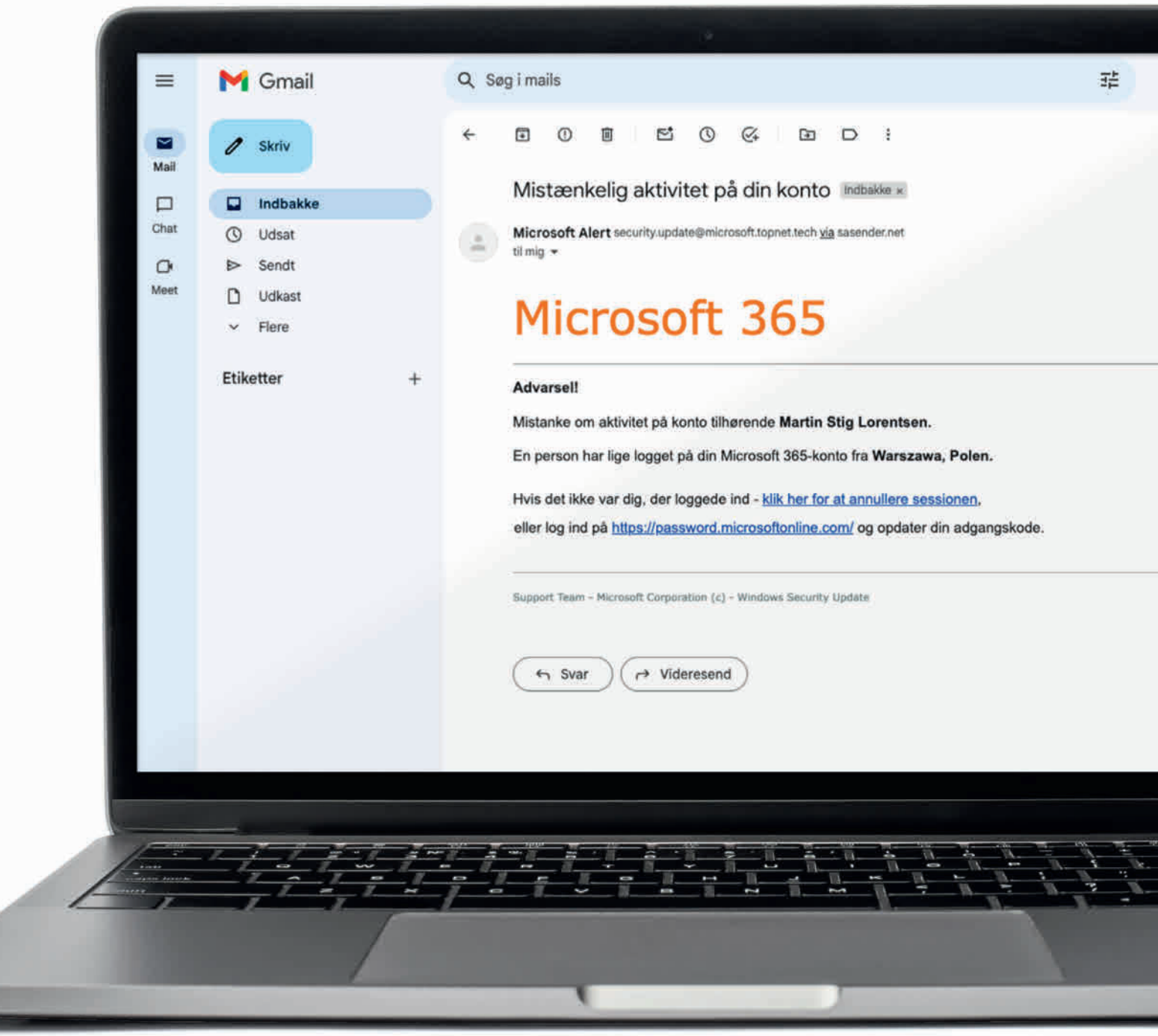
Kan du se, hvad der afslører, at denne mail er farlig?



