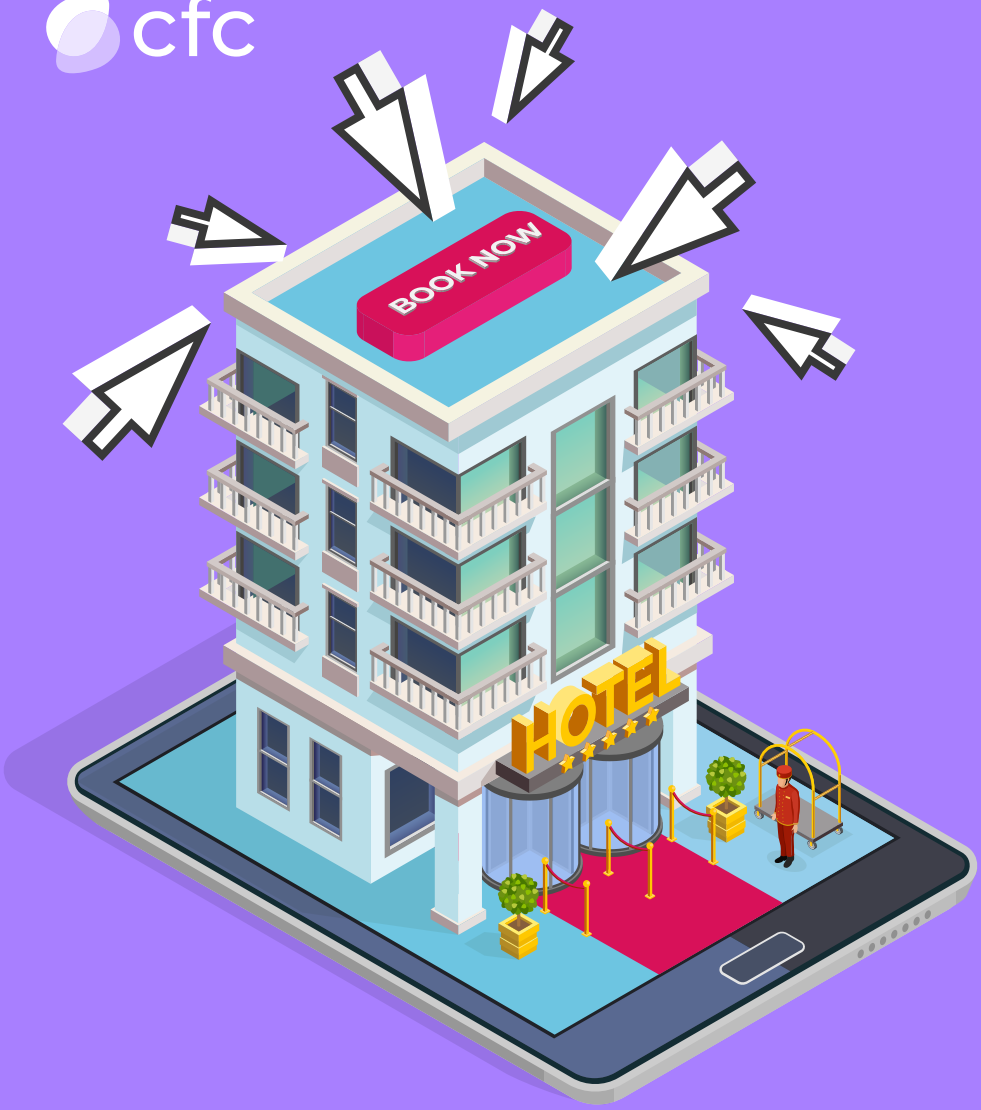

Case study

Search engine setback

When malicious code impairs a hotel's website, it takes longer than expected to get back on track

Over the past two decades, technology has transformed the way businesses operate, and most now depend on their computer systems in one way or another. In particular, the dawn of the internet has opened up a world of opportunity for many businesses, allowing them to reach new markets and increase their revenues. However, these new opportunities also bring new exposures. With many businesses now increasingly reliant on online sales, they are potentially vulnerable to financial losses should their websites become inaccessible to their customers.

One of our policyholders affected by such a loss was a hotel. The hotel operates out of one location in a city popular with tourists throughout the year, but with notable peaks during the spring and summer. Although bookings can be made by telephone or through travel agents, many guests choose to book online through the hotel's website, and thus the hotel is reliant on the smooth functioning of its website.

Cryptojacking causes crashes

The incident began when hackers managed to infiltrate the hotel's website and insert malicious code in the background, seemingly for the purpose of cryptocurrency mining (sometimes referred to as cryptojacking). The basic idea behind cryptocurrency mining is that instead of having to purchase cryptocurrency, individuals can also use computer processing power to verify cryptocurrency transactions and get a portion of cryptocurrency as a reward. **The more computer processing power that an individual has under their control, the quicker they can verify transactions** and mine cryptocurrency.

And this is where the concept of cryptojacking comes in. Rather than bearing all of the processing costs associated with cryptocurrency mining themselves, hackers look to make use of other people's computing resources without their consent to verify more transactions and make more money.

Cryptojacking is usually carried out in two main ways. Either the hackers dupe victims into downloading cryptocurrency mining software onto their computer systems, typically delivered as a link or attachment in a phishing email, or they insert malicious code onto websites or online advertisements and **the cryptomining code works in the background while a visitor to the website browses on that page.** The latter is what happened to the hotel's website.

