



ONLINE FINANSIEL SVINDEL I EN KUNSTIG INTELLIGENS VERDEN

VÆR OPMÆRKSOM OG BESKYT DIG SELV

Online finansiel svindel er ikke nyt, men kunstig intelligens (AI) har gjort det smartere og sværere at få øje på. Kriminelle anvender nu falske meddelelser og websteder, falske berømt profiler og endda AI-genererede stemmer eller videoer, der efterligner din bankrådgiver, dine venner eller din familie til at narre dig.

De rækker ofte ud til dig via sociale medier, beskedsapps, e-mails og uventede opkald der lyder ægte.

Du kan risikere økonomisk tab, identitetstyveri og følelsesmæssig nød. Vær forsigtig og følg disse vigtige tips til at forblive sikker:



Vær opmærksom på eksisterende økonomisk onlinesvindel, der drives af AI,

f.eks. efterligning af personer, phishing, investerings- og forsikringssvindel og endda kærligheds svindel. For at lære mere om forskellige typer svindel se [side 5](#), 6 og 7.

Og her for svindel, der er specifik for krypto se det dedikerede faktaark for krypto svindel ([link](#)).



Genkend advarselstegn:

Lær at genkende mistænkelig adfærd, meddelelser eller tilbud (se [side 2](#))



Beskyt dig selv:

Sikre dine personoplysninger (se [side 3](#)); og



Vid hvad du skal gøre,

hvis du bliver offer for svindel (se [side 4](#)).



Advarselstegn



Et løfte, der virker for godt til at være sandt.



Et uventet opkald fra et ukendt nummer.



En presserende anmodning om penge eller personlige oplysninger, herunder fra en person, der foregiver sig for at være et familiemedlem, en ven eller endda en offentlig figur.



En anmodning om at tage kontrol over din enhed, downloade en app, scanne en QR-kode eller klikke på et link.



En anmodning om personlige oplysninger eller bankoplysninger (f.eks. adgangskoder, kreditkortnumre, legitimationsoplysninger til netbank eller sikkerhedskoder).



En anmodning om betaling via usporbare metoder (f.eks. krypto, gavekort, bankoverførsler eller forudbetalte debetkort).



En mistænkelig eller forkert e-mailadresse eller link (f.eks. stavfejl i webadressen eller usædvanlige webadresser).



En vedhæftet fil fra en ukendt kilde, særligt .exe, .scr, .zip eller makroaktiveret Office-fil (.docm, .xlsm).



Dårlig grammatik eller formatering i et dokument, der ser officielt ud. AI kan dog give svindlere mulighed for at maskere disse fejl mere effektivt.



Et websted, der ser professionelt ud, men mangler verificerede kontaktoplysninger eller CVR oplysninger.



Udtale, der lyder unaturligt, mangler pauser og virker alt for flydende eller robotagtig. Vær opmærksom på "stemmekloning", selv om AI-genereret tale også kan lyde meget naturligt.



Videoer, hvor stemmen kan lyde robotagtig eller overdrejet glat, læbebevægelser og ansigtsudtryk, som ikke stemmer overens med talen, eller baggrund, belysning og skygger som er inkonsekvente. Disse er ofte AI-genererede videoer (deepfakes).

Skridt til at beskytte dig selv

1

Del aldrig personlige oplysninger eller bankoplysninger:

Legitime virksomheder vil aldrig bede om dine pinkoder, adgangskoder, netbankoplysninger eller sikkerhedskoder modtaget via e-mail, sms, sociale medier eller opkald.

2

Pause og tænk dig om, før du handler:

Skynd dig ikke med at sende penge, dele oplysninger eller klikke på links - svindlere skaber bevidst en følelse af hast (f.eks. IT-problemer med din bank, nødopkald, der involverer dine venner og familiemedlemmer, truende sprog osv.). I tilfælde af tvivl, også i mindre tvivlstilfælde, så bør du ikke handle; afslut opkaldet og kontrollér kilden eller identiteten omhyggeligt.

