New Social Engineering Scam Targeting Our Clients

We recently detected a rise in a sophisticated social engineering scam, most prevalent on Facebook. This scam involves deceptive tactics to manipulate individuals into divulging sensitive information or performing actions that could compromise your security.

Essentially the scam involves you receiving a message either via email, as a comment or in a direct message from the scammer disguised as a legitimate communication from Facebook/Meta. It advises you that an "image" you posted/your "recent campaign" has been flagged by the Facebook monitoring system and that your page/advert is at risk of being permanently suspended. The post would then provide a link for you to click on should you wish to verify/dispute this.


? Important Notification - [redacted] Your Facebook page is expected to be permanently removed due to the post violating our trademark rights. We made this decision after careful consideration and in compliance with our intellectual property protection policies. If you believe this is a misunderstanding, we ask that you contact us to restore your page before it is removed from Facebook. Thanks for the co-operation . If you have any questions or concerns, please contact us Here: https://linkbio.co/pilou-0943 Best regards, Support group

How to spot a scam

Social engineering scams often contain:

- **Urgent requests** for personal information, account credentials, or financial details.
- **Psychological manipulation techniques** such as fear, curiosity, or urgency. They may create a sense of urgency or fear of consequences to trick you into taking immediate action without questioning the authenticity of the request.
- **Malicious Links and Attachments** designed to install malware or ransomware. Clicking on these links or downloading attachments can result in unauthorized access to sensitive company/customer data and even financial losses.

New Social Engineering Scam Targeting Our Clients

Why is this a risk to your business?

Data Breach: Disclosing any sensitive information in response to these scams (for example providing account login details) can lead to identity theft, financial fraud and unauthorised access to confidential data.

Financial losses: If you click on any links and submit any login credentials, scammers may use it to access bank accounts, make unauthorised transactions and much more...

Reputation Damage: Falling victim to these social engineering scams or even just leaving the content available on your social media pages can damage your reputation as a trustworthy brand, leading to loss of credibility and customer trust.

Top Tip

Always exercise caution before clicking on links, hover over links to see full URL, scrutinise contact details and any information provided for signs of inconsistencies or irregularities. Never trust messages demanding immediate response or threatening to delete or ban your account.

RiskEye is on alert for this risk and if we find it, we will alert you to it. If you have concerns or require any assistance please reach out to our team on info@riskeye.com

RISKEYE® online reputation security