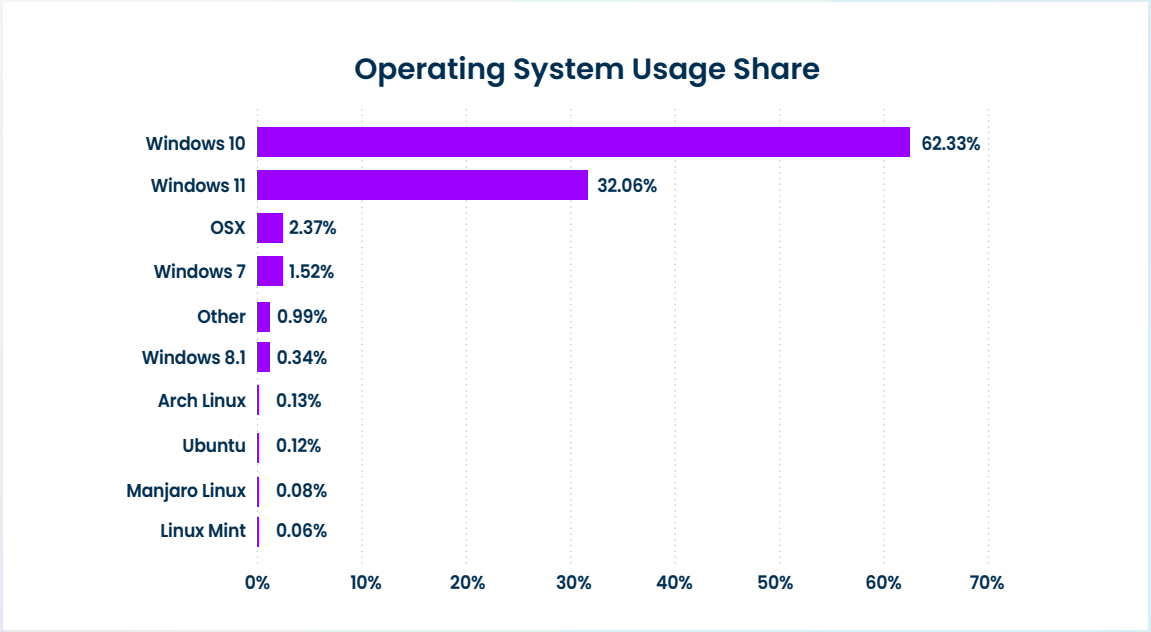
3 SESSION HIJACKING

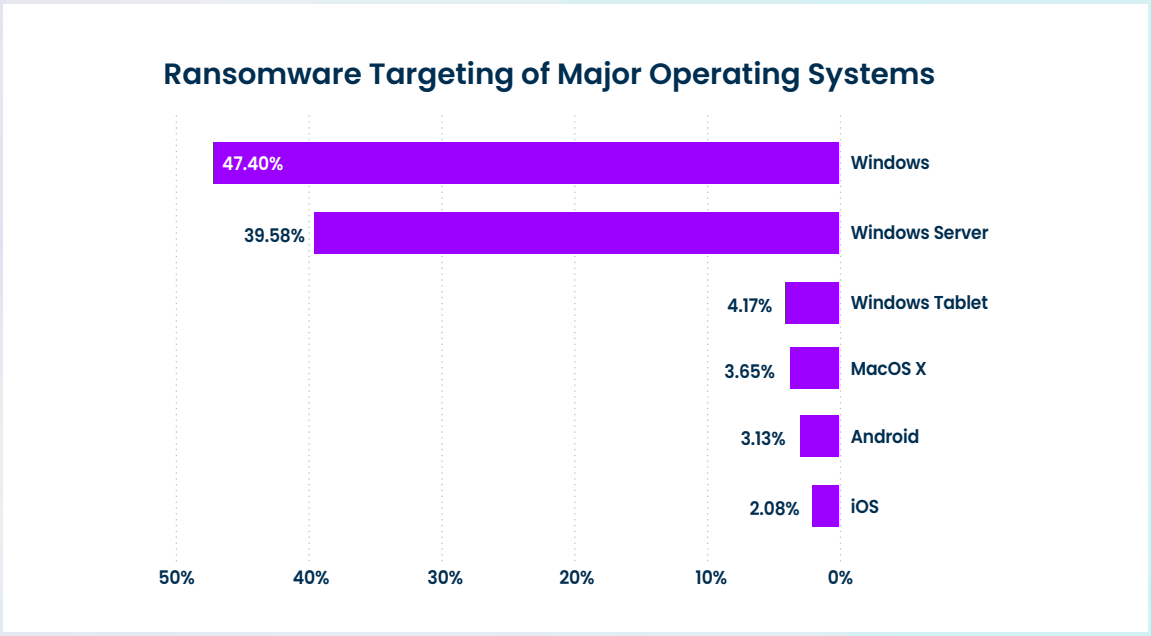
3.2. How attackers gain access to your data in seconds through your OS

Viruses and attacks are tailored towards the most famous options in the market since there is more potential for profit. There are cases of making tools to hack unpopular OS, but, most of the time these are made because a specific company or individual is targeted by hackers.

First, let's take a look below, where statistics can be found in terms of **Operating System Usage Share** and the number of viruses made per Operating System as well as the targeting of ransomware to said Operating Systems. Note that "Other" is considered to be other Linux Distros.

Note that **Windows server** is not presented in the first graph, since the data refer to Operating Systems used by day-to-day users, whereas Windows servers are more tailored to businesses. Perhaps the most interesting thing to note is that **Linux** is responsible for 1.38% of the entire OS usage share, but the amount of ransomware for Linux is almost non-existent compared to other OS. It is also worth mentioning that the Windows 2019 server update is based on Windows 10, meaning almost all viruses tailored for Windows 10 will most likely work for the Windows 2019 server, but not necessarily the other way around.





3 SESSION HIJACKING

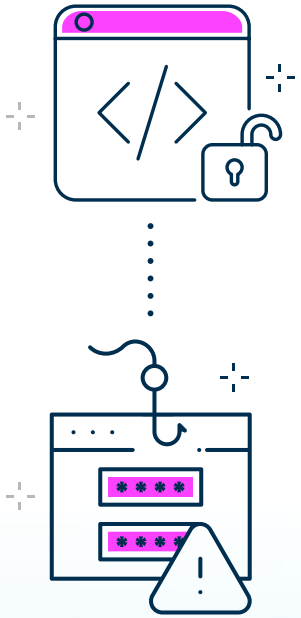
3.2. How attackers gain access to your data in seconds through your OS

There are many open-source and free software that can be used to access and steal all the cookies from a browser including all the saved passwords.

