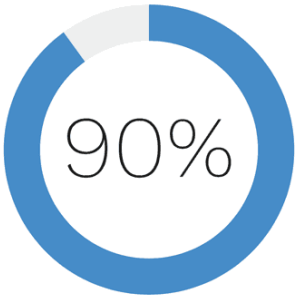
Cyber Security Awareness Training

Social Engineering Spear Phishing

Spear phishing attacks are well crafted and hard to identify. Whaling is a subset of spear phishing, just with a focus on the highest executive levels of an organization.



Spear phishing is normally done by a group of hackers. The hackers spend up to 90% of their time investigating the target!

So, be discreet, as giving out too much information to the public about your specific roles and access level in your organization can make you an easy target.

Spear Phishing Red Flags

Because spear phishing uses emails and links, the same red flags that you learned about in the phishing section will appear. Just be aware that they will be much better crafted and therefore harder to spot.

Email

Unknown sender
Suspicious attachments
Case of urgency
Requests to verify your password or account
Misspelled words

Website URLs

Forged URL
No https://
Different design
Poor grammar
Scare tactics

Additional tips on how to protect yourself

Use your wisdom to identify illegitimate emails and vishing attempts.

- If a top-level manager is asking you to send sensitive information, no matter if it's health data, security numbers or something similar, verify the request via a call or chat message.

- Be suspicious, when websites are crafted with your specific information, e.g., pre-populating your username. Don't use links in an email notification to change a password; type the URL manually or from your browser history. Now you can investigate if the password really needs to be changed.

Continue to deepen your knowledge

Make sure to work the "Secure Browsing" chapter of this training to identify certified websites and distinguish them from spoofed websites.