FINANSIELLA BEDRÄGERIER OCH SCAMS som sker digitalt i en AI-VÄRLD

VAR VAKSAM OCH SKYDDA DIG

Finansiella bedrägerier och scams som sker digitalt är inte nya, men artificiell intelligens (AI) har gjort dem smartare och svårare att upptäcka. Kriminella använder nu falska meddelanden och webbplatser, falska kändisprofiler och till och med AI-genererade röster eller videor som ser ut som din banktjänsteman, dina vänner eller din familj för att lura dig.

De når ofta ut till dig via sociala medier, chattappar, e-post och oväntade samtal som låter verkliga.

Du kan utsättas för risker som ekonomisk förlust, identitetsstöld och psykiskt lidande. Var försiktig och följ dessa viktiga tips för att vara säker:

Var uppmärksam på finansiella bedrägerier och scams som sker digitalt och drivs av AI,
t.ex. imitation, nätfiske, investerings- och försäkringsbedrägerier och till och med romansbedrägerier och scams. För att lära dig mer om olika typer av bedrägerier och scams se sida 5, 6 och 7.

Och här för bedrägerier och scams som är specifika för krypto ( ).

Upptäck varningssignaler:
Lär dig känna igen misstänkta beteenden, meddelanden eller erbjudanden (se sida 2);

Skydda dig själv:
Skydda din personliga information (se sida 3). och

Ha koll på vad du ska göra om du faller offer för bedrägerier
(se sida 4).

Varningssignaler

Ett löfte som verkar för bra för att vara sant.

Ett oväntat samtal från ett okänt nummer.

En brådskande begäran om pengar eller personlig information, inklusive från någon som låtsas vara en familjemedlem, en vän eller till och med en offentlig person.

En begäran om att ta kontroll över din enhet, ladda ner en app, skanna en QR-kod eller klicka på en länk.

En begäran om personlig information eller bankuppgifter (t.ex. lösenord, kreditkortsnummer, internetbankuppgifter eller säkerhetskoder).

En begäran om betalning via ospårbara metoder (t.ex. krypto, presentkort, banköverföringar eller förbetalda betalkort).

En misstänkt eller felaktig e-postadress eller länk (t.ex. stavfel i webbadressen eller ovanliga webbadresser).

En bilaga från en okänd källa, särskilt .exe, .scr, .zip eller makroaktiverad Office-fil (.docm, .xlsm).

Dålig grammatik eller slarvig formatering i ett dokument, även om AI kan göra det lättare för bedragare att dölja sådana brister.

En webbplats som ser professionell ut men saknar verifierade kontaktuppgifter eller information om företagets registrering.

Intonation som låter onaturligt, saknar pauser och verkar alltför flytande eller robotlik. Var uppmärksam på ”röstkloning”, även om AI-genererat tal också kan låta mycket naturligt.

Videor där rösten kan låta robotlik eller alltför slät, läpprörelser och ansiktsuttryck kan vara feljusterade med talet, eller bakgrund, belysning och skuggor kan vara inkonsekventa. Dessa är ofta AI-genererade videor (så kallade deepfakes).

Steg för att skydda dig själv

1 **Dela aldrig personlig information eller bankinformation:**

Legitima företag kommer aldrig att be om dina PIN-koder, lösenord, internetbankuppgifter eller säkerhetskoder via e-post, sms, sociala medier eller telefon.

2 **Pausa och tänk efter innan du agerar:**

Skynda dig inte att skicka pengar, dela information eller klicka på länkar – bedragare skapar medvetet en känsla av brådska (t.ex. it-problem hos din bank, nödsamtal med dina vänner och familjemedlemmar, hotfullt språk osv.). I händelse av tvivel, även mindre, agera inte; avsluta samtalet och verifiera källan eller identiteten noggrant.