3

Kontrollér kilden/identiteten omhyggeligt:

- Kontrollér altid, hvor meddelelser, opkald, e-mails og links kommer fra - selvom de ser officielle ud, synes at komme fra en ven eller din familie eller endda en offentlig figur. F.eks. kan du ringe eller skrive til din familie og venner ved hjælp af et nummer du kender eller via en pålidelig kanal, søge efter stavfejl, mærkelige webadresser eller manglende sikkerhedsindikatorer (f.eks. tjekke at linket til webstedet indeholder et "s" i "HTTPS" for at sikre, at webstedet er sikkert, og tjekke om der er tilføjet eller mangler bogstaver i virksomhedens navn).
- Åbn ikke links fra uopfordrede beskeder, installer kun officielle applikationer gennem pålidelige appbutikker, og scan ikke ukendte QR-koder.
- Aftal med din familie et "safe word" - en hemmelig sætning, du kan bruge til at bekræfte identitet, hvis en person med en velkendt stemme ringer til dig med en hastende anmodning om penge og hævder at være et familiemedlem (f.eks. forældre, søskende, børn).
- Brug verificerede kontaktoplysninger til at kontakte virksomheden eller den enkelte direkte og stol aldrig på de kontaktoplysninger, som den mistænkte svindler har angivet (f.eks. søg efter virksomhedens navn uafhængigt, brug verificerede virksomhedsfortegnelser, tidligere bekræftede kontaktmetoder). Svindlere kan hævde at være godkendt eller efterligne webstedet for en autoriseret virksomhed. Kontrollér, om der er udstedt advarsler af virksomhedens nationale tilsynsmyndighed eller opført på IOSCO's I-SCAN-liste (iosco.org/i-scan/). For kryptoudbydere skal du kontrollere, om de er godkendt i EU (f.eks. kontrollere ESMA's register ([link](#))).

4

Vær opmærksom på potentielle AI-tricks:

Efterhånden som AI-teknologien udvikler sig, bliver svindel mere overbevisende end nogensinde - selv med de bedste sikkerhedstips. Hvis noget føles usædvanligt, eller du opdager nogen af de advarselstegn, der er skitseret ovenfor, skal du stoppe og revurdere.

5

Installer aldrig fjernadgangssoftware eller del din skærm:

Banker og finansielle institutioner vil aldrig anmode om det fra dig.

6

Hold enheder og konti sikre:

Brug stærke og unikke adgangskoder, hold dem hemmelige, og undgå at genbruge de samme legitimationsoplysninger på forskellige platforme. Aktivér multifaktorgodkendelse, hvor det er muligt. Se nogle passwords tips her ([link](#)). Hold din software- og antivirusbeskyttelse opdateret og aktiveret.

7

Vær forsigtig med uventede og tidsbegrænsede investeringsmuligheder:

Hvis det lyder for godt til at være sandt, så er det formentlig ikke sandt.

8

Tænk før du deler oplysninger på sociale medier:

Chatgrupper, fora, opslag på sociale medier og fotos kan være værdifulde kilder til viden for svindlere. At afsløre for meget om dig selv eller dine investeringer kan gøre dig til et nemt mål.

Hvad skal man gøre, når du er blevet offer for svindel



Straks stoppe transaktioner

For at blokere yderligere overførsler til mistænkelige konti og undgå yderligere tab. Stop al kontakt med svindlerne – ignorer deres opkald og e-mails og blokér afsenderen.



Kontakt din bank eller finansielle virksomhed:

Informér straks din bank eller finansielle virksomhed via officielle kontaktkanaler for at undersøge mulighederne for at fastfryse eller tilbageføre transaktioner.



Skift dine adgangskoder på alle dine enheder og apps/websteder.

