COGNISYS
Smarter Cyber Security

WEB APPLICATION SECURITY TESTING
SECURITY AUDITING INTERNAL PENETRATION TESTING
CYBER ATTACK/PHISHING SIMULATION PCI-DSS
AZURE/AWS CLOUD SECURITY REVIEW RED TEAMING
VULNERABILITY MANAGEMENT AS A SERVICE (VMAAS)

Cyber Attack and Phishing Simulation

How susceptible are your users to a targeted phishing attack? Try a simulated attack to find out.

Cognisys can perform simulated phishing attacks, to determine the susceptibility of your organisation to this type of cyber assault.

Working with you to devise a range of phishing scenarios, we will build a series of personalised, targetted and relevant emails. Typically the emails invite recipients to take certain actions that will result in them giving away sensitive information, such as usernames and passwords.

All responses, actions and information are intercepted and assessed, whilst redirecting users to landing pages or delivering convincing error messages to prevent suspicion.

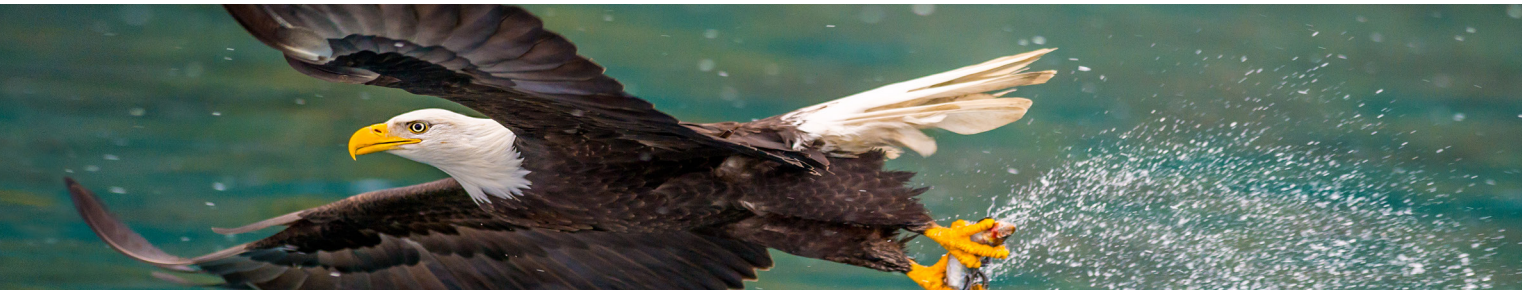
Any opportunities for potential exposure are presented in a format that allows an organisation to determine the security awareness of its employees.

Be smart. Be safe. Be secure.
Call us today on:
01422 416000
sales@cognisys.co.uk www.cognisys.co.uk

Continued overleaf....

COGNISYS
Smarter Cyber Security

WEB APPLICATION SECURITY TESTING
SECURITY AUDITING INTERNAL PENETRATION TESTING
CYBER ATTACK/PHISHING SIMULATION PCI-DSS
AZURE/AWS CLOUD SECURITY REVIEW RED TEAMING
VULNERABILITY MANAGEMENT AS A SERVICE (VMAAS)



BENEFITS

- Quickly discover the extent of any internal awareness problem.
- Discover which employees would benefit most from any cybersecurity awareness training.
- Works in conjunction with your team to raise awareness and increase cyber security maturity
- Efficient, integrated and affordable service

WHALING

Whaling is a cyber attack using a more targeted version of spear-phishing concentrating more on a particular individual (usually a high-ranking C-suite executive such as a CFO or CEO) rather than a single organisation. The idea is that the bigger the target, the harder the fall and the greater the potential payoff.

The goal of a simulated whaling attack is to trick an individual into disclosing information by using social engineering, email spoofing and content spoofing efforts.

For example, we may send the victim an email that appears to be from a trusted source, including links back to a customised website that has been created especially for the attack.

Our emails and websites can be highly customised and personalised, incorporating the target's name, job title or other relevant information gleaned from a variety of sources.

Preventing these types of cybersecurity threat requires all employees to take responsibility for protecting the company's assets.

In the case of whaling and phishing, all employees, and not just high-level executives should be trained about these attacks and how to identify them.

IDENTIFY

- Categorisation of templates into easy, medium and difficult to spot to escalate training.
- Identification of overall Cyber security awareness
- Training can be built-in to landing pages

REMEDIATE

- Understand how to better defend your organisation using a layered defence approach.
- Provide cyber security awareness training for your employees if required
- Build an effective cyber-threat reporting culture, with a "no-blame" approach for maximum uptake, throughout your organisation.

Find out more about us and our other Cyber Security services here – **www.cognisys.co.uk**

Be smart. Be safe. Be secure.
Call us today on:

01422 416000

sales@cognisys.co.uk www.cognisys.co.uk