These typically gather all passwords and cookies of all browsers present in the targeted device. Additional information hackers can extract by accessing your Windows device physically may include:

- Windows product keys
- Stored passwords (Web browsers, Clients' email addresses, Network connections)
- Detailed system and hardware information
- Insight on active network connections
- Wi-Fi network details
- Recover deleted files
- Wi-Fi passwords of all the networks the device has connected to (applies mostly to laptops)
- Network traffic
- Browser history and caches
- Startup programs
- Hidden passwords revealed in various applications
- All the devices ever connected using the USB interface
- Processes and services running
- System event logs
- Installed software and drivers
- Hidden files

All the information above can be extracted in seconds if all the software is loaded in a USB stick and run simultaneously using a command line. Each program would, then, create a file with all the information that can be extracted from the device to which it is connected. Hence, a hacker would need access to an unattended device for less than a minute in order to extract all of the information mentioned.



3 SESSION HIJACKING

3.3. How hackers are exploiting USB sticks & Charging Cables

As stated before, attackers nowadays have more tools than ever at their disposal, with a lot of these tools being physical tools, with the **USB stick** being the most prominent example. The USB storage stick is one of the most popular compact storage solutions in the modern era and has been weaponized by hackers to engage in malicious behaviour. The simplest - and most common - way a hacker can use a USB in a malicious way is to load it with malware, backdoor software and other forms of viruses, and transfer all this to a hotel staff computer in order to gain information, access usernames and passwords, cookies etc.

Bad actors or blackhat hackers can infect a device by approaching individuals or somehow manage to get the individuals to approach a third party they control in order to give them free electronic devices that, when used, are going to give them **backdoor remote access to all the devices they desire**. More often than not, the way these devices end up on someone's computer is by attending a public event and having the event organisers give away free merchandise; USB sticks, for instance, are a really common gift in tech-related events, in particular.

The hacker, thus, would have to either have prior access to the merchandise that is going to be given away for free or mix their malicious devices with the event giveaway ones. The only difference between the two options is the scale; in the first case, the bad actor would be able to swap and replace the original event merchandise with their own, while, in the second case, the bad actor could toss their malicious devices into a batch of the original devices sent out by the event organisers.

One method hackers use to achieve this is by using the **USB drive-by method** on Windows PCs. This involves the hacker attaching a microcontroller onto a USB device (usually USB sticks and other storage devices) and loading that controller module with code that, when plugged into a Windows device, it would execute applications or imitate the mouse and keyboard to disable the antivirus, download, and execute malicious software they have uploaded in a public repository on the Internet.

The exact same hacking idea works with Android and iPhone devices as well, with the difference that this time the hacking occurs through the **charging USB cables**. A malicious USB cable with inserted modified controllers can access information on the victim's phone or Windows PC, download and execute malicious software, and create backdoors for hackers to remotely access, and, in the case of the phone, track your device's precise location.

The simplest - and most common - way a hacker can use a USB in a malicious way is to load it with malware, backdoor software and other forms of viruses, and transfer all this to a hotel staff computer in order to gain information, access usernames and passwords, cookies etc.

3 SESSION HIJACKING

3.4. How to protect your OS to avoid cookie stealing & USB attacks

The best options to protect your devices in the case of a virus attack either from cookie stealing or from inserting malware via a USB, are the two most basic and fundamental rules that have already been mentioned: Proper training and antivirus software.

When it comes to OS, hackers primarily target popular operating systems and use various malicious tools to gain access to sensitive information quickly and efficiently on a large scale. Most likely, the most - if not all - PCs at hotels use Windows with some exceptions of Mac PCs and developers who most likely use some Linux Distro. Hence, since most users use the same operating systems, it is logical that most viruses are tailored to Windows devices.

The best course of action against cookie stealing and USB attacks - besides proper training for staff and a good antivirus software - is being **very strict with who can access the devices** that staff operate on. Additionally, **all devices should require a password** to access the computer while computers with sensitive information should be kept at a safe location.

For example, someone should **always be present at the front desk** of the hotel, because if an attacker sees the opportunity to attack, they will. Unattended systems, especially laptops, thus, are vulnerable, because they can be very easily stolen. From the moment an attacker gets access to the device without a staff of the hotel supervising, the situation is going to escalate very rapidly. Cookie stealing can happen with remote attacks as well.

4 NETWORK & WI-FI ATTACKS

In this section, we are going to focus on the **risks regarding hotel network and Wi-Fi attacks**. Wi-fi attacks are usually conducted when a hacker is in the vicinity of the hotel and it could pose a threat both for hotels and for their guests.

4.1. Why IoT devices are unreliable

Nowadays, Internet of Things (IoT) devices are everywhere, and, perhaps the most widely used is the router that everyone uses to connect to the Internet. Typically, though, IoT devices are trying to cut as much cost as possible in order to have 'smart' functionalities while also having competitive prices. Hence, this means that **manufacturers cut corners in the security of the software, which results in lower protection from cyber threats and network intruders** that wish to steal data.

Wi-fi attacks are usually conducted when a hacker is in the vicinity of the hotel

4.2. Getting access to your router

Once a hacker has access to the router, they have access to the entire map of your network. The first thing hackers will try to do in order to infiltrate a network is **get access through the main access point**. Hackers know that routers have the ability to create 'guest mode' access points, which are regular networks with regular network access for the standard user, but it limits the amount of resources a user has - typically the kind of resources a standard user is not interested in. In order to access the main network, the bad actor would need to approach either a computer with a wired connection or an employee's device with access to the main network, get the Wi-Fi credentials and log in.

If the hacker wants to get initial access to the main network, they could visit the hotel during a period when it is not very crowded and scan all **Wi-Fi networks** in order to eliminate the prospect of hidden networks. The next step is to **make a hotspot using their laptop by implementing the same** SSID, which imitates the actual networks and enables them to log in with the credentials of the actual network as long as an employee with authorised access enters within the vicinity of the hotspot and try to access the network through their personal device. The connection, however, would fail since the hacker does not know the actual credentials. The credentials provided through the employee's device are going to get stored and used to access the main network, and the hotspot would be disabled.