Svindlere køber lækede adgangskoder online og prøver dem på flere konti. Det er ikke nok kun at ændre ét password. Sørg for at ændre dem alle, så svindlere ikke kan genbruge dem.



Indberetning og varsling:

Indberet hændelsen til politiet eller din nationale tilsynsmyndighed og informer dit netværk (f.eks. venner og familie) for at øge bevidstheden. Disse handlinger kan hjælpe dig med at beskytte dig selv og andre.



Pas på svindel i forbindelse med indrivelse:

Svindleren kan kontakte dig vel vidende, at du er offer for en tidligere svindelsforsøg, og hævde at være en offentlig myndighed (f.eks. politiet, skat eller en finansiell tilsynsmyndighed osv.) og tilbyde at inddrive dine tabte penge mod et gebyr. Dette er ofte et andet forsøg på at snyde dig. Husk: At blive snydt én gang forhindrer dig ikke i at blive snydt igen.

TYPER AF ONLINE FINANSIEL SVINDEL DREVET AF AI



IDENTITETS SVINDEL OG BRUG AF DEEP FAKE

Du modtager et uventet opkald fra en person, der hævder at være din bank, en offentlig myndighed (f.eks. politi, skatte- eller anden finansiell myndighed osv.), en forsikringsdistributør, et IT-selskab eller endda et familiemedlem. Den, der ringer, kan opfordre dig til at overføre penge for at holde dem sikre på baggrund af mistænkelig aktivitet på din konto eller din forsikringspolice. De kan også bede dig om at oplyse dine bankoplysninger (f.eks. betalingskortnummer, bankoplysninger eller adgangskoder), klikke på et link eller installere en software, der foregiver, at det hurtigt kan løse problemet. Den, der ringer op, kan bruge et forfalsket nummer, der ofte matcher din banks telefonnummer, så det fremstår legitimt (spoofing).

Svindlere kan bruge AI til at skabe falske videoer, billeder eller lyd, der efterligner en persons stemme (f.eks. din bankrådgiver eller et familiemedlem), ansigt (f.eks. en berømt person) eller bevægelser. Dette er kendt som "Deepfake".

Hvad kan der ske:

Ved at nævne personlige oplysninger og skabe en følelse af hast kan svindleren narre dig til handlinger, du ikke havde til hensigt at tage - såsom at sende penge til deres konto, klikke på et ondsindet link eller installere en malware på din enhed. Dette kan give svindleren direkte adgang til dine bankoplysninger. Med disse oplysninger kan de ændre din adgangskode, få adgang til din bankkonto og stjæle dine penge. Husk: Bare fordi en person, der ringer til dig, kender personlige oplysninger om dig, betyder det ikke, at han/hun er troværdig.



PHISHING OG SOCIAL ENGINEERING

Du modtager en e-mail eller besked, der ser ud til at komme fra din bank eller et finansielt selskab, og som advarer dig om "mistænkelig aktivitet" på din konto. Logoet, layoutet og sproget ser professionelt ud, og meddelelsen vises muligvis i samme tråd som andre samtaler fra din bank. Meddelelsen opfordrer dig til at klikke på et link for at bekræfte din konto eller nulstille din adgangskode. Linket fører til en falsk hjemmeside, der er identisk med din netbank. Uden at indse det, indtaster du dine oplysninger på et websted, der er designet til at stjæle dine personlige oplysninger.

Svindlere bruger AI til at udforme overbevisende phishingmeddelelser ved at analysere data fra sociale medier for at identificere deres ofre og tilpasse indholdet til hvert mål.

Hvad kan der ske:

Svindleren får adgang til din bankkonto og stjæler dine penge eller opretter en falsk profil med dine personlige oplysninger for at begå svindel.