SVAR: Afsenderen ser mærkelig ud

På skærmen ser du et eksempel på, hvordan en mail, der angiveligt kommer fra Microsoft og handler om mistænkelig aktivitet, kan se ud. I virkeligheden er mailen fra en svindler, og det kan du blandt andet opdage ved at nærstudere afsenderadressen. Den er lang og kringlet og udstråler ikke den adressestandard, som man må forvente fra et kæmpefirma som Microsoft.

SVAR: Logoet er forkert

Et andet tegn på, at denne mail er fra svindlere og ikke fra Microsoft, er, at Microsoft 365-grafikken ikke stemmer overens med det rigtige grafiske udtryk. For det første er skriftfarven ikke den, som Microsoft bruger i sin markedsføring, og for det andet ville teksten "Microsoft 365" altid være ledsaget af Microsofts velkendte logo til venstre for teksten.

Foto: Random435/Shutterstock.com

SÅDAN FÅR DU ØJE PÅ SVINDEL I TIDE:

10 sikre tegn på en farlig mail

Hackere sender svindelmails som aldrig før, og derfor er det vigtigt, at du ved, hvilke tegn du skal holde øje med, når du får en mistænkelig mail.

Journalist
Martin Lorentsen

Der dukker en e-mail op i indbakken, der ser ud til at være fra et leveringsfirma. I mailen står der, at du har en pakke på vej med posten, men at der er opstået et lille problem: Pakken kan ikke leveres, medmindre du betaler et mindre beløb.

Mailen virker umiddelbart troværdig, og du føler måske, at du bør reagere, men den slags mail er næsten altid svindel. Her forsøger svindlere gennem phishing at franarre dig dine personfølsomme data som betalingsoplysninger, CPR-nummer eller adgangskoder. Og der dukker flere og flere af den slags mails op i vores indbakker. Det anslås således, at 1,2 procent af alle mails, der sendes på verdensplan, er phishingangreb.

Phishing kan koste dig dyrt

Hvis du falder i en af hackernes mange fælder, risikerer du først og fremmest at installere malware på din computer, hvilket blandt andet kan føre til, at du senere mister dine filer. Men du kan også komme i langt større problemer og fx blive udsat for identitetstyveri eller i færste fald miste hele din opsparing, hvis hackerne formår at narre dig til at udlevere dine personfølsomme oplysninger.

Hackere skjuler svindel bedre

Nogle svindelmails er mere åbenlyse end andre, men den teknologiske udvikling gør det stadig sværere at gennemskue, hvad der er svindel, og hvad der er en legitim mail.

I begyndelsen af 2025 måtte Google fx udsende en advarsel til sine mange brugere af Gmail om, at 2,5 milliarder konti var blevet mål for hackere, der brugte kunstig intelligens til at gøre deres svindel mere troværdig.

Heldigvis er det langt fra alle hackere, der er så udspekulerede, og det er bestemt ikke umuligt at gennemskue, når en mail er svindel. Men det kræver, at du ved, hvilke tegn du skal holde øje med i din indbakke.

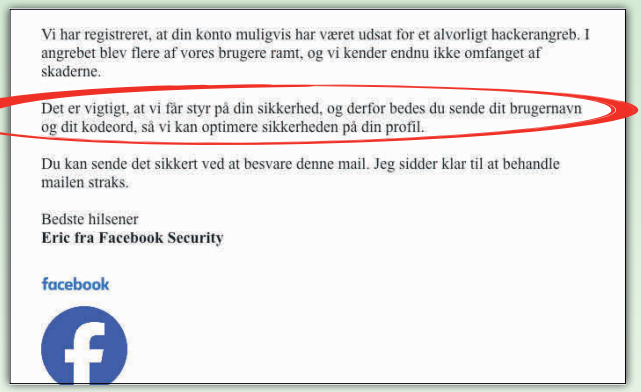
Mange tegn går igen på telefonen

Phishing foregår ikke kun via e-mail, men også via sms-beskeder på mobilen, hvor fænomenet kaldes “smishing”. Ligesom via mail forsøger svindlerne at narre dig til at klikke på links, åbne vedhæftede filer eller oplyse personlige data. Mange af de faresignaler, der gælder for e-mails, bør du også holde øje med i sms-indbakken.