After that, the hacker would need to check if there is wireless isolation **(AP Isolation)**. When wireless isolation is present, it means that the access to different resources are compiled into silos or segments. Below are four examples of network isolation:

- Isolated wireless devices can not see other users/devices logged on to the same Wi-Fi network (a.k.a. SSID).
- Isolated wireless devices can not see users/devices on other Wi-Fi networks created by the router.
- Isolated devices can not see any device connected via Ethernet to the router.
- Isolated devices can not directly access the router. Even if they know the user ID/password to log in to the router, they are prevented from loading the routers login web page.

4 NETWORK & WI-FI ATTACKS

4.2. Getting access to your router [Continued]

The last of the four examples is where hackers would want to focus on, as, if there is network isolation, a hacker would need to turn their device into one with enough access to log in to the router or find a wired access point, which in most routers is enough to bypass the isolation mode. Next, they would need to get the credentials of the router. If the router has a physical location and the initial credentials have not been changed, the hacker could just flip the router upside down, take a picture and get hold of the credentials.

A more sophisticated way they could do this is by a **'man-in-the-middle' attack** as was described earlier. The hacker would get in-between the router and all devices connected to the network. They would, then, try to make the connection bad on purpose so that a technician would try to log in to the router, and they would intercept the packets from the technician's device and the router. Since most router interfaces are HTTP sites and not HTTPS by default, the credentials would be in plain text.

After that, it's game over; the hacker could do something really drastic, like disable all Wi-Fi connections, log out all devices on the network and change the settings or sabotage. But the most likely course of action would be a **silent attack that users would not be able to easily detect**, thus, they would not realise immediately that they are being attacked. Here is a visualisation of a router network note whose IP address depends on the router manufacturer:

To put it more simply, a hacker with access to the precise location of your devices (the IP) can take control of that device; from changing your thermostat settings and schedule to man-in-the-middle attacks.

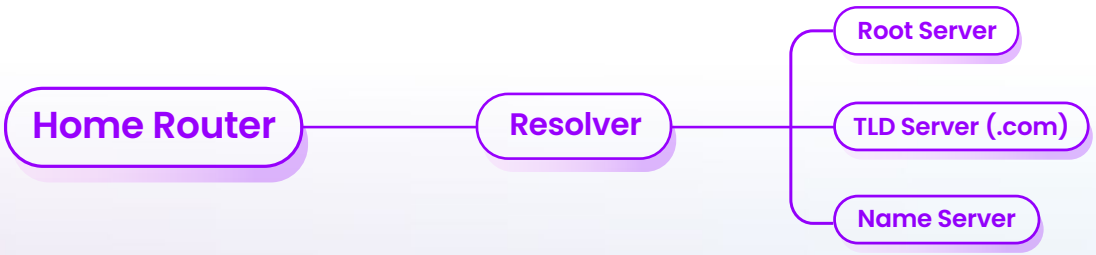
A 'man-in-the-middle' attack where the hacker would get in-between the router and all devices connected to the network

4 NETWORK & WI-FI ATTACKS

4.3. DNS Hijacking

Taking all these into consideration, the most suitable attack for a business like a hotel would be **DNS Hijacking**, where **DNS** stands for **Domain Name System**. When someone searches for a website, for example google.com, our router needs to connect with a server somewhere on the Internet. The first step for the computer to connect to that website is to contact the router and ask for the IP address of the server that corresponds to the domain specified (in our case, google.com). If the IP address is not cached (stored) in the router, the router would contact your ISP (Internet Service Provider, i.e. Cosmote, Vodafone, Wind etc.).

In the rare case where your ISP does not have the website cached, the next step is to contact a Resolver. The resolver would take you to one out of the thirteen DNS nameservers which contain an index of all the up to date TLD (Top-Level Domain) servers. Each responsible for a different TLD, the nameserver would take you to the TLD server that is responsible for ".com" and the TLD server would forward the query request to the authoritative name server (Name Server in the graph below). The name server would then return the correlation between the domain google.com with the IP of the Google server. A visualisation can be seen below:



DNS hijacking, thus, occurs in the router. The hacker would redirect all **queries/requests** to a local IP address of one of their own devices. This means that once a user has searched for google.com (after caches have been cleared or for new network devices) the hacker is going to redirect the user to a different website. This at first seems like a minor inconvenience, but hackers will not present a different website - they will present an exact copy of google.com that is going to copy all your credentials upon login. After the login attempt, the fake website is going to redirect you to the real google.com. While all this is happening, the user would have no idea that a redirection has taken place, but the **passwords** of their account would have been **leaked**.

4 NETWORK & WI-FI ATTACKS

4.3. DNS Hijacking [Continued]

In the case of Google, if a user uses Google Chrome and has sync enabled, the hacker could be able to use the newly-acquired credentials, login to the account and sync all their browsing data. These data typically include:

- Bookmarks
- History
- Autofill information: Form data, such as names, addresses, phone numbers, and email addresses
- Passwords
- Extensions
- Apps
- Open tabs
- Themes and settings
- Payment methods
- Search engines

So, basically, with access to merely one account, a hacker can have access to all your passwords and many more. Thus, we can imagine that, if this were to happen to a hotel, the scale would be **many times larger than that of a home network**.

With access to merely one account, a hacker can have access to all your passwords

The following example is not directly related to hacking, but more related to cybersecurity in general. One common issue hotel owners and management face is guests exploiting their free Wi-Fi access to download huge files and a lot of times pirate copyrighted content. There have been cases in the past where hotel owners were charged with a **heavy fine** due to the fact that they did not secure their network enough and allowed guests to freely pirate content.

4 NETWORK & WI-FI ATTACKS

4.4. Exploring the Vulnerabilities of Point-of-Sale (POS) Systems

POS systems share a very similar structure with IoT devices mentioned above and are another prominent device that is used to manage thousands of transactions every day. Hotels, of course, are one of the places where POS devices are used consistently, so, it is crucial to understand how bad actors may be able to exploit them in order to gain access to data and payment info.

POS devices face the same issues as any IoT devices mentioned above, as the manufacturers tend to cut costs and, by doing so, cut corners in terms of security. They most likely use some sort of password protection platform and run on one of the most popular operating systems such as Windows, iOS, Android or Linux, depending on the manufacturer. The major difference between POS and IoT devices, though, is that some of them are cloud-based with one of the OS mentioned and mostly work with a permanent internet connection and the servers of the provider handle the transaction and inventory part.

