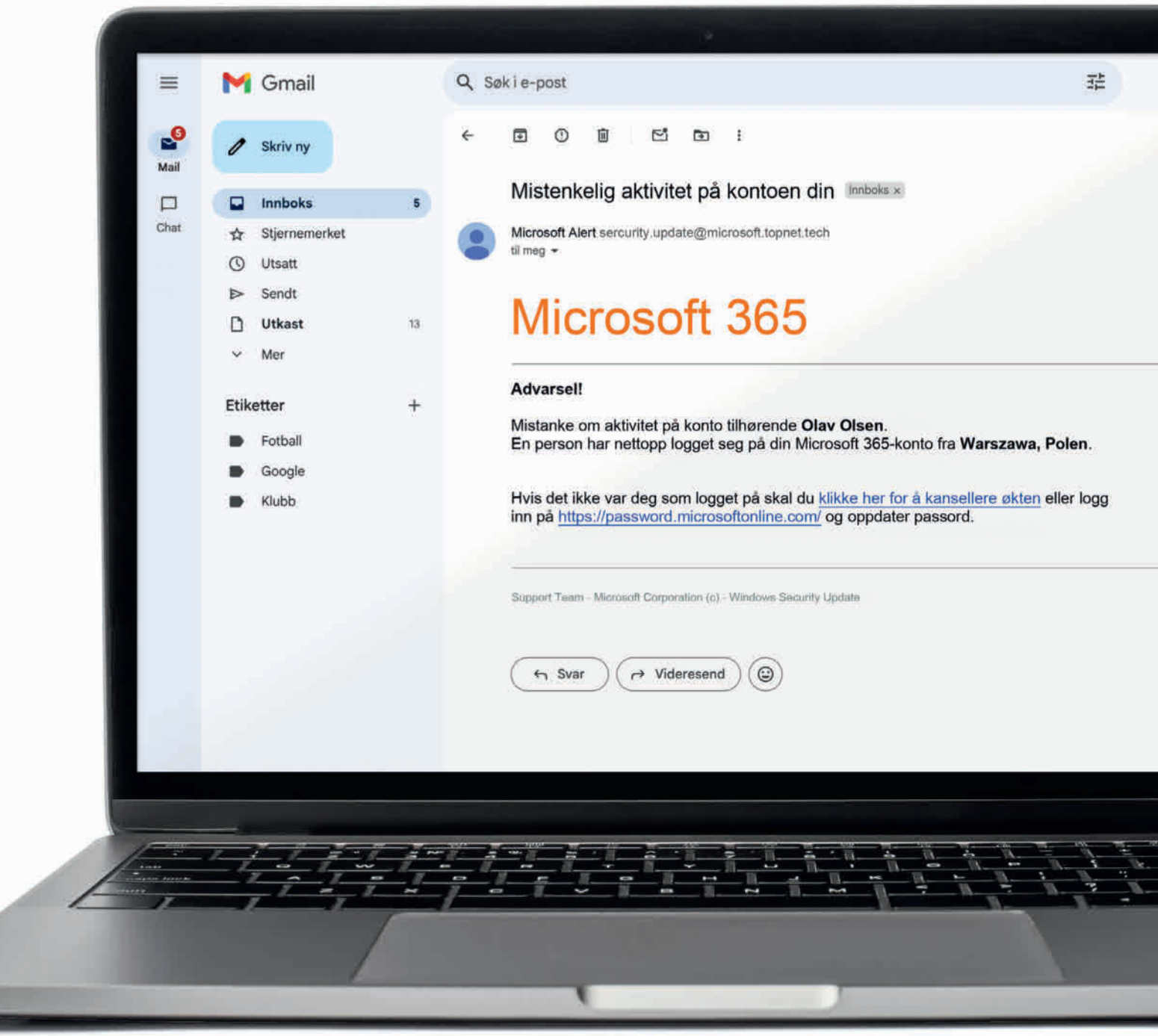
Ser du hva som viser at denne e-posten er farlig?



SVAR: Underlig avsenderadresse

På skjermen ser du et eksempel på hvordan en e-post som utgir seg for å komme fra Microsoft, og handler om mistenkelig aktivitet, kan se ut. E-posten er egentlig fra en svindler, og det ser du blant annet ved å kaste et kritisk blikk på avsenderadressen. Den er lang og krongle-te og oppfyller ikke standarden man må kunne forvente fra et seriøst selskap som Microsoft.

SVAR: Feil logo

Et annet tegn på at denne e-posten er fra svindlere, og ikke fra Microsoft, er at Microsoft 365-grafikken ikke stemmer overens med selskapets grafiske uttrykk. For det første er ikke skriftfargen den samme som Microsoft benytter i sin markedsføring. For det andre ville teksten "Microsoft 365" alltid vært ledsaget av den velkjente Microsoft-logoen til venstre for teksten.

