SVINDELERNES REDSKABER

Phishing
En svindelteknik hvor bedragere udgiver sig for at være rigtige virksomheder eller personer der via e-mail har til hensigt at lokke personlige oplysninger ud af folk. De sender typisk links til falske hjemmesider, der ligner de ægte.

Smishing (SMS-Phishing)
Samme koncept som phishing, men via SMS-beskeder i stedet for e-mail.

Scamming
Et overordnet begreb for alle former for bedrageri, hvor målet er at snyde folk for penge eller personlige oplysninger. Kan foregå ved opkald med et tilbud om ”hjælp til computeren” eller en opdatering af programmer

Vishing (Voice-Phishing)
Telefonsvindel hvor bedragere ringer og udgiver sig for at være fra banker, myndigheder eller andre troværdige organisationer.

Pig Butchering (Sha Zhu Pan)
En langvarig svindelmetode hvor bedrageren opbygger et forhold til offeret (ofte romantisk) for gradvist at lokke dem til at investere i falske krypto- eller investeringsprojekter.

Cryptoscamming
Svindel relateret til kryptovaluta, ofte gennem falske investeringsmuligheder eller falske krypto platforme.

Spoofing
At forfalske afsenderidentitet i kommunikation. Ofte benyttes spoofing til at udgive sig for en anden myndighed eller person. Spoofing bevirker at mobilnummeret der ringes fra spoofes til at ligne et nummer fra banken, politiet eller endda en ven i ens kontaktliste.

Identitetshacking
(Identitetstyveri)
En form for cyberkriminalitet hvor en person stjæler og misbruger en anden persons identitet for at opnå fordele eller begå svindel.

QRishing
er en kombination af QR-koder og phishing, hvor svindlere bruger manipulerede eller falske QR-koder til at narre folk til at besøge skadelige hjemmesider eller downloade malware.

Social Hacking
(Social Engineering)
En mere omfattende form for manipulation hvor hackere udnytter menneskelig psykologi og sociale relationer til at få adgang til systemer eller information.
Dette foregår ofte ved at hackerne gennemgår ofrets profiler på alle sociale medier og benytte medierne til at skabe forbindelse eller for at udgive sig for at være en bekendt af en anden ven.

MITM (Man-in-the-middle)
Et WiFi-baseret Man-in-the-Middle angreb sker når en angriber placerer sig mellem din enhed og det WiFi-netværk, du tror du forbinder til. Det er som en digital mellemmand, der kan se al den trafik, der går mellem din enhed og internettet. Angriberen kan gøre dette ved at oprette et falsk WiFi-netværk, der ligner et legitimt netværk (f.eks. en café eller hotel's WiFi). Når du forbinder til dette falske netværk, går al din internettrafik - passwords, beskeder, emails, kreditkortinformation - gennem angriberens system, før det sendes videre til det rigtige internet

EVIL TWIN (Den onde tvilling)
En Evil Twin er en ondsindet kopi af et legitimt WiFi-netværk, som er opsat til at ligne det ægte netværk fuldstændigt. Angriberen opretter et access point med præcis samme navn (SSID) som det legitime netværk, f.eks. "CafeWiFi" eller "HotelNet". Din enhed kan ikke skelne mellem det ægte og det falske netværk, og hvis det falske signal er stærkere, vil din enhed ofte automatisk vælge at forbinde til det.

Juice Jacking
er et angreb der udnytter offentlige USB-opladningsstationer eller -kabler. Når du sætter din telefon eller enhed til opladning i en manipuleret USB-port (f.eks. på en lufthavn, café eller andet offentligt sted)

Spear Phishing (Målrettet Phishing)
En avanceret og målrettet form for phishing, hvor svindleren bruger personlige oplysninger fra datalæk eller sociale medier til at gøre henvendelsen mere troværdig.

"Stop op, tænk dig om, og tjek en ekstra gang - for hvis noget virker for godt til at være sandt eller giver dig tidspres, er det sandsynligvis svindel."