The most common issue POS devices face is the password-related vulnerability issue that was mentioned earlier, which - if exploited - grants unauthorised individuals access to the account that the POS is registered to. All settings regarding the POS are on that account, so, if the hacker also gets physical access to the POS device they can change everything about it, and could even change the payment method of the specific POS so that all the transactions made using this device are going to the hacker's account, which most likely is not their real account, but a hacked account they have access to.

On the hardware side, the vulnerabilities are the same as any Operating System. Hackers can create backdoors and have remote access to the POS device anytime from any location they please if they successfully manage to install software on it. This, however, is harder for a hacker to achieve due to the architecture of the POS devices, so they most likely will not go for such an attack, but it is still a possibility. Additionally, It is worth mentioning that **malware and ransomware are still possible attacks;** the owner of the POS will most likely not be able to access the OS, the device will be rendered useless and the only reasonable way of resolving the issue would be to contact the POS provider.

Hackers can create backdoors and have remote access to the POS device anytime from any location they please if they successfully manage to install software on it.

4 NETWORK & WI-FI ATTACKS

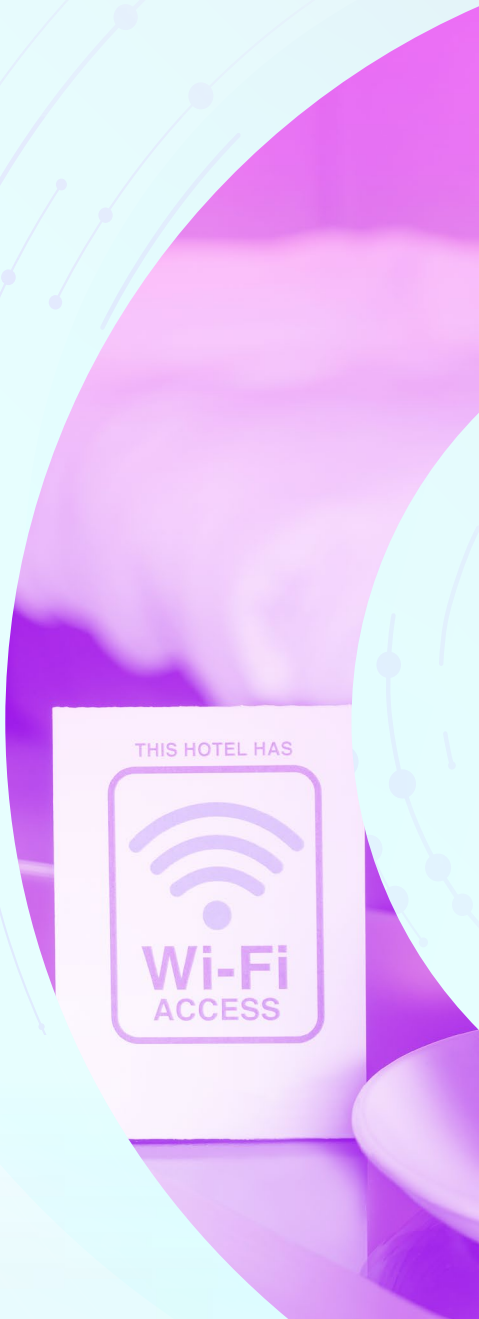
4.5. How to protect your network from Wi-Fi attacks

Network isolation should also be turned on and the router firmware should be updated regularly.

There are several ways you could go about dealing with those kinds of attacks. The first step - which is also the easiest - is to use a strong Wi-Fi password and the latest encryption standard, which is WPA3 as of today for all Wi-Fi networks. Network segmentation should be turned on and configured so that guests, employees, POS, and management are on different networks. It is recommended that the default router provided by the ISP is also changed, since ISPs usually try to cut costs as do most businesses. The routers provided, thus, tend to provide little customisation and security options. Routers may be expensive, but are worth every penny of the cost for the features they provide. Network isolation should also be turned on and the router firmware should be updated regularly.

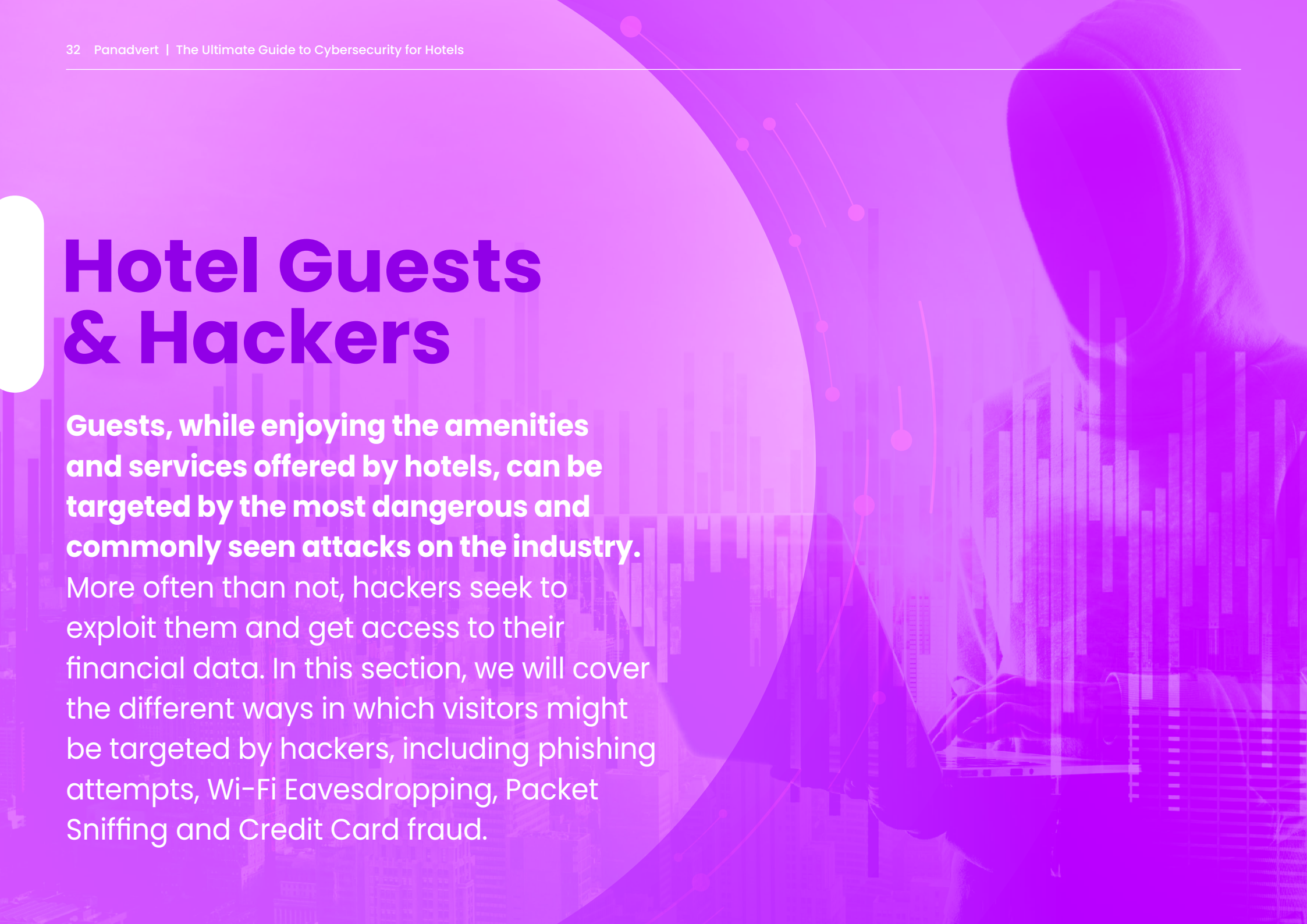
In terms of IoT devices, they should be on their own network, separate from guest user networks and employees' networks. **Firmware updates should also be implemented in the devices that support updating. The most practical thing, that in most situations can be accommodated at a hotel Wi-Fi is bandwidth limiting.** It is also recommended to block access to malicious websites, torrent websites and fraud-related websites. It is highly recommended, when it comes to networks, to hire a professional to take care of all the networking and setup for all IoT devices. Point-of-Sale Systems can be secured in the same manner.