INVESTERINGS- ELLER FORSIKRINGSSVINDEL

Du ser en annonce på sociale medier eller et websted, der promoverer en "tidsbegrænset investeringsmulighed med lav risiko" eller "tidsbegrænset rabat" på en forsikring fra en velkendt virksomhed. Annoncen indeholder et billede af en berømt person og anbefalinger, der ofte er falske. Når du har udtrykt interesse ved at klikke på et link eller udfylde en formular, bliver du kontaktet og omdirigeret til en platform eller meddelelseskanal, hvor du modtager professionelt udseende råd og dokumenter. Du opfordres til at investere et lille beløb, efterfulgt af større beløb, eller til at betale præmien i, hvad der synes at være en sikker konto.

Svindlere bruger AI-værktøjer til at gøre disse falske forslag eller e-mails meget overbevisende og vanskelige at opdage. De bruger også AI-drevne bots på sociale medier til at oprette falske konti, der interagerer med dig, spreder misinformation og simulerer reel adfærd for at få tillid og påvirke dine beslutninger.

Hvad kan der ske:

Efter at have forsøgt at hæve dine penge eller fremsætte et krav, holder kontaktpersonen op med at svare. Du opdager, at virksomheden ikke eksisterer, eller at risikoen, som du forsikrede, ikke er dækket. Du indser derefter, at du har sendt penge direkte til en svindler. Desværre kan du ikke få dine penge tilbage, og dine personlige og økonomiske oplysninger kan bruges til at begå yderligere svindel (f.eks. underskrive kontrakter på dine vegne, som kan føre til, at du mister endnu flere penge).



KÆRLIGHEDSSVINDEL

Du er blevet kontaktet på sociale medier, dating apps eller via telefon / sms af en person, du ikke har mødt i det virkelige liv. Denne person deltager i hyppige, personlige og romantiske samtaler og opbygger tillid ved hjælp af falske profiler. Over tid skifter samtalen mod penge eller økonomiske muligheder, såsom kryptoinvesteringer med løfter om højt afkast og lav risiko. Personen beder dig om at overføre penge til en konto eller guider dig gennem oprettelse af en konto og foretager en lille indledende indbetaling for at få svindlen til at se legitim ud, før de motiverer dig til at investere mere.

Svindlere bruger AI til at generere falske profiler, identificere deres ofre på sociale medier/datingapps ved hjælp af data, du har stillet til rådighed, eller bruge chatbots til at generere meddelelser.

Hvad kan der ske:

Svindleren trækker så mange penge ud som muligt, afskærer derefter al kommunikation og forsvinder. Den svigagtige investeringshjemmeside eller -app er taget offline, så du kan ikke få adgang til de formodede investeringer. Ud over økonomisk tab kan de personlige oplysninger, du har delt, bruges til at målrette svindel mod dine venner og familie eller til identitetstyveri, som kan have økonomiske eller juridiske konsekvenser for dig (f.eks. kan svindleren foretage køb, tage lån i dit navn, eller du kan blive holdt ansvarlig for gæld eller forbrydelser begået under dit navn, indtil det modsatte er bevist).



SVINDEL VED KØB AF VARER

Du støder på en attraktiv aftale for et køb på en online markedsplads. Den virksomhed, der tilbyder handlen, anmoder om en betaling udenom den officielle platform og hævder, at den anvender et "sikkert betalingssystem", og sender dig et link til at gennemføre købet. Linket omdirigerer dig til en svigagtig bankgodkendelsesside, der efterligner bankens officielle hjemmeside og bruger dens logo og design, så du indtaster dine online bankoplysninger for at foretage betalingen.

Svindlere bruger AI til at skabe meget overbevisende falske bankhjemmesider, ordrebekræftelser og fakturaer. AI hjælper dem med at efterligne ægte virksomheders tone, branding og stil. I nogle tilfælde bruger de AI-chatbots til at besvare spørgsmål og få aftalen til at virke mere troværdig.

Hvad kan der ske:

Betalingen via et tredjepartslink går udenom markedspladsens beskyttelse. Svindleren får dine login-oplysninger til din bankkonto og stjæler dine penge.