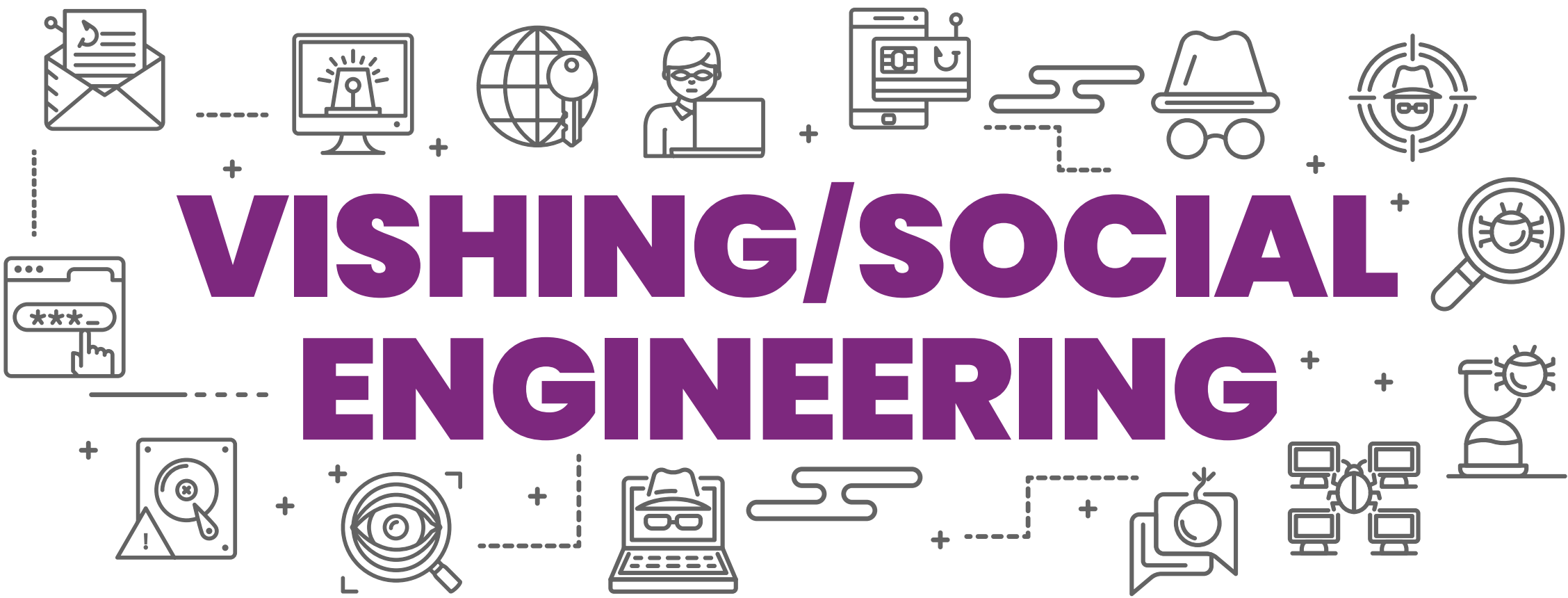


FRAUD AWARENESS

Steps businesses and individuals can take to protect themselves from cyber frauds.



Cybercriminals use various tech tactics to trick users into revealing sensitive info, like vishing, pretexting, smishing, and impersonating support staff.

MODUS OPERANDI



Fraudsters investigate the background of their intended targets and launch campaigned attacks.



Mostly happens on call asking you to click on links, donate money, update account details, etc.



They psychologically manipulate the victim taking advantage of their natural reactions.



If followed, the user themselves reveal confidential information and gives access to financial data or sensitive information.

HOW TO STAY SAFE

The golden rule is to avoid inbound customer service/technical service calls or email support requests.



In case any tech support is needed, initiate it from your end after checking contact details from official websites only.



Never entertain calls from people posing as bank representatives. Banks never call and ask for CVV/PIN/OTP.



In case a remote co-worker calls and asks for account credentials or official information, keep the IT Security team in loop and do as instructed.



Stay away from offers too good to be true.