Routers may be expensive, but are worth every penny of the cost for the features they provide



Hotel Guests & Hackers

Guests, while enjoying the amenities and services offered by hotels, can be targeted by the most dangerous and commonly seen attacks on the industry. More often than not, hackers seek to exploit them and get access to their financial data. In this section, we will cover the different ways in which visitors might be targeted by hackers, including phishing attempts, Wi-Fi Eavesdropping, Packet Sniffing and Credit Card fraud.



5 DEFINING PHISHING ATTACKS

Phishing is the act of impersonating an individual or a company in order to steal, deceive or infect unsuspected victims with viruses. Usually, these attacks are conducted via email, or other communication platforms that allow conversation with strangers. The goal of the perpetrator is to trick users into sharing personal information. Cybercriminals may pose as the hotel or hotel staff, requesting customers to click on malicious links or attachments that contain malware or to provide personal information directly. It is by far the most popular attack, because it can be sent to millions of users simultaneously.

5.1. Preventing Phishing Attacks

Most of the best practices in terms of protection have already been mentioned. Having said that, **the most important protection measure would be to always be on the lookout**. When blackhats contact you, they will eventually ask for some sort of payment or they will try to make you install software on your device. **Be on the lookout for these people.**

Their email address will probably be a newly made email address. Since Google, Microsoft and other tech giants have good security measures, their email accounts do not last long, thus, they are always on the move and making new email addresses. **A common thing this type of scammers do is to change the name of the email address to that of a legitimate company. Therefore, always check the email address of the sender.** When companies contact individuals, they will have an email address containing the domain name of the website as mentioned in the section '1.2. How to steer clear of Social Engineering'.

Another method hackers use to intimidate users is to find a password that is connected to their account in some way, most commonly from a database leak, and straight up request money because they supposedly have compromised your device with the credentials they acquired. **A way to check if your accounts or passwords have been in a database leak is to visit** Have i Been Pwned. There is a section for email address and a section for a password. The accounts compromised under the email section **should be changed immediately**. The passwords

Cybercriminals may pose as the hotel or hotel staff, requesting customers to click on malicious links or attachments that contain malware or to provide personal information directly.

that are compromised are also recommended to be changed. The key difference is that the password section shows if your password has ever been compromised in the past while the email section shows if your account has been compromised.

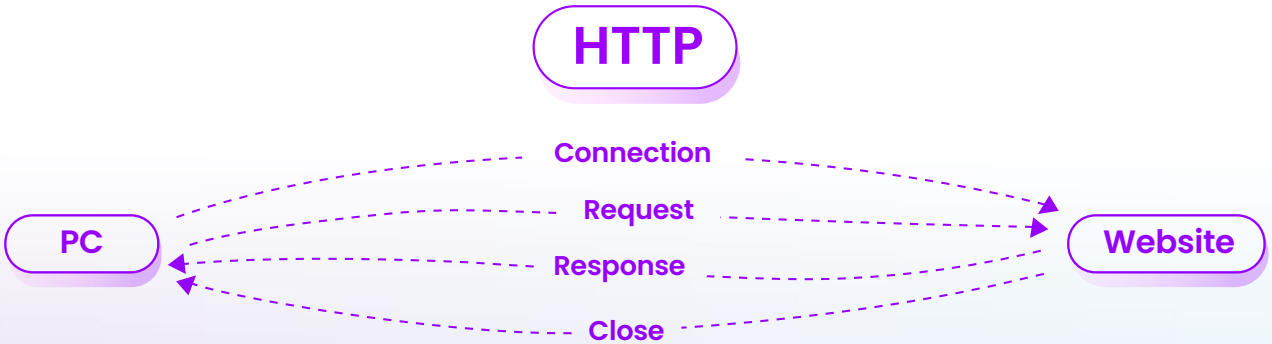
The passwords that are compromised are also recommended to be changed.