Mailen beder dig om at udlevere følsomme oplysninger

Uanset hvor korrekt sproget i en mail er, og hvor troværdig den ser ud, skal du aldrig skrive følsomme oplysninger som adgangskoder i en mail. Det gælder særligt mails fra en afsender, der uden forudgående dialog beder dig om at gøre det.

Virksomheder som Facebook eller Netflix, din bank eller offentlige myndigheder vil aldrig bede dig om at udlevere dine oplysninger via en helt almindelig e-mail.



Vi har registreret, at din konto muligvis har været udsat for et alvorligt hackerangreb. I angrebet blev flere af vores brugere ramt, og vi kender endnu ikke omfanget af skaderne.

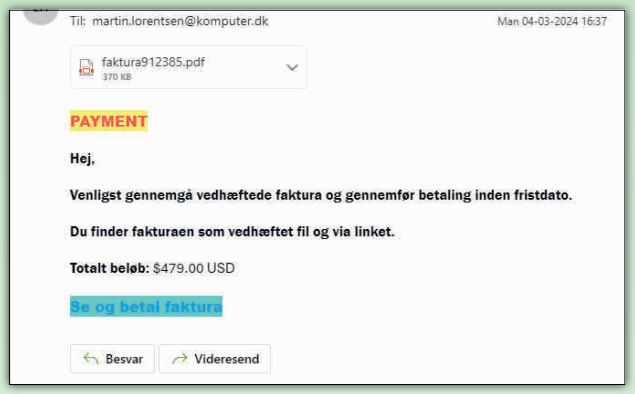
Det er vigtigt, at vi får styr på din sikkerhed, og derfor bedes du sende dit brugernavn og dit kodeord, så vi kan optimere sikkerheden på din profil.

Du kan sende det sikkert ved at besvare denne mail. Jeg sidder klar til at behandle mailen straks.

Bedste hilsener
Eric fra Facebook Security

facebook

Bliver du bedt om at sende en mail med dit kodeord, bør dine alarmklokker ringe, for det vil et legitimt firma aldrig bede om.



Til: martin.lorentsen@komputer.dk Man 04-03-2024 16:37

faktura912385.pdf
370 KB

PAYMENT

Hej,

Venligst gennemgå vedhæftede faktura og gennemfør betaling inden fristdato.

Du finder fakturaen som vedhæftet fil og via linket.

Totalt beløb: $479.00 USD

Se og betal faktura

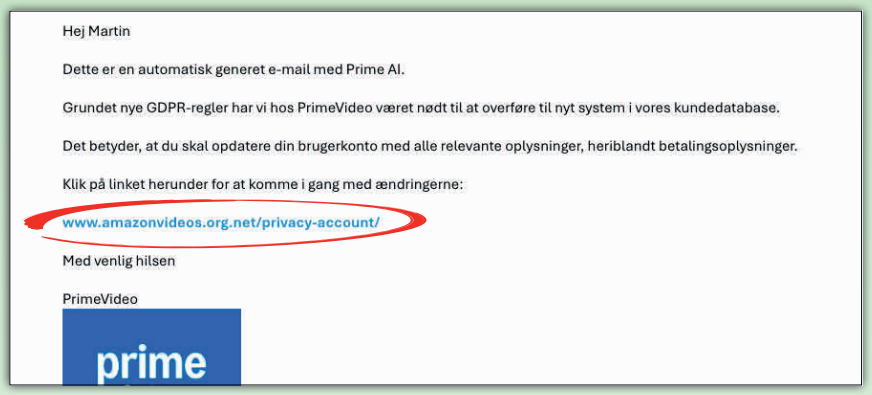
Besvar Videresend

Typisk er det en falsk faktura, som svindlere opfordrer dig til at åbne på din pc, så du kan betale det, du skylder.

Pas på vedhæftede filer

Hvis du modtager en mail, hvor du opfordres til at åbne en vedhæftet fil, kan der være svindlere på spil. Det er ikke unormalt, at hackere skjuler virus og malware i selv de mest almindelige filtyper som PDF-filer, der typisk bruges til fx fakturaer eller kontrakter.