Foto: Random435/Shutterstock.com

SLIK OPPDAGER DU SVINDELFORSØKENE:

10 sikre tegn på en farlig e-post

Hackere sender ut svindelmeldinger som aldri før, og derfor gjelder det å vite hvilke tegn du skal se etter for å avsløre bedrageriforsøket.

Journalist
Martin Lorentsen

Det dukker opp et e-brev i innboksen som ser ut til å stamme fra et transportselskap. Budskapet går ut på at det er en pakke på vei med posten, men at det har oppstått et lite problem. Pakken kan nemlig ikke leveres før du har betalt et mindre beløp.

Det virker umiddelbart troverdig, og du føler kanskje at du bør reagere, men e-post av denne typen er nesten alltid svindel. Her forsøker svindlere å benytte nettfiske til å frarøve deg følsomme opplysninger som betalingsinformasjon, personnummer eller passord. Dessverre dukker det opp stadig flere av disse e-postene i milliarder av innbokser over hele verden. Globalt antas det nå at 1,2 prosent av all e-post som sendes, egentlig er forsøk på nettfiske.

Prisen kan bli høy

Går du i en av hackernes mange feller, risikerer du først og fremst å installere skadevare på din egen pc. Det kan føre til at du senere mister personlige, viktige filer. Du kan også havne i et langt verre uføre og for eksempel bli utsatt for identitetstyveri eller i verste fall miste alle dine oppsparte midler – hvis hackerne klarer å lure deg til å utlevere sensitiv informasjon.

Hackerne har blitt flinkere

Noen svindelforsøk er lettere å gjennomskue enn andre, men den teknologiske utviklingen gjør det stadig mer krevende å oppdage hva som er svindel og hva som er ekte.

Tidlig i 2025 måtte for eksempel Google sende ut en advarsel til alle Gmail-brukere om at 2,5 milliarder kontoer hadde blitt mål for hackere som benyttet kunstig intelligens til å gjøre svindelforsøkene mer troverdige.

Heldigvis er det langt fra alle hackere som er så utspekulerte, og det er ikke på noen måte umulig å gjennomskue svindelforsøkene. Men det krever at du vet hvilke tegn du skal se etter i innboksen.

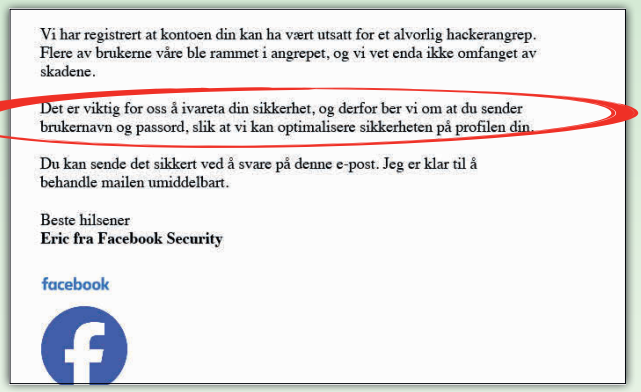
Mange tegn går igjen på mobilen

Nettfiske foregår ikke bare via e-post, men også via sms-meldinger i et fenomen som kalles ”smishing”. På samme måte som via e-post forsøker svindlerne å lure deg til å klikke på koblinger, åpne vedlagte filer eller oppgi personlige data. Mange av faresignalene som gjelder for e-post, gjør seg også gjeldende for tekstmeldinger.

Du blir bedt om å oppgi følsom informasjon

Uansett hvor korrekt språket er og hvor troverdig meldingen virker, må du aldri oppgi følsom informasjon som passord i en e-post. Det gjelder særlig hvis meldingen kommer uten noen forutgående dialog der du blir bedt om å gjøre det.

Selskaper som Facebook eller Netflix, banken din eller myndighetene vil aldri be deg om å oppgi slik informasjon via vanlig e-post.



Vi har registrert at kontoen din kan ha vært utsatt for et alvorlig hackerangrep. Flere av brukerne våre ble rammet i angrepet, og vi vet enda ikke omfanget av skadene.

Det er viktig for oss å ivareta din sikkerhet, og derfor ber vi om at du sender brukernavn og passord, slik at vi kan optimalisere sikkerheten på profilen din.

Du kan sende det sikkert ved å svare på denne e-post. Jeg er klar til å behandle mailen umiddelbart.

Beste hilsener
Eric fra Facebook Security

facebook

Blir du bedt om å sende en e-post med passordet ditt, bør alle varsellamper blinke. Det vil nemlig aldri et legitimt firma be om.

faktura12385.pdf
370 KB

PAYMENT

Hei,

vennligst gå gjennom den vedlagte fakturaen og fullfør betalingen innen forfallsdato.