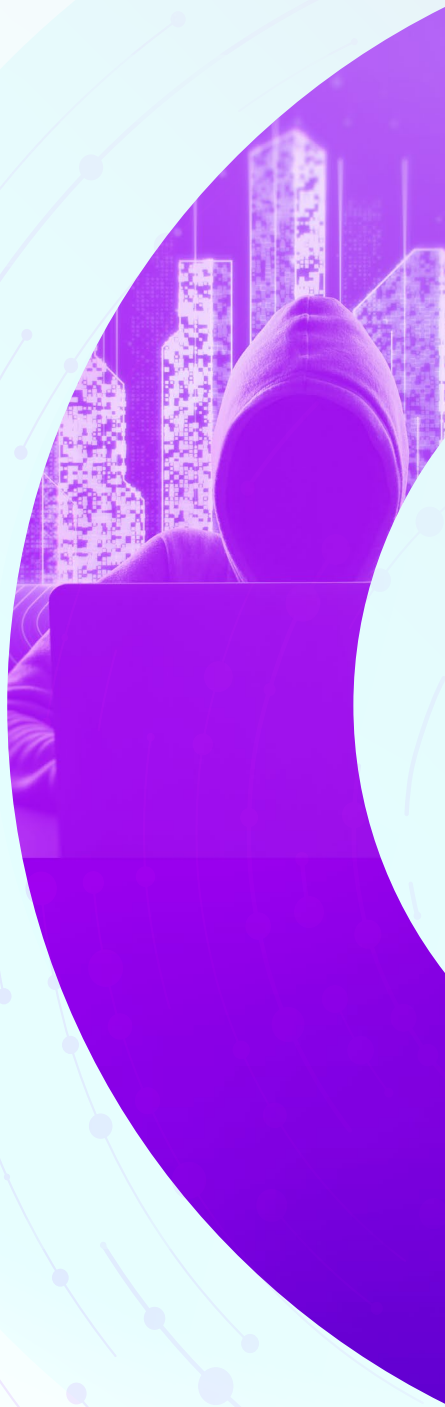
6 UNRAVELLING THE DANGERS OF WI-FI EAVESDROPPING AND PACKET SNIFFING

Wi-Fi Eavesdropping, as mentioned in the '[Network & Wi-Fi Attacks]' section, is when hackers set up a hotspot that copies the name of the Hotel's Wi-Fi. **It is also referred to as the '[Evil Twin]' attack.** The difference, in this case, is that the hacker instead of targeting the hotel targets the guest/user.

The key in this situation is for the hacker to have already acquired access to the Wi-Fi or for the Wi-Fi to be available for free. **In this situation the most common goal of the hacker is to perform [SSL stripping] and man-in-the-middle attacks on the users connected to the 'evil twin' Wi-Fi**. SSL stands for Secure Socket Layer and it is a standard defined before 1995, yet the first version was never published due to security flaws. It is the predecessor of currently used [TLS 1.2], and, even though TLS 1.3 has been published since, it hasn't surpassed TLS 1.2 in popularity, but it is most likely present in the most popular browsers.

The process of stripping SSL is to remove the encryption of a website and have all information passed from the user in plain text. This can be achieved in a small-scale DNS poisoning fashion as mentioned earlier, where the hacker would redirect the user to a copy of the website the user is trying to access or redirect the users to use the HTTP version of the website instead of HTTPS. The diagram below shows how HTTP works in a very simplistic manner without involving the [TPC/IP handshake].





6 UNRAVELLING THE DANGERS OF WI-FI EAVESDROPPING AND PACKET SNIFFING

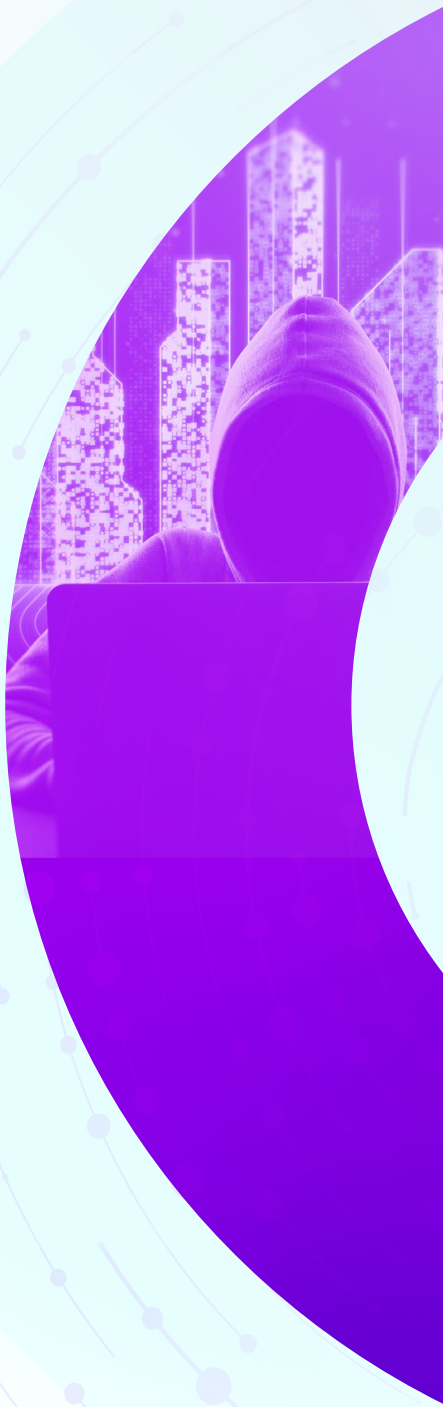
HTTPS works the same way, but with asynchronous encryption, meaning that the encryption algorithm uses a key pair instead of a single key to encrypt and decrypt information. If the encryption is removed from the equation, the hacker can rebuild all the information using a program like Wireshark or any other packet sniffing tool. The information transmitted is all the information the end-user is presented with when using any application or website. For example, if a user falls victim to this attack, and they log in to a platform or website like Instagra≠m, their username/email and password is visible to the hacker along with all the information that loads with the website/application.

This information includes:

- Conversations with other users
- Photos of other users
- Usernames of the friend list of the user

If a user falls victim to an attack, and they log in to a platform or website like Instagram, their username/email and password is visible to the hacker along with all the information that loads with the website/application.

Basically everything the user can see with the application open, like their feed, is totally visible to the hacker since the information transmitted is no longer encrypted. The connection does not have to be intercepted at this level though. If the information is in plain text, it is all the way through, meaning that in each network hop there is a chance your information is intercepted. Note that for the hacker it is as easy as setting a filter specifying they are interested only in HTTP connections.



6 UNRAVELLING THE DANGERS OF WI-FI EAVESDROPPING AND PACKET SNIFFING

The simplest and most effective method of protection is to make sure all connections used online are using encryption.

6.1. Protection against Wi-fi Eavesdropping and packet sniffing

Chrome-based browsers show a lock to the left of the website URL. In the absence of encryption, in the same location the browsers would prompt 'Not Secure'.

It is advised to not use free Wi-Fi access points, as they tend to use less secure methods of connection and are potential hotspots of 'Evil Twin' attacks. Best practice would be to use your own mobile data when abroad. In the case of a hotel, it would be best to use a wired connection with an ethernet cable and disable Wi-Fi altogether.

