Cybersecurity: How to Protect Yourself in the Digital Battlefield

Submitted by haston on Fri, 27/09/2024 - 15:58

*HBX Group garnered expert insights from **Christo Butcher**, global lead for threat intelligence at Fox-IT, on how travel professionals can safeguard against cybersecurity attacks.*

The hospitality industry is fantastic. This is a sector which thrives on the human connection, with a workforce which is inherently helpful and kind. There are benefits to this: from an enhanced customer experience to collaboration, innovation and morale, the sector's greatest strengths can be attributed to a collective passion and empathy.

Unfortunately, these positive traits also serve as a gateway to vulnerability.

Cybercriminals love the travel industry. Consisting of numerous companies, a vast number of individuals, and significant financial assets, it is an appealing target. On top of this, its current level of cybersecurity is often lower than other sectors.

So, how can travel professionals protect themselves from cyberattacks?

The answer lies in understanding the cybercriminals, and working to strengthen against those weaknesses they exploit.

Know Your Enemy

Cybercriminals are inherently creative, functioning much like entrepreneurs seeking lucrative opportunities. When they discover effective methods for earning money, they exploit them until those methods become ineffective. They then look for another way to attack – and in an industry as far-reaching as the travel industry, the access points are plentiful.

Moreover, we exist in an evolving digital world. It can be hard for the average person to keep up – but for the hackers, cybercrime is their livelihood. They're adept at staying up-to-date, looking for any opportunity to exploit their targets' weaknesses.

Here are just a few tactics techniques which you might already be familiar with:

- **Email Phishing:** a fraudulent attempt to obtain sensitive information, steal credentials, or infect the target computer via deceptive emails that appear to be from legitimate sources.
- **Chat Phishing:** a scam where attackers use instant messaging platforms to manipulate users into sharing personal information or downloading malicious software.
- **Voice Phishing (Vishing):** a technique where scammers use phone calls to trick individuals into revealing confidential information or perform actions information by pretending to be a trusted entity.

As mentioned, the travel sector is a particularly friendly one. This makes its workforce susceptible to hacking via **social engineering**. Cybercriminals are master manipulators and have no issue with brazenly taking advantage of their proposed victims – if that travel agent, check-in clerk or phone operator is in a very helpful mood, it makes them extra vulnerable. However, there is a way to channel that helpfulness into a form of protection.

Strengthening Defense Through Collaboration

Transparency around cybersecurity offers a pathway to beating cybercriminals. Although many businesses feel ashamed to have suffered a cyberattack, others have gone public, choosing to bring attention to the crime in the interest of the greater good.

Of course, not every company wants to admit to falling victim to what are increasingly common attacks. It’s easy to understand why: few want to appear vulnerable, especially when entrusted with valuable customer data. That said, sharing experiences of cybercrime, especially technical details of the attacker’s modus operandi, within the travel sector and with trusted authorities (like Fox-IT and NCC Group) anonymously reporting cybercrimes to an authority (like Fox-IT) is a valuable step to helping others and the industry as a whole to prepare and defend themselves from suffering the same fate.

By sharing, we can build a stronger defense: it’s better to learn from the collective experience, than to sit with our own mistakes.

In addition to leaning into the spirit of transparency – that much-loved trait that our travel professionals possess in spades –, keeping abreast of developments in the realm of digital technology and cybersecurity is paramount. After all, cybersecurity is not a static field: it continually evolves alongside the techniques deployed by cybercriminals. The public media has plenty of useful information, but engaging with specialised cybersecurity firms can provide valuable insights at speed.

Here at **Fox-IT**, we're immersed in the landscape of ongoing cyberattacks. As committed cybersecurity specialists, our mission drives us to contribute to a safer society for all. From conducting cybersecurity assessments to sharing providing trainings on the issue, our technical and innovative solutions enable us to do just that.

However, the most promising strategy for the travel and tourism sector is **fostering a culture of collaboration** – this is something we experienced first-hand when joining HBX Group at this year's **MarketHub**, where we were able to speak directly to travel professionals about the challenges they face. These are individuals who have seen the issue from close by; businesses of all sizes, who have seen the damage caused. Mutual exchanges, such as those at the MarketHub (or in other forums) can significantly enhance resilience against sophisticated attacks.

Awareness of this issue is growing, and to protect ourselves, we must work together to find a solution. This Cybersecurity Awareness Month, I wish to echo the sentiment that cybersecurity is a collective obligation – it's time to **empower ourselves by leveraging our diverse experiences** and expertise as vital insights, as we work to **strengthen our defences against cybercrime.**

Christo Butcher has been safeguarding companies since the turn of the century. He excels at illuminating the challenges posed by real-world cyberattacks and developing evidence-based strategies to fortify organisations against them. In an era marked by constantly evolving cyberthreats, Christo Butcher is dedicated to providing clarity, insight, and data-driven resolutions. His passion lies in growing clients' cyber maturity and enhancing the safety of our digital landscape.

Thumb image