

Microsoft Solutions Partner

Modern Work

Compete 366

Case Study: Gulf Keystone strengthens cyber awareness with Microsoft attack simulation training

© Compete366 2026. All rights reserved

engage@compete366.com

GULF KEYSTONE PETROLEUM

Gulf Keystone has strengthened employees' ability to recognise and report suspicious emails, improved responses in successive phishing simulations and given management clearer visibility of cyber awareness trends. By bringing the programme in-house, the business has also reduced delivery costs and gained greater control over campaign content and scheduling, while targeted follow-up training helps sustain improvements across its distributed workforce.

Business Background

Gulf Keystone Petroleum (GKP) operates the Shaikan Field in the Kurdistan Region of Iraq, which has been in production since July 2013. Its business spans a London head office and operations in Kurdistan, with employees working across locations and travelling between them.

For this distributed workforce, cyber awareness needs to reach beyond a single office or a one-off training session. GKP was looking for a practical way to educate employees, test how they responded to suspicious emails and identify where further support was needed.

Key Challenges

Turning awareness into everyday behaviour. GKP needed employees to recognise social engineering attempts, question unexpected requests and report suspicious messages rather than simply complete training. Early simulations revealed gaps in awareness and provided a starting point for targeted education.

Keeping training relevant. Employees encountered different risks depending on their roles, location and the systems they used. Finance and supply chain teams regularly dealt with external organisations, while travel and remote working added complexity. A generic message would not always reflect the situations employees faced.

Reaching a multilingual workforce. Some employees needed support in Kurdish or Arabic. Language and cultural differences meant that training content needed adaptation, not just distribution.

Making the programme sustainable. The business had trialled using an external consultancy to deliver a cyber awareness programme.

As Firya Abubaker, IT Supervisor with responsibility for IT Infrastructure and Cybersecurity at GKP explains "As a business we realised that we needed to run campaigns regularly, provide follow-up training and show management how results changed over time, without relying on an external consultancy for each exercise. New joiners also needed to be included in an ongoing cycle of awareness and testing."

© Compete366 2026. All rights reserved

The Solution

After doing some research and with guidance from Compete366, Firya realised that the Microsoft Defender suite could be a good solution. So GKP brought the programme in-house using attack simulation training in Microsoft Defender for Office 365. The approach combines employee education with simulated phishing campaigns, targeted follow-up and management reporting.

A repeatable quarterly cycle

The company runs phishing simulations quarterly, varying the scenarios to keep the exercises relevant. Awareness presentations at company Town Hall meetings help explain the risks. The simulations then test how employees apply that learning with a typical campaign following an awareness session by around two to three weeks which would run for a few days.

Employees who need further support are assigned training available within the simulation platform. Where travel or work rotations make online completion difficult, Gulf Keystone supplements this with face-to-face cyber awareness sessions.

Scenarios tailored to the business

Rather than relying solely on generic messages, Gulf Keystone adapts templates to reflect familiar systems and timely themes. Typical examples included HR-related communications and access to the HR system, seasonal shopping offers such as those that happen around Black Friday and QR-code phishing.

These exercises help employees practise recognising suspicious messages in contexts they might encounter at work.

The team also customised follow-up communications after some employees initially mistook genuine training reminders and landing pages for further phishing attempts. This highlighted the importance of explaining both how to recognise suspicious emails and what to expect from the training programme.

Reporting and ongoing adaptation

Campaign results are compared with previous exercises and shared with management to show trends and identify priorities for further training. The same approach supports awareness activity beyond phishing, including training on AI risks and practices.

Local delivery remains important: GKP translates or adapts material into Kurdish and Arabic where needed and adjusts examples to reflect employees' cultural and working context.

© Compete366 2026. All rights reserved

Benefits

Greater awareness and more confident reporting
Gulf Keystone reports that employees are better able to recognise suspicious emails and share them with the security team. As Firya explains “Now our finance and supply chain employees question unexpected payment requests and are asking for checks before taking action. Employees have also identified suspicious activity involving external suppliers which can be a vulnerability that is easy to overlook.”

Improved responses over time
GKP has seen stronger results in successive simulations and fewer instances of employees being caught out by real phishing attempts.

Clearer visibility for management
Comparing campaign results gives leaders a way to understand awareness trends and where further education is needed. Simulations also make security risks tangible, helping support wider discussions about additional measures such as multifactor authentication and access controls.

More control over delivery and cost
Running the programme internally allows GKP to choose campaign themes, adapt content and schedule exercises around business needs. This is much less expensive than commissioning an external consultancy to deliver the education and testing.

An ongoing learning cycle
Quarterly campaigns create recurring opportunities to reach new joiners, reinforce learning and respond to changing threats. Targeted online training, face-to-face support and locally adapted content help make the programme relevant across the workforce.

Prevention rather than costly recovery
Responding to a real cyber breach can be expensive and time-consuming, with investigation and recovery diverting people and resources from day-to-day business. Regular simulations give employees opportunities to learn from mistakes in a controlled setting rather than during a live incident. Although awareness training cannot eliminate every risk, helping employees recognise and report suspicious messages supports a proactive approach to reducing the likelihood of disruption and costly recovery.

For GKP, the value lies not simply in running simulated attacks, but in connecting education, practical testing and follow-up. The result is a repeatable awareness programme that is changing how employees respond to suspicious communications and strengthening support for cybersecurity across the business.

© Compete366 2026. All rights reserved

Find out more about Microsoft Attack Simulator…

Cyber awareness for businesses of every size

Attack Simulation Training is not only for large enterprises. Small and mid-sized organisations can use the same practical approach to run realistic phishing exercises when required, assign targeted training and report on results, without building a complex standalone programme.

The service requires Microsoft Defender for Office 365 Plan 2, which can be purchased as an add-on to eligible Microsoft 365 subscriptions or is included with Microsoft 365 E5. This gives organisations a scalable way to start with focused campaigns and expand their programme as their workforce and security needs evolve.

Ready to strengthen your organisation's cyber awareness?

Contact Compete366 to discuss your Microsoft 365 environment, the security solutions available and how Attack Simulation Training could work for your business.

Warren Duke on 020 3282 7186
or email engage@compete366.com

© Compete366 2026. All rights reserved