Du finner fakturaen som vedlegg og via lenken.

Totalbeløp: $479.00 USD

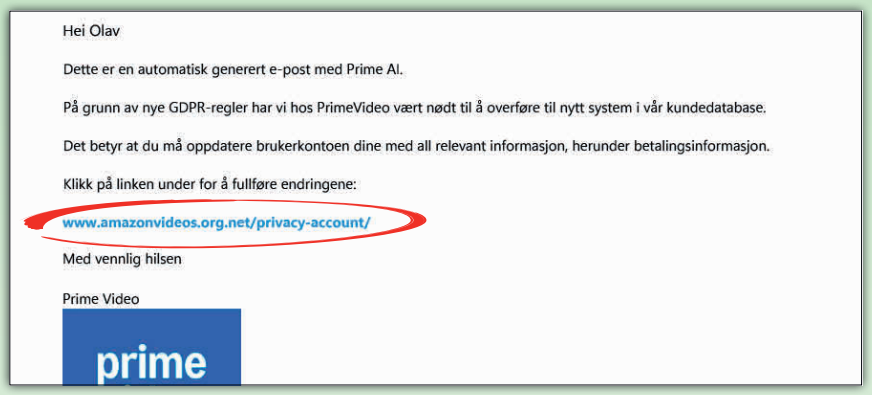
Se og betal fakturaen

Det er gjerne en falsk faktura som svindlere oppfordrer deg til å åpne på pc-en, slik at du kan betale det du skylder.

Pass deg for vedlagte filer

Hvis du mottar en e-post der du blir bedt om å åpne en vedlagt fil, er det stor fare for at det er forsøk på svindel. Det er ikke uvanlig at hackere skjuler virus og skadevare i selv vanlige filtyper som pdf-filer, som vanligvis brukes til for eksempel fakturaer eller kontrakter.

Hvis du åpner den vedlagte filen på pc-en, risikerer du å aktivere en skjult kildekode som infiserer maskinen med skadelig programvare. Det kan være løsepengevirus som låser filene dine og krever betaling for å låse dem opp, eller spionprogrammer til å overvåke deg.



Hei Olav

Dette er en automatisk generert e-post med Prime AI.

På grunn av nye GDPR-regler har vi hos PrimeVideo vært nødt til å overføre til nytt system i vår kundedatabase.

Det betyr at du må oppdatere brukerkontoen dine med all relevant informasjon, herunder betalingsinformasjon.

Klikk på linken under for å fullføre endringene:

www.amazonvideos.org.net/privacy-account/

Med vennlig hilsen

Prime Video

prime

Denne koblingen er lang og stemmer ikke med avsenderens domene.

Manglende samsvar mellom domene og kobling

Lenker og e-postadresser fra svindlere vil ofte ha ukurante domenenavn som ikke samsvarer med det offisielle navnet på selskapet svindlerne hevder å representere.

I eksempelet over har man forsøkt å utgi seg for å være fra strømmetjenesten Prime Video, men koblingen, eller URL-adressen, som du blir bedt om å klikke på i meldingen, heter ”amazonvideos.org”, og det er jo noe annet enn det virkelige domenet, nemlig ”primevideo.com”.

Noen hackere skjuler en falsk hjemmeside bak en kobling som ligner det riktige domenet. Det er lett å sjekke om en lenke er legitim ved å kopiere den til utklippstavlen og legge den inn i verktøyet for sjekk av nettsider hos sikkerhetsselskapet TrendMicro. Det finner du her: **komputer.no/lenkesjekk**

Ubehjelpelig språk

Selv om kunstig intelligens gjør det lettere å skjule svindel, er mange svindelmeldinger preget av et håpløst uidiomatisk språk. Svindlere vil gjerne lure alle, uansett nasjonalitet, og derfor er de ikke så nøye med språkbruken.

Vær særlig skeptisk til språkfeil og formuleringer som ikke virker norske, for eksempel altfor mange eiendomspronomener …

(!) Abonnementet ditt er kansellert

Hei Ove

Betalingen din ble avvist fordi kortutstederen din ikke kunne validere betalingsmåten din (Visa****). Klikk for mer informasjon om avviste betalinger

Oppdater betalingsmåten din slik at abonnementet ditt (Google One) opprettholdes.

OPPDATER KORTBETALING

Uvanlig ordvalg og stavefeil er klare tegn på at det er snakk om svindel.

Du vil jo ikke gå glipp av en pakke!

Et av de mer utbredte svindelforsøkene handler om en pakkeutlevering som skal ha gått skeis. Meldingen, som ofte også sendes som sms, kommer som regel uventet og inneholder en kobling du må klikke på for å "rette opp feilen".