> The malicious code inserted by the hackers had a particularly debilitating effect on the hotel's website.

In many cases, the business running a website which has been subject to cryptojacking may not even notice the presence of the malicious code working in the background. However, in some cases **the introduction of malicious code can have unintended consequences.**

In this instance, the malicious code that had been inserted by the hackers had a particularly debilitating effect on the hotel's website. **The site started to run very slowly and was subject to intermittent crashes;** staff members were unable to login to the site; and bookings were unable to be processed correctly.

Drop in ranking creates drop in sales

Noticing that something was clearly wrong, it was at this point that the hotel contacted CFC's incident response team. Working with the hotel's website developer and one of our forensic partners, **we were able to locate and remove the malicious code from the site and address the vulnerabilities** that had allowed the hackers to gain access to the site, allowing the site to return to its normal functionality within a few weeks. Our forensic partners also conducted a forensic investigation to confirm that sensitive customer data had not been accessed or exfiltrated as a result of the hack.

However, despite the website being back in action, **the hotel faced an additional problem in relation to its website's ranking on search engines.** In effect, if a search engine such as Google or Bing thinks your website has been compromised and is a danger to visitors, it will apply either a manual or an algorithmic penalty to the affected website, resulting in the site appearing lower in the search rankings. In the case of algorithmic penalties, the affected website is usually not informed that it has been penalised. In addition, the search engine might also include a warning to potential visitors that the site may have been compromised by attackers and could result in the visitor's information being stolen or deleted.

Unfortunately there is no way of manually overturning an algorithmic penalty, such as requesting that your site be returned to its former position in the search rankings. You just have to wait until the algorithm updates. However, because **the initial drop in rankings often results in a significant reduction in visits to a site** and because search engine rankings are partly determined by the number of visits to a website, it means that a return to your original rankings can be difficult unless corrective action is taken.

In the hotel's case, it would appear that the website was hit with an algorithmic penalty as the business was never formally notified of a penalty being applied. Nonetheless, **the hotel saw its search engine rankings for certain keywords decrease significantly** following the incident, in spite of the website now being functional and malware-free once more. For example, when typing in keywords such as "hotels in city X" or "hotels in X area", the insured's website would normally feature in the top 5 rankings on any given search engine. But following the incident, the hotel often dropped out of the top 10 search results and even the top 20 in some cases.

Optimization helps boost bookings

The hotel's lower search result rankings were resulting in a reduction in the number of visits to the website and ultimately a reduction in the number of bookings too. To make matters worse, **the attack had occurred just before the summer season and any prolonged drop in search engine rankings during this period of peak bookings was likely to be highly detrimental** to the hotel's finances.

In order to assist the hotel and mitigate its potential business interruption loss, we engaged a third party company that specialises in what is known as search engine optimization. Search engine optimization essentially refers to the process of increasing the number of visitors to a website by ensuring that the site appears high on a search engine's results page. In this case, we used the third party specialist to engage in an AdWords campaign for the three peak months of the summer holiday season, whereby **the hotel's website appears under keyword searches as a sponsored website at the top of the page.** This allowed the hotel to generate more visits to the website and gradually increase its overall ranking in the search engine results to the point where sponsorship was no longer needed.

Although the hotel did see a drop off in bookings during and immediately after the attack on its website, the use of **the AdWords campaign helped to mitigate the loss and allowed the business to make up lost ground** in the following weeks and months, saving the business from any serious financial loss over the long term. However, the incident wasn't without its costs. In total, $15,587 was incurred for the cost of removing the malware, carrying out forensics and engaging the third party to carry out the AdWords campaign. Thankfully, **these expenses were all covered under the hotel's cyber insurance policy with CFC.**

Indemnity periods and attack aftermath

This claim highlights a couple of interesting points. Firstly, it shows how the impact of a cyber event can last longer than we usually think. Many people assume that if your website or other computer systems get taken down or disrupted by a cyber event or system failure, then you only need to restore the affected systems in order to halt any potential business interruption loss. But **this claim clearly illustrates that even when a website has been restored to its functionality, a return to normality is not automatically guaranteed.** In this case, the hotel was still seeing lower search rankings and reduced bookings even after the website was cleared of malware.

This is an important point from a cyber insurance perspective because of the way indemnity periods vary from policy to policy. Some cyber policies will only reimburse policyholders for the financial losses incurred during the period that systems are down (in this case that would be the time during which the website was disrupted by the malicious code). Other policies will reimburse policyholders for the financial losses incurred while systems are down plus an arbitrary number of days (typically 30 days) after computer systems are back up and running. And some policies, such as CFC's, will continue to reimburse policyholders after systems have been restored to their normal functionality, up to the point where policyholders are back to the same financial position that they would have enjoyed had the cyber event or system failure not occurred. **This is a key distinction because a business can continue to be affected financially even after its systems have been restored,** and any policy that doesn't cover this could leave the business financially exposed. Brokers should therefore be sure to check how any given cyber policy's indemnity period operates.

Finally, this claim illustrates the increasing dependence that most modern businesses have on their digital assets, whether that be their electronic data, software programmes, or websites. In this case, although the hotel wasn't completely reliant on its computer systems to operate, it did depend on its website for a substantial portion of its bookings. When that site was badly affected by malicious code, the website's search engine ranking was impaired and the hotel saw fewer bookings as a result. With more and more businesses relying on their digital assets to generate revenue, **having a cyber insurance policy in place can provide a valuable safety net** in the event that these digital assets are damaged or become inaccessible. ●