3 **Kontrollera källan/identiteten noggrant:**

- Kontrollera alltid var meddelanden, samtal, e-postmeddelanden och länkar kommer ifrån - även om de ser officiella ut, verkar komma från en vän eller din familj, eller till och med en offentlig person. Till exempel, ring eller smsa din familj och vänner med hjälp av ett känt nummer via en betrodd kanal; leta efter stavfel, konstiga webbadresser eller säkerhetsindikatorer som saknas (t.ex. kontrollera att webbplatslänken innehåller ett ”s” i ”HTTPS” för att se till att webbplatsen är säker och kontrollera om det finns några tillsatta eller saknade bokstäver i företagsnamnet).

- Öppna inte länkar från oönskade meddelanden, installera bara officiella applikationer via betrodda appbutiker och skanna inte okända QR-koder.

- Kom överens med din familj om ett “säkert ord”- en hemlig fras som du kan använda för att bekräfta identiteten om någon med en bekant röst ringer dig med en brådskande begäran om pengar och påstår sig vara en familjemedlem (t.ex. föräldrar, syster / bror, barn).

- Använd verifierade kontaktuppgifter för att nå företaget eller individen direkt och förlita dig aldrig på de kontaktuppgifter som tillhandahålls av den misstänkta bedragaren (t.ex. sök efter företagets namn självständigt, använd verifierade företagskataloger, tidigare bekräftade kontaktmetoder). Bedragare kan hävda att de är auktoriserade eller efterlikna ett auktoriserat företags webbplats. Kontrollera om några varningar har utfärdats av din nationella finansiella tillsynsmyndighet eller tagits upp i Iosco I-SCAN-förteckningen (iosco.org/i-scan/). För kryptoleverantörer, kontrollera om de är auktoriserade i EU (t.ex. kontrollera Esmas register ( ).

4 **Var uppmärksam på potentiella AI-trick:**

När AI-tekniken utvecklas blir bedrägerier mer övertygande än någonsin - även med de bästa säkerhetstipsen. Om något känns ovanligt eller om du upptäcker någon av de varningssignaler som beskrivs ovan, stoppa och ompröva.

5 **Installera aldrig fjärråtkomstprogram eller dela din skärm:**

Banker och finansiella institut kommer aldrig att begära det från dig.

6 **Håll enheter och konton säkra:**

Använd starka och unika lösenord, håll dem hemliga och undvik att återanvända samma inloggningsuppgifter på olika plattformar. Aktivera multifaktorautentisering där så är möjligt. Se några tips om lösenord här ( ). Håll din programvara och ditt antivirusskydd uppdaterat och aktiverat.

7 **Var försiktig med oväntade och tidsbegränsade investeringsmöjligheter:**

Om det låter för bra för att vara sant, är det förmodligen det.

8 **Tänk efter innan du delar information på sociala medier:**

Chattgrupper, forum, inlägg på sociala medier och foton kan vara värdefulla kunskapskällor för bedragare. Att avslöja för mycket om dig själv eller dina investeringar kan göra dig till ett enkelt mål.

Vad du ska göra om du har blivit offer för bedrägeri eller scams

Stoppa omedelbart transaktioner

För att blockera ytterligare överföringar till misstänkta konton och undvika ytterligare förluster. Stoppa all kontakt med bedragarna – ignorera deras samtal och e-postmeddelanden och blockera avsändaren.

Kontakta din bank eller ditt finansiella företag:

Informera din bank eller finansiella företag omedelbart via officiella kontaktkanaler, för att undersöka alternativ för frysning eller reversering av transaktioner.

Ändra dina lösenord på alla dina enheter och appar/webbplatser.

Bedragare köper läckta lösenord online och försöker använda dem på flera konton. Det räcker inte med att bara byta ett lösenord. Se till att ändra dem alla, så att bedragare inte kan återanvända dem.

Rapport och varning:

Anmäl incidenten till polisen och din nationella finansiella tillsynsmyndighet (↖) och informera ditt nätverk (t.ex. vänner och familj) för att öka medvetenheten. Dessa åtgärder kan hjälpa dig att skydda dig själv och andra.

