

10

WAYS
SPEAR
PHISHING &
DEEP FAKE
THREATS
CAN BE
TACKLED





Q U O D
O R B I S

1.

EMPLOYEE ENGAGEMENT & TRAINING

It's important to educate employees about spear phishing and deep fake attacks, including how to recognise these threats and report any suspicious behavior.

Additionally, implementing simulated phishing campaigns can help assess and improve team awareness, ensuring they are better prepared to handle real threats.



2.

MULTI- FACTOR AUTHENTICATION (MFA)

To enhance security, ensure multi-factor authentication (MFA) is implemented for accessing all company systems. Regularly update MFA protocols to maintain their strength and effectiveness in protecting against potential threats.





Q U O D
O R B I S

3.

COMMUNICATION CHANNELS THAT ARE SECURE

Ensure that communication channels used for sensitive conversations and data exchanges are encrypted to safeguard information.

Additionally, it is crucial to establish protocols for verifying the identity of anyone with whom you plan to share sensitive information.





Q U O D
O R B I S

4.

EMAIL SECURITY

Implement advanced spam filters to block malicious emails and enhance security by using email authentication protocols like DKIM, DMARC, and SPF to verify the legitimacy of incoming messages.

Plus, scan all attachments and links for any suspicious content to further protect against threats.





5.

MONITOR & DETECT

Implement continuous monitoring across your entire ecosystem, utilising advanced threat detection tools to observe network traffic and identify spear phishing and deep fake activity.

Regularly analyse user behaviour to detect unusual patterns that may signal a compromised account or system.





Q U O D
O R B I S

6.

PROTECT YOUR DATA

Encrypt your data to safeguard it from unauthorised access, and enforce strict access controls to ensure that only authorised personnel can access sensitive information.



www.quodorbis.com



Q U O D
O R B I S



7.

PLAN FOR AN INCIDENT

Start by establishing a comprehensive incident response plan that specifically addresses spear phishing and deep fake attacks. Regularly test this plan to ensure that teams are fully familiar with the protocols and can respond quickly in the event of an attack.



8.

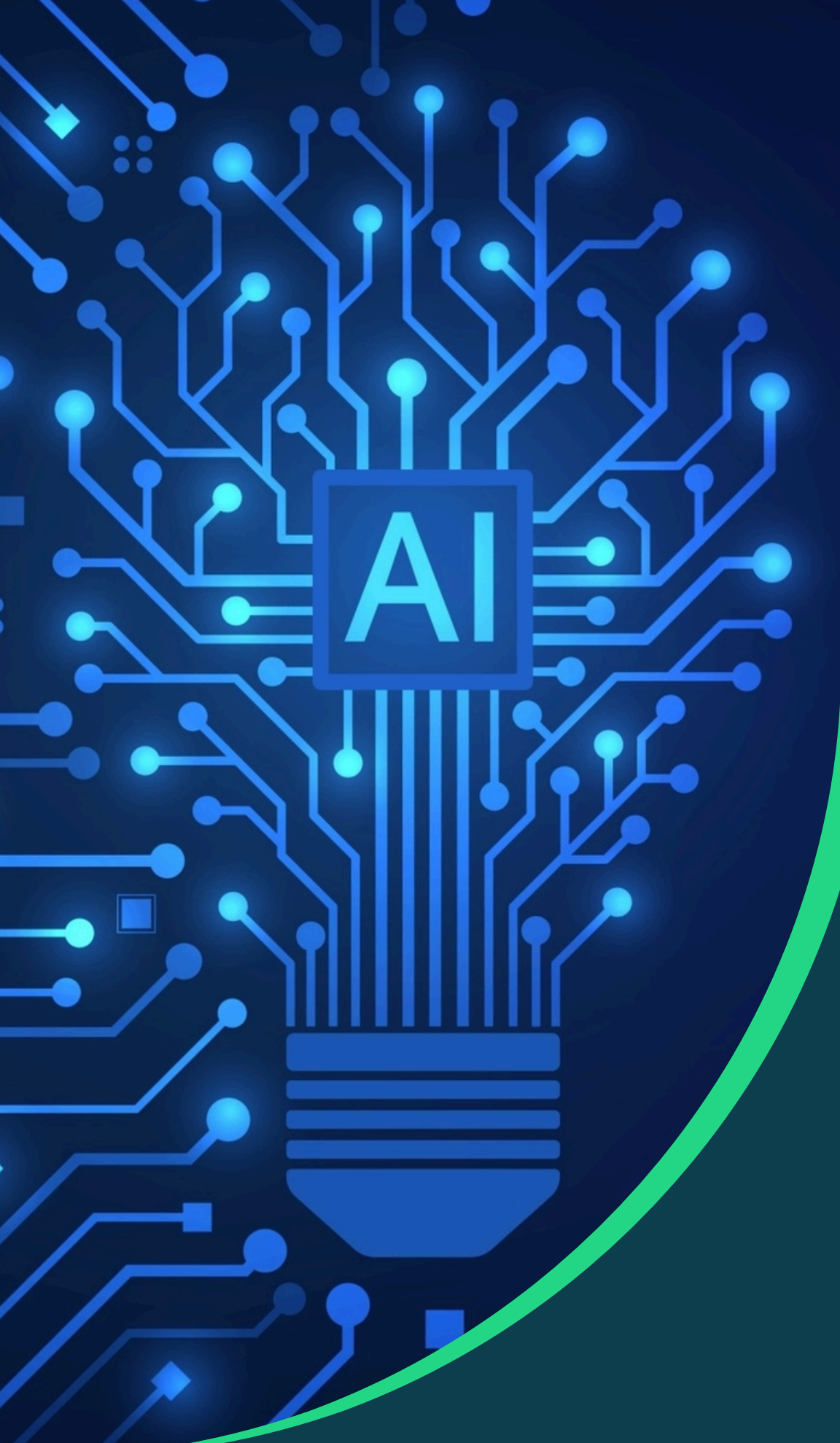
THIRD-PARTY RISK

Evaluate the security practices of your vendors to ensure they do not become a weak point in your overall security. Include specific security requirements and breach notification clauses in their contracts to further protect your organisation.





Q U O D
O R B I S



AI

9.

HOW AI & MACHINE LEARNING CAN HELP

Leverage AI and machine learning tools to detect and mitigate spear phishing and deepfake attacks by analysing patterns and identifying anomalies.

Also, deploy specialised deepfake detection tools to identify manipulated content in images, audio, and video.





10.

COMPLETE SECURITY UPDATES AND AUDITS REGULARLY

Stay updated by ensuring all systems, security solutions, and software are fully patched to provide the highest level of protection against vulnerabilities.

Regularly conduct security audits to identify potential weaknesses and enhance your security measures.



Speak to the team to learn how our Continuous Controls Monitoring platform provides total visibility into your business ecosystems.



Speak to the team >