QUOD ORBIS

The Red Flags of Deepfake Spear Phishing: Verification Protocols to Outsmart Cyber Criminals

WWW.QUODORBIS.COM

@QUOD-ORBIS

QUOD ORBIS

The Red Flags of a Deepfake Spear Phishing Attack on Your Company

01 Unusual or urgent requests

You may think you trust the source, but if this includes urgent, unusual requests, like financial transfers or confidential information, then validating the source is crucial.

02 Inconsistent communication patterns

The message might display subtle shifts in tone or language, such as a formal individual suddenly becoming casual, or the reverse.

03 Visual or audio evidence

Videos or audios shared to add credibility should be analysed. Look for unnatural facial movements, mismatched lip-syncing, odd blinking, or robotic voices lacking natural intonation.

04 Email spoofing indicators

You may be asked to avoid using the usual email and switch to a personal one.

05 Unfamiliar file attachments or links

The message may contain unfamiliar files or links that seem legitimate but lead to malicious sites or malware.

QUOD ORBIS

The Red Flags of a Deepfake Spear Phishing Attack on Your Company

06 Unusual timing

The message may be sent at an unusual time, like late at night or during holidays, raising suspicion about its authenticity.

07 Attempts to avoid verification

Excuses for avoiding normal verification protocols, such as not responding when asked to share screens, delaying video calls, or avoiding face-to-face meetings.

08 Requests for untraceable payments

Requests for payments via unconventional or untraceable methods, like cryptocurrency, can be a red flag.

09 Mismatch in content and context

The content may not align with past conversations or projects, indicating it may not be from a genuine source.

10 Requesting confidential information

Requests for confidential information without following proper procedures may indicate a deepfake attack.

QUOD ORBIS

Key Verification Protocols to Implement in your Business

IMPLEMENT A VERIFICATION PROCESS FOR SENSITIVE REQUESTS

Why: Deepfake attacks impersonate trusted individuals for financial transfers or sensitive information.

How: Require secondary verification, like a video call with specific actions or a phone call.

STRENGTHEN EMAIL SECURITY PROTOCOLS

Why: Spear phishing often begins with malicious emails, making email security essential.

How: Use protocols like DMARC, DKIM, and SPF to authenticate emails and reduce phishing risks.

ADOPT A ZERO-TRUST SECURITY MODEL

Why: Zero-trust security requires verification of every user, device, and system to minimise the attack surface.

How: Enforce strong identity verification, segment the network, and restrict access based on roles.

USE AI-POWERED PHISHING DETECTION TOOLS

Why: AI can identify anomalies in communication that traditional systems might miss.

How: Use AI tools to scan emails, voice, and video for unusual patterns and deepfake characteristics.

ENFORCE STRICT COMMUNICATION POLICIES

Why: Deepfake phishing often targets casual communication channels.

How: Limit unofficial platforms for business use and ensure encrypted communication for sensitive discussions.

REGULAR TRAINING FOR EMPLOYEES ON PHISHING

Why: Human error is a key vulnerability, but trained employees can be the first line of defense.

How: Provide regular training on phishing identification and conduct simulations to test awareness.

SET UP INCIDENT RESPONSE PROTOCOLS

Why: A swift response to suspected attacks can limit damage.

How: Develop a formal incident response plan for deepfake spear phishing and train employees to report suspicious activities.

A Story of Thwarting an AI Deepfake Spear Phishing Attack

THE DIARY OF A CEO

Our CEO, Martin Greenfield, thwarted a deepfake spear phishing attack, highlighting the growing threat of AI in cybercrime. Scammers impersonated the chairman of a recently acquired company via WhatsApp, requesting help and directing him to a fake lawyer for an NDA. Recognising red flags, Martin identified the scam and emphasised the importance of vigilance and security for CEOs.

To hear more about Martin's story, you can watch the recent feature on BBC Click with BBC Journalist, Joe Tidy.

If you would like to take a look then you can access this here.

> Now is the time for vigilance. We all need to acknowledge that AI is being leveraged by cyber criminals to target organisations, with CEOs usually the intended victim.