E-posten kan for eksempel påstå at det er feil i mottakeradressen, eller at det har kommet et uventet tollkrav på pakken, som skal betales via en lenke. Hvis du ikke reagerer, risikerer du ifølge meldingen at pakken blir returnert.

Får du e-post av denne typen, bør du alltid sjekke om du faktisk har bestilt noe, og om det i så fall skal leveres av transportøren som angivelig har sendt meldingen.


[Postinformasjon]:

Varen din har ankommet leveringsstasjonen, men kan ikke leveres fordi informasjonen på ytteremballasjen er uklar.

Vennligst klikk på lenken nå: http://is.gd/8yequFC?psg=olbjqei

Vi sender deg en ny e-post så snart informasjonen er oppdatert.

Takk for at du tok deg tid

DHL

Klikk aldri på koblingen! I stedet tar du kontakt med fraktselskapet via den offisielle hjemmesiden for å finne ut hva som har skjedd.


Avast

WARNING

HØY RISIKO REGISTRERT

Advarsel: Det er oppdaget skadelig aktivitet på din pc.

Alvorlighetsgrad: Høy
Tidspunkt: 12:42 - 10/03/2025
Aktivitet: Beskyttelse
Detaljer: En uautorisert pålogging i Windows tilhørende: Olav Olsen

Takk,
Avast

I stedet for å bli beskyttet, blir pc-en infisert av virus hvis du gjør som meldingen ber deg om.

Antivirusprogrammet sender advarsler via e-post

Med mindre du har abonnert på et nyhetsbrev, hører du sjelden fra antivirusprogrammet ditt via e-post, og i hvert fall ikke om trusler på maskinen. Slike advarsler vises direkte på pc-skjermen.

Får du e-post som hevder å være sendt fra antivirusprogrammet, kan du trygt slette den. I stedet åpner du antivirusprogrammet på maskinen og kjører et virussøk – for sikkerhets skyld.

E-posten prøver å stresse deg ved å gi inntrykk av at noe haster

Mange av oss treffer forhastede slutninger når vi får panikk. Derfor har e-postsvindel ofte en lettere alarmistisk tone. Det kan for eksempel hevdes at du vil miste tilgangen til en brukerkonto hvis du ikke følger instruksene i e-posten. Meldingen vil ofte inneholde en kobling til en falsk nettside som ligner den offisielle. Hvis du legger inn påloggingsinformasjon der, gir du hackerne tilgang.

Er du i tvil, kan du alltid sjekke kontoen til tjenesten som omtales i e-posten, ved å oppsøke selskapets offisielle nettside eller åpne den tilhørende appen og logge inn for å se om alt er som det skal.


NETFLIX

Unngå å miste bruker

Grunnet for mange registrerte devices på brukeren d , lukker vi kontoen din innen 24 timer.

Du kan hindre dette nå ved å gå til neftlix.net/account

Her skal du logge inn med brukernavn og melde av en device innen 24 timer.

Etter 24 timer ser vi oss nødt til å lukke brukeren din og du mister alle data fra din Netflix.

Best wishes
Netflix

Du får vite at det er noe galt med kontoen, og at du må skynde deg å gjøre endringer innen en viss tidsfrist.


CONGRATS!
YOU'VE WON!

Hei Olav

Gratulerer! Du har vunnet hovedpremien MacBook Air i vår "Anniversay Giveaway" konkurranse.

Her ser du hvordan du gjør krav på premien:

1. Send en e-mail til jordanstarr@applecontestwin.com og bekreft at du har vunnet.
2. Vennligst bekreft at det er OK at vi publiserer fornavnet ditt på hjemmesiden vår og våre sosiale mediekanaler.
3. Det er valgtfritt, men hvis du er like glad for å vinne som vi er, så ta en selfie og send den til oss.

Har du spørsmål, er det bare å svare på denne mailen, så er jeg glad for å være til hjelp.

Vennlig hilsen fra Jordan

Får du en e-post ut av det blå om at du har vunnet en eller annen konkurranse, har det neppe rot i virkeligheten.

Du må bare bekrefte noe …

Det er alltid hyggelig med gode nyheter, for eksempel om at du har arvet et større beløp fra en fjern og ukjent slektning eller har vunnet en stor premie. Haken er bare at du må bekrefte noe før du kan få pengene.

Ifølge avsenderen kan det gjøres både raskt og enkelt, men det er som regel svindlere som står bak slike meldinger. Når du tror du bekrefter mottak av en premie, gir du i stedet uvedkommende tilgang til personlig informasjon og kan dermed få alvorlige problemer.

Får du e-post av denne typen, bør du først sjekke om du har deltatt i konkurransen som nevnes. Ta eventuelt kontakt med avsender, men uten å klikke i e-posten.