NEWSLETTER

INFORMATION SECURITY

2025 – Protecting Our Company from CEO Phishing Attacks

As part of our commitment to maintaining a secure work environment, we want to provide you with important tips to help protect yourself and our organization from Social Engineering and especially the CEO phishing way of attacks in emails and other messaging platforms.

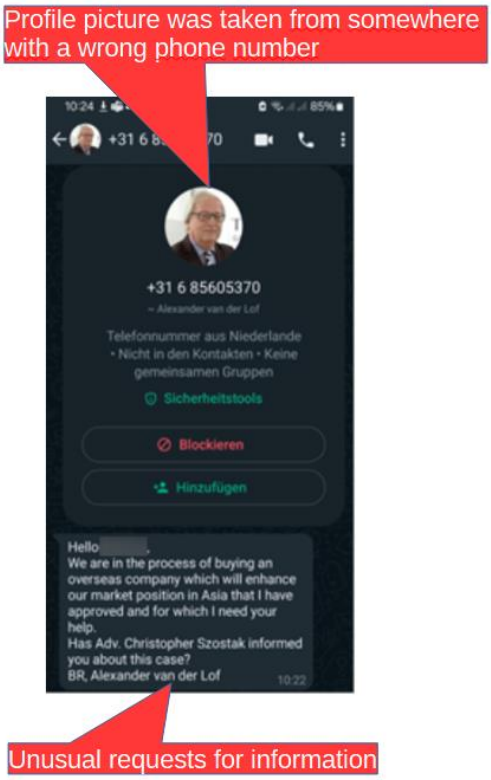
What is CEO Phishing? CEO phishing involves cybercriminals impersonating company executives to deceive employees into disclosing sensitive information or performing fraudulent transactions. These attacks pose a serious risk to our organization, potentially resulting in financial losses, reputational damage, and compromised data security.

Your Role in Defense Phishing attacks are becoming increasingly sophisticated (see example below).

Please note that several employees within the TKH Group received a WhatsApp/sms message from "Alexander van der Lof".

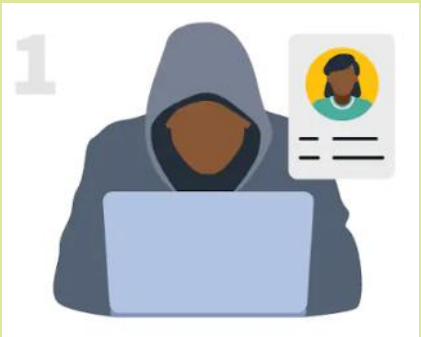
This is an actual fake and a CEO fraud attempt.

Note that our CEO from TKH Group (Alexander van der Lof) will never approach you in this way.



TKH AIRPORT SOLUTIONS

Common way of Social Engineering preparation and attack



The social engineer gathers information about their victims.

The social engineer poses as a legitimate person and builds trust with their victims.

It's crucial that we remain vigilant to safeguard against them. Here are some essential security tips to keep in mind:

Verify Requests: Always verify the legitimacy of requests for sensitive information or financial transactions, especially if they come from executives. Take the time to confirm such requests through a separate communication channel, such as a phone call or an in-person conversation.

Watch for Urgency: Be cautious of emails or messages that pressure you to act quickly or urgently. Cybercriminals often use urgency to manipulate individuals into making hasty decisions.

Check Sender's information: Carefully review the sender's email address or contact details for any unusual or suspicious elements. Phishing emails may use fake or slightly altered information to appear legitimate.

Scrutinize Email Content: Pay close attention to the content of emails or messages for any signs of phishing, such as spelling errors, grammatical mistakes, or unusual requests for information.

Be Wary of Attachments and Links: Exercise caution when interacting with email attachments or links, especially if they're from unfamiliar senders. Hover over links to check the URL before clicking, and avoid downloading attachments from unknown sources.

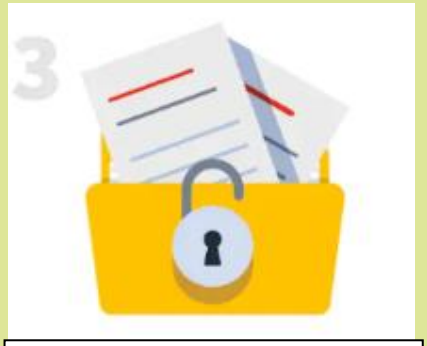
Protect Your Login Information: Never share your passwords or login credentials in response to emails, messages, or other communications, even if they appear to be from trusted sources. Phishing attackers often use deceptive tactics to trick individuals into disclosing their login information.

Report Suspicious Activity: Report any suspicious emails, messages, or activity to our IT security team immediately. Your prompt reporting can help prevent potential security breaches and protect our company's data.

Stay Updated: Stay informed about updates to our company's security policies and procedures. Regularly review security guidelines and communicate with your colleagues about best practices for staying safe online.

By following these tips and remaining vigilant, we can work together to safeguard our company from phishing attacks and other cyber threats.

Thank you for your commitment to our company's security.



The social engineer gathers information about their victims.

The social engineer poses as a legitimate person and builds trust with their victims.

Still have questions?

Please contact IT Support Servicedesk or mailto:a.boeijink@tkh-airportsolutions.com