Se upp för återhämtningsbedrägerier:

Bedragaren kan kontakta dig med vetskap om att du är offer för en tidigare bluff, som påstår sig vara en offentlig myndighet (t.ex. polis, skatte- eller finansiell tillsynsmyndighet etc.) och erbjuder sig att återkräva dina förlorade pengar mot en avgift. Detta är ofta ett annat försök att lura dig. Kom ihåg: Att bli lurad en gång hindrar dig inte från att bli lurad igen.

Europeiska bankmyndigheten, Europeiska försäkrings- och tjänstepensionsmyndigheten, Europeiska värdepappers- och marknadsmyndigheten, 2025

Luxemburg: Europeiska unionens publikationsbyrå, 2025

PDF ISBN 978-92-9407-243-6 doi:10.2853/9588197 DZ-01-25-131-SV-N

Typer av finansielliella BEDRÄGERIER och SCAMS som sker digitalt och drivs av AI

Identitetsbedrägerier och användning av deep fake

Du får ett oväntat samtal från någon som påstår sig vara din bank, en offentlig myndighet (t.ex. polis, skatte- eller finansiell tillsynsmyndighet etc.), en försäkringsdistributör, ett IT-företag eller till och med en familjemedlem. Den som ringer kan uppmana dig att överföra pengar för att hålla dem säkra, med hänvisning till misstänkt aktivitet på ditt konto eller din försäkring. De kan också be dig att avslöja dina bankuppgifter (t.ex. betalkortsnummer, internetbankuppgifter eller lösenord), klicka på en länk eller installera en programvara och låtsas att de snabbt kan lösa problemet. Den som ringer kan använda ett förfalskat nummer som ofta matchar din banks telefonnummer för att framstå som legitimt (så kallad spoofing).

Bedragare kan använda AI för att skapa falska videor, bilder eller ljud som efterliknar någons röst (t.ex. din banktjänsteman eller familjemedlem), ansikte (t.ex. en kändis) eller rörelser. **Detta kallas ”deep fake”.**

Detta kan hända:

Genom att nämna personuppgifter och skapa en känsla av brådska lurar bedragaren dig till åtgärder som du inte hade för avsikt att vidta – till exempel att skicka pengar till deras konto, klicka på en skadlig länk eller installera ett skadligt program på din enhet. Detta kan ge bedragaren direkt tillgång till dina bankuppgifter. Med denna information kan de ändra ditt lösenord, komma åt ditt bankkonto och stjäla dina pengar. Kom ihåg: Bara för att den som ringer känner till dina personuppgifter betyder det inte att han eller hon är pålitlig.

Nätfiske och social ingenjörskonst (social engineering)

Du får ett e-postmeddelande eller meddelande som verkar komma från din bank eller ett finansiellt företag och varnar dig för ”misstänkt aktivitet” på ditt konto. Logotypen, layouten och språket ser professionella ut, och meddelandet kan visas i samma tråd som andra konversationer från din bank. Meddelandet uppmanar dig att klicka på en länk för att verifiera ditt konto eller återställa ditt lösenord. Länken leder till en falsk webbplats som ser identisk ut med din internetbank. Utan att inse det anger du dina uppgifter på en webbplats som är utformad för att stjäla din personliga information.

Bedragare använder AI för att skapa övertygande nätfiske-meddelanden genom att analysera data från sociala medier för att identifiera sina offer och anpassa innehållet för varje mål.

Detta kan hända:

Bedragaren kommer åt ditt bankkonto och stjäl dina pengar eller skapar en falsk profil med dina personuppgifter för att begå ett bedrägeri.

