Whaling Awareness Email Template

Whaling can be much easier to fall for than your typical phishing attack, and has the potential to be much more destructive. The e-mail below will provide your employees with the necessary knowledge to identify and avoid whaling attacks:

Dear team,

To further enhance our company's cyber defences, we want to highlight a common cyber-attack that everyone should be aware of – whaling.

Whaling is a type of scam aimed at getting an employee to transfer money or send sensitive information to a hacker acting as a trusted source via email. Whaling is extremely easy to fall for and can result in significant financial losses.

These e-mails can be difficult to catch because they appear to be harmless, and have a normal, friendly tone and no links or attachments. They will appear to come from a high-level official at the company, typically the CEO or CFO, and often ask you to disclose sensitive information or initiate a wire transfer.

A few things to watch out for in a typical whaling attempt:

- ***Doppelganger**: Whalers may utilize fake e-mail domains that look similar to our domain. Watch out for things like: [EMAIL]@[VARIATION ON COMPANY DOMAIN]*
- ***A hurried tone**: Whalers will often ask you to send money immediately, stating that they're busy or in a meeting, and can't do it themselves.*
- ***E-mail only**: Since whaling relies on impersonating an employee via a fake, yet similar email address, they will ask you not to call with questions and only reply through e-mail.*

If you receive an e-mail that you suspect to be a whaling attempt, or if you are unsure of an e-mail's legitimacy, please do not respond. Instead, [INSERT COMPANY PROTOCOL].

Remember, nobody from [COMPANY NAME] will ever request personal information, usernames, passwords, or money from you via email.

Thanks again for helping to keep our network, and our people, safe from these threats.

Please let us know if you have any questions.

Regards,

[NAME]