Hvis du åbner den vedhæftede fil på din pc, risikerer du at aktivere en skjult kildekode, der inficerer din computer med skadelig software. Det kan være ransomware, der låser dine filer og kræver betaling for at låse dem op, eller spyware, der overvåger din færden.



Hej Martin

Dette er en automatisk generet e-mail med Prime AI.

Grundet nye GDPR-regler har vi hos PrimeVideo været nødt til at overføre til nyt system i vores kundedatabase.

Det betyder, at du skal opdatere din brugerkonto med alle relevante oplysninger, heriblandt betalingsoplysninger.

Klik på linket herunder for at komme i gang med ændringerne:

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

Med venlig hilsen

PrimeVideo

prime

Linket her er langt og matcher ikke afsenderens domæne.

Linket i mailen passer ikke med domænet

Links og mailadresser i mails fra svindlere vil ofte have mærkværdige domæner, der ikke passer til det officielle firma, som svindlerne udgiver sig for at være.

I ovenstående eksempel har man forsøgt at udgive sig for at være fra streamingtjenesten Prime Video, men linket, eller URL-adressen, som du bedes klikke på i mailen hedder "amazonvideos.org", og det stemmer ikke overens med det virkelige domæne, som er "primevideo.com".

Nogle hackere skjuler en falsk hjemmeside bag et link, der ligner det korrekte domæne. Du kan nemt tjekke, om et link er legitimt ved at kopiere linket til udlipsholderen og efterfølgende indsætte det i sikkerhedsfirmaets TrendMicros værktøj til at scanne hjemmesider. Find værktøjet her: **komputer.dk/linktjek**

Sproget er mærkeligt

Selv om kunstig intelligens gør det lettere at skjule svindel, er mange svindelmails præget af et sprog, der ikke ligner det, vi bruger til daglig. Svindlere forsøger som regel at snyde alle uanset nationalitet, og derfor er oversættelserne ofte mangelfulde.

Vær derfor skeptisk, hvis en mail indeholder sprogfejl eller formuleringer, der virker mærkelige.

(!) Dit abonnement ophæves

Hej Martin

Din betaling blev afvist, da din kortudsteder ikke kunne validere din betalingsmetode (Visa****). Klik for flere oplysninger om afviste betalinger

Opdater din betalings metode, så at dit abonnement (Google One) forbliver.

OPDATER KORTBETALING

Usædvanlige ordvalg og stavefejl er tydelige tegn på, at svindlere står bag en mail.

Du vil nødig gå glip af pakken

En af de mest udbredte svindelmails handler om en pakkelevering, der angiveligt er gået galt. Mailen, der også ofte sendes som sms, kommer som regel uventet og indeholder et link, du skal klikke på for at "rette op på fejlen".

Mailen kan fx påstå, at der er problemer med modtageradressen, eller at der er opkrævet uventet told på pakken, som skal betales via et link. Hvis du ikke reagerer, risikerer du ifølge mailen, at pakken ikke bliver leveret.

Får du en mail af den type, bør du altid først tjekke, om du rent faktisk har bestilt noget for nylig til levering med det fragtfirma, der angiveligt er afsenderen af mailen.

[Postoplysninger]:

Din vare er ankommet til leveringsstationen, men den kan ikke leveres, fordi den ydre emballageinformation er uklar.

Klik venligst på linket nu: http://is.gd/8yequFC?psg=olbjqei

Vi sender igen, så snart oplysningerne er opdateret.

Tak

DHL

Klik aldrig på linket. I stedet bør du tage kontakt til fragtfirmaet via den officielle hjemmeside og få opklaret, hvad der er sket.

Avast

WARNING

HØJ RISIKO REGISTRERET

Advarsel: Der er registreret skadelig aktivitet på din pc.

Alvorlighed: Høj
Tidspunkt: 12:42 - 10/03/2025
Aktivitet: Beskyttelse
Detaljer: Et uautoriseret login på Windows tilhørende: Martin Lorentsen

Tak,
Avast

I stedet for at blive beskyttet bliver pc'en inficeret, hvis du gør, som mailen beder dig om.

