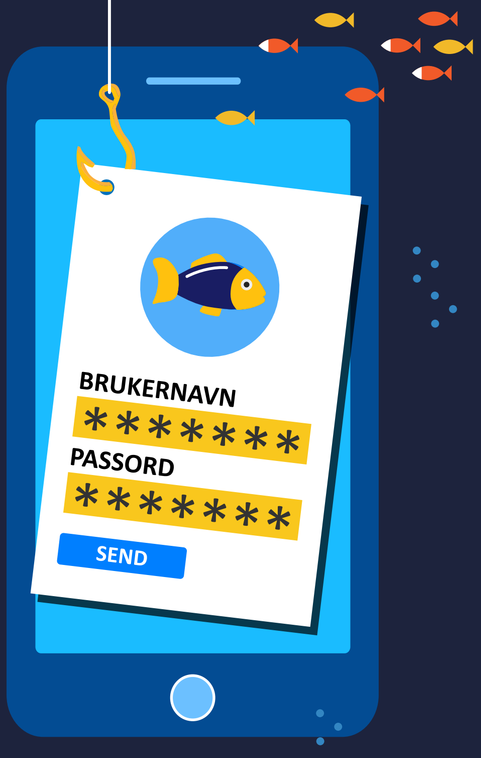
NETTBASERTE TRUSLER

SE TO GANGER FØR DU KLIKKER

Du kan miste pengene dine, personopplysninger og til og med lagrede data, hvis enheten ikke fungerer lenger. Ikke bli lurt!



HVORDAN KAN DET SKJE?

PHISHINGANGREP: De lurer brukere til å oppgi personlig informasjon ved å gi seg ut for å være en pålitelig entitet. Det spres gjennom e-post, tekstmelding eller sosiale mediaplattformer.

SURFING PÅ NETTSIDER: Mobilenheten din kan bli infisert ved å besøke en usikker nettside.

NEDLASTING AV FILER: Ondsinnede lenker og vedlegg kan være direkte inkludert i en e-post.

HVORFOR ER DET EFFEKTIVT?

Mobilenheter er KONSTANT KOBLET TIL Internett.

Den REDUSERTE STØRRELSEN PÅ ENHETENS SKJERM er en generell begrensning. Mobilnettlesere viser URL-er på begrenset skjermplass, noe som gjør det vanskelig å se om domenet er legitimt.

IMPLISITT BRUKERTILLIT er mobilenhetens personlige natur.

HVA KAN DU GJØRE?

Vær skeptisk hvis du mottar en SMS eller en telefonsamtale fra et selskap som ber om personlig informasjon. Du kan bekrefte at meldingen/samtalen er legitim ved å ringe selskapet direkte på deres offisielle nummer.

https://

Når du surfer på nettet på mobilenheten, sørg for at tilkoblingen er sikret gjennom HTTPS. Du kan alltid sjekke det ut i begynnelsen av URL-en.

Klikk aldri på en lenke/et vedlegg i en uventet e-post eller SMS. Slett den umiddelbart.

^BE:%}
W@RY
*)Z#$=

Vær skeptisk hvis du lander på en side som inneholder dårlig grammatikk, feilstaving eller lav skjermoppløsning.

Hvis tilgjengelig, installer en mobilsikkerhetsapp som vil varsle deg om eventuell mistenkelig aktivitet.

EUROPOL EC3 European Cybercrime Centre
POLITIET
CCIS
NTNU Norwegian University of Science and Technology
NorSIS Norsk senter for informasjonssikring

#MobileMalware