Cyber Security Awareness Training

Social Engineering First Aid

Social Engineering is a method which works way too often. It is not a technical vulnerability which could be patched! A successful Social Engineering attack totally depends on the attacker and the victim (the human element).

What do you do if you think you are a victim?

Internal Report

If you believe you might have revealed sensitive information about your organization, report it to the appropriate people within the organization, including your security and IT departments. They can be on alert for any suspicious or unusual activity.

Watch Accounts

If you believe your financial accounts may be compromised, contact your financial institution immediately and close any accounts that may have been compromised. Watch for any unexplainable charges to your account.

Change Passwords

Immediately change any passwords you might have revealed. If you used the same password for multiple resources, make sure to change it for each account and do not use that password in the future. Where possible, choose a second layer of authentication, for example, combining a password and SMS verification (→Two-factor authentication).

Watch out

for other signs of identity theft.

Report to the police

Consider reporting the attack to the police and file a report with the Federal Trade Commission (US) or the appropriate agency in your country.

Source: www.ftc.gov

Powered by Sonic Performance Support
Hamburg, Germany