Another commonly referred method is to use a VPN. It is not recommended to use a VPN service, since it requires trust in the service provider. Sometimes the VPN server is possible to get hacked, so a user that is not using a VPN can be more secure in comparison. If a user would want to implement a VPN it is best to host their own VPN and use a service like cloudflare tunnel to ensure a secure connection.

Finally, in order to be safe in terms of clone websites, **you should always check the URL of the website**. When hosting a domain or a local domain, the hacker cannot use the official domain name. Hence, it is guaranteed that they are going to use either a completely different domain or a domain that is really close to the real domain. In the case of facebook.com, for example they might use facbook.com. The only way to use the actual domain is by DNS Hijacking.

6.2. Protection Against DNS Hijacking

Best method to counter DNS hijacking is by using a custom DNS. **The best DNS one can use would be cloudflare's DNS which is 1.1.1.1 or quad9 DNS which is 9.9.9.9, these account both for privacy and security**. Another secure alternative is google's DNS which is 8.8.8.8. Note that all DNS providers have alternatives in the case the original does not function properly.

It is advised to not use free Wi-Fi access points. Best practice would be to use your own mobile data when abroad.

7 CRYPTOMINING

Cryptomining, also referred to as cryptojacking, is an attack usually delivered in the form of crypto-malware software.

The device of an individual can be compromised by the usual phishing methods, backdoors, other viruses and unauthorised use of one's device. It is a relatively new form of malware that recently went over the roof due to the popularity of the cryptomining scene.

7.1. A few things about crypto

Cryptocurrencies are based on cryptography for the transactions executed and for the verification of transactions. Like most things that need to be transferred online, cryptography uses asymmetric encryption, a concept mentioned earlier in the article. Cryptocurrencies make use of digital wallets and can theoretically be considered a form of online payment. Not many websites allow the use of cryptocurrencies, even in the modern era, due to the reliance on the blockchain, the heavily fluctuating prices and the fact that, in order to get your money, you need to resale the cryptocurrency received.

Crypto can also be mined in most cases, the most popular and powerful coins, however, have moved to proof-of-stake, meaning these cryptocurrencies cannot be mined anymore. The most popular one that recently moved to this kind of proof-of-stake is Ethereum. A prime example of the exact opposite, which is called proof-of-work (basically mining), is utilised by Bitcoin. The process of mining a coin relies on the Graphics card of the device as it is the most efficient unit (compared to the processor) for hashing. This is how hackers create viruses.

7 CRYPTOMINING

7.2. Crypto-malware

Modern hackers make use of stealth options and tools that are really hard to detect as a process instead of trolling the user and constantly presenting pop-ups. This way, they make sure they can use as many of the device's resources as they can for a longer period of time.

There is malicious software that detects the presence of task managers and can stop their intensive work processing, meaning that an unsuspected user might feel that their device is getting slower, but when they open the task manager, they see low percentages of utilisation. This can be a really hard attack for even intermediates to detect. The machine infected, thus, is going to constantly run software that is going to mine for a specific wallet online.

Even if the user finds the wallet that their machine is unwillingly mining, they cannot do much. The best they can do is report the wallet on platforms that support reporting. Imagine now the described scenario in hundreds or millions of devices that, every time they run, they mine cryptocurrencies for an individual; they basically get free money without any electricity bills or any hardware hosts.

A hotel is a place where many people come together with vastly different backgrounds in computing knowledge.

Crypto-malware, like DDoS (explained below), are mostly targeted at older people or people that are not familiar with technology, as they are the perfect individuals to have these viruses running on their device for a really long time. How does this tie in with your hotel? A hotel is a place where many people come together with vastly different backgrounds in computing knowledge. Building on top of our previous case, a user that connects to the hotspot of a hacker is susceptible to malicious software due to the reasons mentioned in the previous section.

Another way **hackers manage to install malicious software on one's device is through Facebook and YouTube advertisements.** They make a click-bait title, a good looking thumbnail and a malicious executable behind-the-scenes and that is all they need. They can still impersonate a hotel, copy the advertisements or make new advertisements with publicly accessible materials; all they have to use is the brand name. The only form of defence, thus, your business can use is to own an expensive trademark for the brand name, which, in most cases, is not a viable option. Hence, they mostly rely on the online platform to detect and take down these attempts.

7.3. How to avoid being infected with crypto-malware

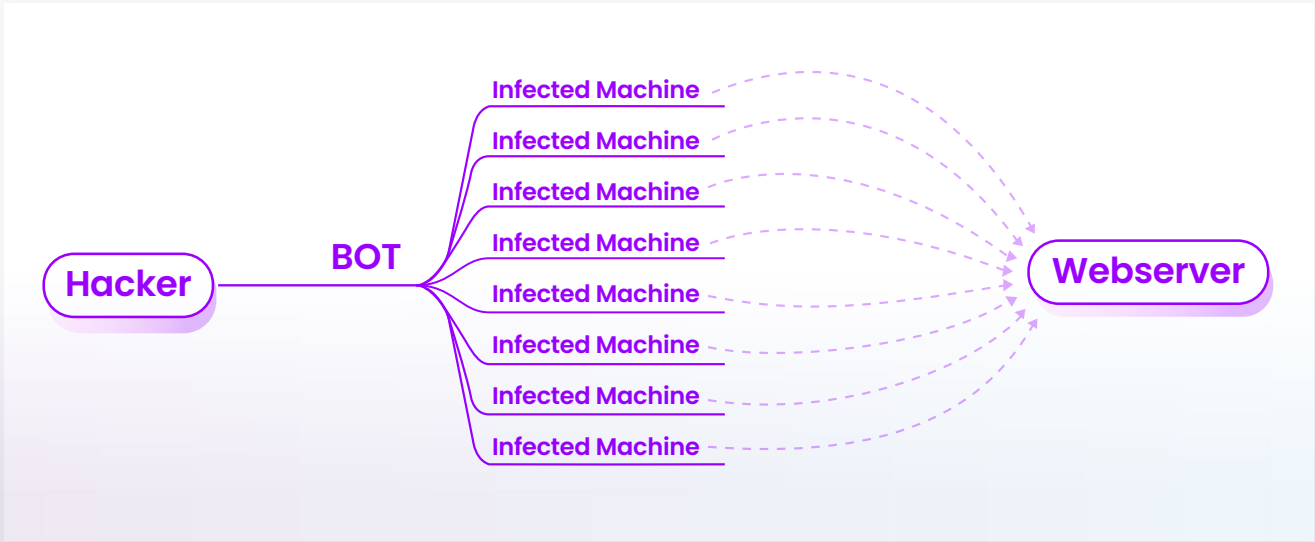
From the user side, **the best practices have already been mentioned, as the distribution of these attacks are from malicious software that, in general, is detectable by antivirus software**. Same goes for crypto-malware and cryptomining attacks. It is also important that guests are aware of these types of attacks and how they could be detected.