Antivirusprogrammet sender dig advarsler over mail

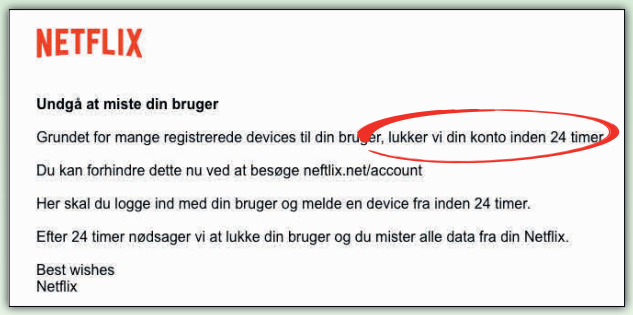
Medmindre du har tilmeldt dig et nyhedsbrev, hører du sjældent fra dit antivirusprogram via e-mail, og især ikke om trusler på din computer. Den slags advarsler vises direkte på din pc.

Hvis du modtager en mail, der påstår at komme fra dit antivirusprogram, kan du trygt slette den. Åbn i stedet antivirusprogrammet direkte på din computer og foretag en scanning.

Mailen forsøger at stresse dig med en panisk tone

Mange af os træffer forhastede beslutninger, når vi er i panik. Derfor har svindelmails ofte en lettere alarmistisk tone. De kan fx hævde, at du risikerer at miste adgangen til en brugerkonto, hvis du ikke følger instruktionerne i mailen. Mailen vil typisk indeholde et link til en falsk hjemmeside, der ligner den officielle. Hvis du indtaster dine loginoplysninger dér, overgiver du dem til hackerne.

Er du i tvivl, kan du altid tjekke din konto til den tjeneste, mailen omtaler, ved at besøge virksomhedens officielle hjemmeside eller åbne den tilhørende app og logge ind for at se, om alt er, som det skal være.



NETFLIX

Undgå at miste din bruger

Grundet for mange registrerede devices til din bruger, lukker vi din konto inden 24 timer.

Du kan forhindre dette nu ved at besøge neftlix.net/account

Her skal du logge ind med din bruger og melde en device fra inden 24 timer.

Efter 24 timer nødsager vi at lukke din bruger og du mister alle data fra din Netflix.

Best wishes
Netflix

Du får at vide, at noget er gået galt med din konto, og at du skal skynde dig at lave ændringer inden for en tidsramme.

CONGRATS!
YOU'VE WON!

Hej, Martin

Tillykke! Du har vundet hovedpræmien MacBook Air i vores "Anniversay Giveaway" konkurrence.

Her ser du, hvordan du gør krav på din præmie:

1. Send en e-mail til jordanstarr@applecontestwin.com og bekræft, at du har vundet.
2. Venligst bekræft, at det er OK, at vi offentliggør dit fornavn på vores sociale medier og hjemmeside.
3. Dette er valgtfrit, men hvis du er lige så glad for at vinde, som vi er, så tag en selfie og send den til os.

Hvis du har spørgsmål, skal du bare svare på denne mail, og jeg vil være glad for at hjælpe.

De bedste hilsner fra Jordan

Modtager du ude af det blå en mail om, at du har vundet en konkurrence, er det desværre næppe en oprigtig mail.

Du skal bare lige bekræfte noget

Det er altid rart at modtage gode nyheder, fx at du har arvet en masse penge fra en ukendt fjern slægtning eller vundet en stor præmie. Den eneste hage er, at du lige skal bekræfte noget, før du kan få din gevinst.

Ifølge afsenderen kan det gøres hurtigt og nemt, men desværre er det ofte svindlere, der står bag sådanne mails. Når du tror, du bekræfter modtagelsen af en præmie, kan du i stedet give svindlerne adgang til dine personlige oplysninger og dermed ende i store problemer.

Får du en mail af denne type, bør du tjekke, om du har deltaget i den nævnte konkurrence. Tag eventuelt kontakt til afsender, men uden at klikke på noget her.