Investerings- eller försäkringsbedrägeri

Du ser en annons på sociala medier eller en webbplats som marknadsför en ”tidsbegränsad investeringsmöjlighet med låga risker” eller ”tidsbegränsad rabatt” på en försäkring från ett välkänt företag. Annonsen innehåller ett kändisfoto och rekommendationer som ofta är falska. Efter att ha uttryckt intresse genom att klicka på en länk eller fylla i ett formulär kontaktas du och omdirigeras till en plattform eller meddelandekanal där du får professionell rådgivning och dokument. Du uppmuntras att investera ett litet belopp, följt av större summor, eller att betala premien till vad som verkar vara ett säkert konto.

Bedragare använder AI-verktyg för att göra dessa falska förslag eller e-postmeddelanden mycket övertygande och svåra att upptäcka. De använder också AI-drivna sociala mediebots för att skapa falska konton som interagerar med dig, sprider felaktig information och simulerar verkliga beteenden för att få förtroende och påverka dina beslut.

Detta kan hända:

Efter att ha försökt ta ut dina pengar eller göra ett anspråk slutar kontakten att svara. Du upptäcker att företaget inte finns eller att försäkringen inte gäller för det du trodde att den skulle täcka. Du inser då att du har skickat pengar direkt till en bedragare som en del av ett bedrägligt system. Tyvärr kan du inte få tillbaka dina pengar, och dina personliga och ekonomiska uppgifter kan användas för att begå ytterligare bedrägerier (t.ex. underteckna kontrakt för din räkning som kan leda till att du förlorar ännu mer pengar).

Romansbedrägeri och bluffar

Du har blivit kontaktad på sociala medier, dejtingappar, eller via telefon / sms av någon du inte har träffat i verkliga livet. Den här personen engagerar sig i frekventa, personliga och romantiska konversationer och bygger förtroende med hjälp av falska profiler. Med tiden skiftar samtalet mot pengar eller finansiella möjligheter, såsom kryptoinvesteringar med löften om hög avkastning och låg risk. Personen ber dig att överföra pengar till ett konto eller guidar dig genom att skapa ett konto och göra en liten första insättning för att få systemet att se legitimt ut innan de uppmuntrar dig att investera mer.

Bedragare använder AI för att skapa falska profiler, identifiera sina offer på sociala medier/dejtingappar med hjälp av data som du har gjort tillgänglig eller använda chatbots för att generera meddelanden.

Detta kan hända:

Bedragaren extraherar så mycket pengar som möjligt, stänger sedan av all kommunikation och försvinner. Den bedrägliga investeringswebbplatsen eller appen tas offline, vilket gör att du inte kan komma åt de förmodade investeringarna. Utöver ekonomisk förlust kan de personuppgifter du delat användas för att rikta in sig på dina vänner och din familj eller för identitetsstöld som kan få ekonomiska eller rättsliga konsekvenser för dig (t.ex. kan bedragaren göra inköp, ta lån i ditt namn, eller så kan du hållas ansvarig för skulder eller brott som begåtts i ditt namn tills motsatsen bevisas).

Bedrägeri vid köp

Du stöter på en attraktiv affär för ett köp på en digital marknadsplats. Företaget som erbjuder affären begär en betalning utanför den officiella plattformen och hävdar att det använder ett ”säkert betalningssystem” och skickar en länk till dig för att slutföra köpet. Länken omdirigerar dig till en bedräglig bankautentiseringssida som imiterar bankens officiella webbplats och använder dess logotyp och design, så att du anger dina digitala bankuppgifter för att göra betalningen.

Bedragare använder AI för att skapa mycket övertygande falska bankwebbplatser, orderbekräftelser och fakturor. AI hjälper dem att efterlikna tonen, varumärket och stilen hos det riktiga företaget. I vissa fall använder de AI-chatbots för att svara på frågor och få affären att verka mer trovärdig.

Detta kan hända:

Betalningen via en tredjepartslänk kringgår marknadens skydd. Bedragaren får dina inloggningsuppgifter till ditt bankkonto och stjäl dina pengar.