The hotel could provide information to the guests about this kind of threat whether physically or digitally by raising awareness about hacking.

8 DISTRIBUTED DENIAL OF SERVICE (DDOS)

Another attack hackers can perform on guests, either on the premises of the hotel or remotely, is Distributed Denial of Service (DDoS). DDoS is an attack that can happen on the hotel's website but it can also be distributed through the hotel, and it is when many devices are infected with a stealth virus and can be controlled remotely to make requests on the Internet. When this virus is distributed to several devices, just like crypto-malware, it gives a lot of power to the hacker that controls the virus.

They, then, can use their network of hacked devices to make thousands or even millions of requests to a specific website in order to take it down. The hosting server of the website is going to detect that there is a lot of traffic that they cannot or they are not getting paid to cover and they take the website down for a short amount of time. It is one of the very few attacks that can affect guests and the hotel at the same time. A diagram of a DDoS scheme can be seen below:



DDoS is an attack that can happen on the hotel's website but it can also be distributed through the hotel.

The bot that is there indicates that the hacker does not have to manually give instructions to each device individually, but they give the instructions to a custom bot they have created prior to the attack in order to control the network of infected devices.

8.1. How to battle DDoS

In terms of DDoS protection, **the best bet is to use a hosting service that has strong security, is popular in the market, and can provide enough resources for the needs of your hotel's website**. From the user side, the best practices have already been mentioned, as the distribution of these attacks are from malicious software that, in general, is detectable by antivirus software, as well as being aware about this kind of cyber-threat.

9 KEY CARD HACKING

In today's digitally connected world, **cryptographic key pass invasion** poses an increasing threat, as it takes advantage of weak points in electronic locking mechanisms to give access to unlawfully secured areas. With more facilities opting for electronic security systems due to their ease and perceived safety, it is crucial to comprehend the risks associated with **key pass intrusions**, the frailties of electronic locking systems, and the necessary preventive and remedial actions to safeguard your enterprise and personal interests.

9.1. Comprehending Electronic Locking Apparatus

Electronically managed locking devices predominantly function via magnetic strip cards or contactless intelligent cards. **Magnetic strip cards** retain data within a magnetic strip akin to a bank card, which is accessed by the lock when swiped. Alternatively, **contactless intelligent cards** utilise Radio-Frequency Identification (RFID) or Near-Field Communication (NFC) technologies, permitting users to unlock doors by placing the card in proximity to the reader.

9.2. Key Card invasion

Illegal Entrance: Key pass invasions allow lawbreakers to get unauthorised access to hotel rooms, offices, or other secure locations, allowing for pilferage, espionage, and other malicious acts. This might result in the loss of expensive belongings, secret data, or even endanger personal safety.

Intrusion of Seclusion and Reputational Erosion: Cyber criminals who successfully penetrate electronic locks might violate an individual's privacy by accessing rooms without their knowledge or consent. This invasion of privacy can cause anguish and a sense of vulnerability. Businesses, particularly hotels, can then suffer significant reputational degradation when their electronic security systems are breached, as customers may lose trust in the institution, causing a downturn in clientele and revenue.

Legal and Monetary Ramifications: If a business fails to sufficiently secure its premises, it may be held responsible for losses, damages, or injuries arising from key pass invasions. This could lead to expensive legal disputes and monetary consequences.

9 KEY CARD HACKING

9.3. Key Card system faults

Duplication and Eavesdropping: Cyber felons can duplicate magnetic strip cards by transferring data to a vacant card using a card encoder. In the case of RFID or NFC cards, culprits can employ eavesdropping apparatuses to intercept card information when in close range. With this data, they can create a facsimile card or utilise a smartphone to imitate the card's functionality.

Brute Force Attack Methods: Intruders can apply exhaustive assault techniques to produce and test various code combinations until the accurate one is identified. Though time-consuming, this approach can prove fruitful, particularly when the electronic locking system employs feeble encryption or predictable coding patterns.

Flaws in Software and Firmware: Electronic locking mechanisms may exhibit weak points in their software or firmware, which trespassers can exploit to unlawfully access them. Such occurrences may be attributed to substandard coding practices, infrequent updates, or the utilisation of obsolete systems.

Psychological Manipulation: Cyber felons may resort to psychological manipulation strategies, such as impersonating hotel personnel, to acquire key passes or access codes from unsuspecting victims. In some instances, they may even compromise the hotel's computer infrastructure to issue new key passes for their own usage.

9.4. How to secure the hotel's Key Cards

The best practice is to upgrade to a smart key card system that uses contactless and encrypted keycards or any solution that is not susceptible to cloning. Moreover, a **pin code or** biometrics should be required to access restricted areas of the hotel on top of the keycard protection. In terms of **auditing and logs**, it is recommended to use some form of access control system that would monitor keycard use.

A new keycard should be allowed on the network with the information of the time created, and, in many systems, which account the keycard was created on, i.e. front desk, to be present in the log files. If a security breach takes place, thus, more information can be given to the local police for finding the people responsible for the cloning.

The best practice is to upgrade to a smart key card system that uses contactless and encrypted keycards or any solution that is not susceptible to cloning.

A pin code or biometrics should be required to access restricted areas of the hotel on top of the keycard protection.

Conclusion

In conclusion, the value of cybersecurity in the hospitality business cannot be emphasised enough. As technology evolves and becomes more intertwined with our daily lives, so does the potential for cyber dangers. This guide has discussed social engineering, platform hijacking, cookie theft, USB attacks, operating systems, network and Wi-Fi protection, cryptomining, DDoS assaults, and keycard protection.

Hotel management needs to be one step ahead of hackers and cybercriminals, and are advised to use the latest protocols and security features available. Hotels can considerably minimise their exposure to cyberattacks by using the best practices and guidelines given in order to protect their guest's personal information and guarantee a secure and enjoyable experience for all.