GALGORM
SPA & GOLF RESORT

CASE STUDY

Tackling Cyber Threats in Hospitality

MetaCompliance®

Tackling Cyber Threats in Hospitality

There has been a myriad of data breaches in the hospitality industry. Marriott, Radisson Hotel Group, InterContinental, Four Seasons and Hilton Hotels are just some of the major corporations that have hit the headlines in recent years as a result of a data security attack.

The Marriott is often cited as one of the biggest data breaches to ever take place, resulting in a fine of more than $120 million. However, these basic security failings not only cause devastating financial losses, but they also cost organisations their reputation, jobs, investment and business.

These consequences are too great to ignore and last year, PwC's Hotels Outlook report stated that the hospitality sector had the second-largest number of Cyber Security breaches after the retail sector.

The Weakest Link

Staff are often an organisation's greatest asset, but they can also be the weakest link in Cyber Security.

As such, hospitality is a lucrative industry for cybercriminals because of the value and volume of Personally Identifiable Information these organisations hold. This, coupled with a large workforce, provides ample opportunities for intruders to infiltrate the reservation system or the in-house restaurant POS to capture critical customer data.

Acknowledging this growing threat, the Galgorm Spa and Golf Resort, a premier luxury hotel based in Northern Ireland, wanted to take a proactive approach to increase awareness amongst employees and educate staff about their role in keeping the organisation safe.

Recognising and Responding to Cyber Threats

Following an expansion, the Galgorm Spa and Golf Resort had grown their staff across multiple locations. As a result, the organisation was experiencing an increase in email communication and phishing threats. Recognising that Cyber Security is everyone’s responsibility, the Galgorm Spa and Golf Resort was finding it increasingly difficult to clearly communicate cyber security hygiene and train employees on how to recognise and respond to common cyber threats.

Educate and Engage Employees

With 76% of businesses affected by phishing attacks in 2019, the Galgorm Spa and Golf Resort recognised the need to increase vigilance through automated phishing simulations.

Using MetaCompliance's award winning MetaPhish solution, the Galgorm Spa and Golf Resort can now identify those users most at risk and direct them to point of need learning experiences that provide advice on how to avoid future phishing attempts. Using tailored phishing campaigns which are based around real-life scenarios also helps to drive engagement amongst staff and supports employees to identify various forms of phishing attacks in a controlled environment.

> “Phishing was an area of most concern and **MetaPhish was the one product that met our specific needs.** It has helped us identify vulnerabilities within the organisation and given us insight which we have used to enhance our cyber awareness training.”

Elaine Kelly
Systems Policies & Project Manager

Reporting on Results

Despite running ad-hoc awareness campaigns in the past, the management at the Galgorm Spa and Golf Resort were unable to determine how effective the training was or establish a baseline for current user awareness.With MetaCompliance's detailed reporting dashboard, the Galgorm Spa and Golf Resort can now demonstrate an evidence trail of their awareness campaigns, pinpoint users who are vulnerable to attack and outline the need for additional staff training.

Management has also been able to share reports with board members and executives which has helped to create a shared responsibility model across the organisation.

Shared Sense of Responsibility

For management at the Galgorm Spa and Golf Resort, creating a shared sense of responsibility was key. Since introducing MetaPhish, the organisation has been able to develop a culture of Cyber Security, enhance personal accountability and embed security as a top priority across all areas of operations.

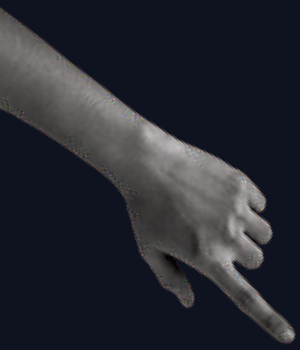
Working in partnership with the Galgorm Spa and Golf Resort, the MetaCompliance Customer Success Team has been able to advise on the latest phishing trends and help create customisable templates that are relevant to specific users.

> **“The implementation process was fantastic and could not have been better. The team at MetaCompliance was there to answer our questions, give suggestions for campaigns and provide their expert advice.”**

In just a few months, the Galgorm Spa and Golf Resort has noted an **increase in awareness,** with employees following best practice guidelines and applying caution before they click on any email links. The Galgorm Spa and Golf Resort has also been able to maintain a consistent approach to awareness, issuing regular simulated phishing tests using the automated workflow which has helped save time and resources.

> **“Working with MetaCompliance has highlighted the importance of good Cyber Security hygiene throughout the organisation. We have noticed users being more mindful of their behaviours and acting with caution because they are now aware of the risks and consequences resulting in a cyber attack.”**

With the hospitality industry increasingly prone to malicious cyber attacks, the Galgorm Spa and Golf Resort now plan to maintain awareness amongst staff through ongoing awareness campaigns which incorporate a hybrid approach of physical and digital assets such as poster campaigns, phishing simulations, quizzes, and engaging eLearning.



Mitigate Risk

With cybercriminals representing a persistent risk to organisations of all sizes, it's vital that your cyber awareness campaign provides a real defence against cyber threats and educates staff on the importance of their role in safeguarding sensitive company data.

To hear how MetaCompliance can help you to automate your cyber awareness campaigns and develop cyber resilient staff, **get in touch.**

✉ info@metacompliance.com

@ www.metacompliance.com

MetaCompliance®