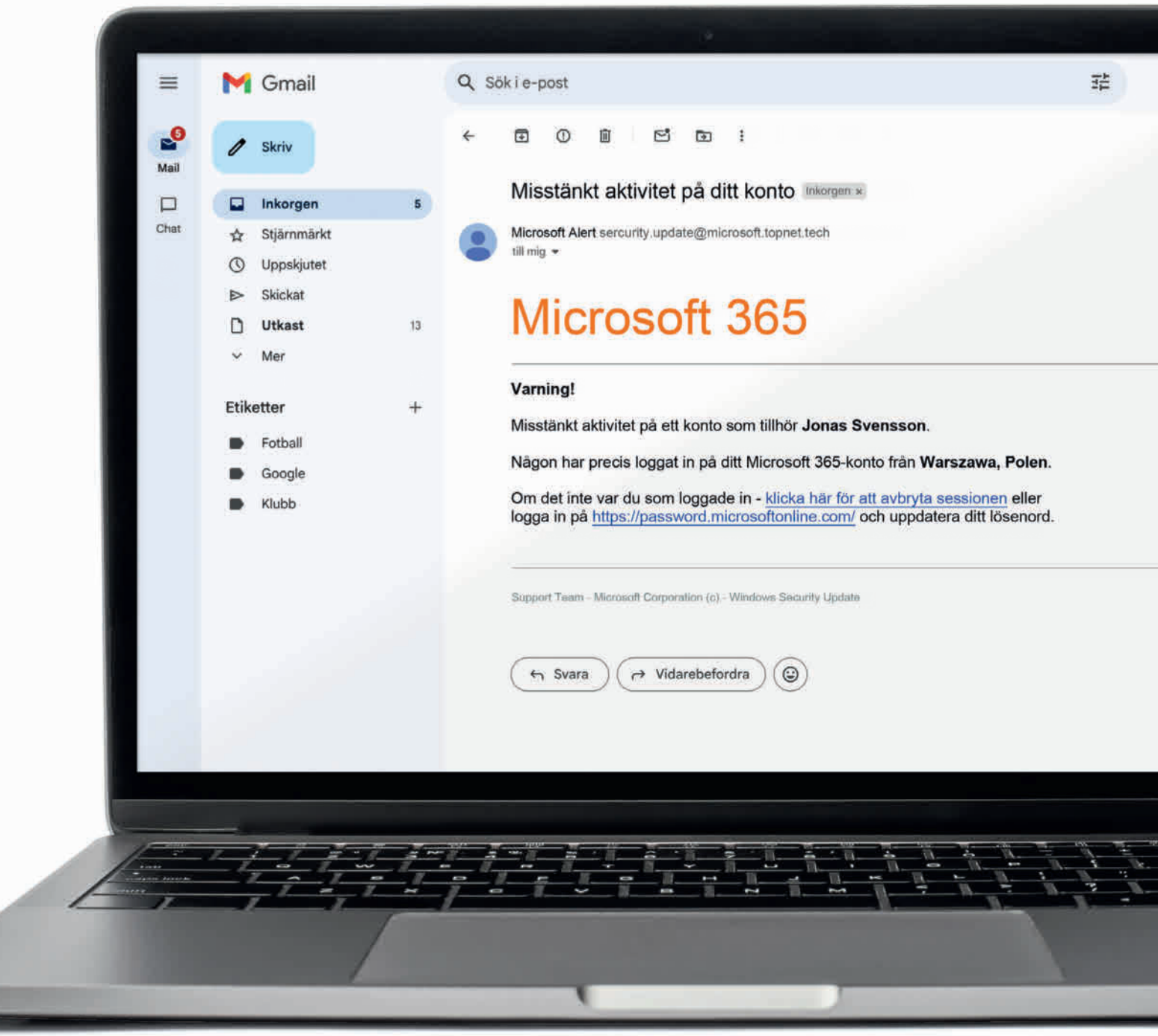
Vad avslöjar att det här mejlet är farligt?



SVAR: Avsändaren ser märklig ut

På skärmen ser du ett exempel på hur ett mejl som påstås komma från Microsoft om misstänkt aktivitet kan se ut. I själva verket är mejlet från en bedragare, och du kan upptäcka det genom att titta närmare på avsändaradressen. Den är lång och invecklad och har inte den adresstandard som man kan förvänta sig av ett jätteföretag som Microsoft.

SVAR: Logotypen är fel

Ett annat tecken på att det här mejlet kommer från bedragare och inte från Microsoft är att Microsoft 365-grafiken inte stämmer överens med den riktiga grafiken. För det första är färgen på teckensnittet inte den som Microsoft använder i sin marknadsföring, och för det andra skulle texten ”Microsoft 365” ha den välkända Microsoft-logotypen till vänster om texten.

Foto: Random435/Shutterstock.com

SÅ UPPTÄCKER DU BEDRÄGERIER I TID

10 säkra tecken på ett farligt mejl

Hackare skickar bluffmejl som aldrig förr, så det är viktigt att du vet vilka tecken du ska vara uppmärksam på när du får ett misstänkt mejl.

Journalist
Martin Lorentsen

Det dyker upp ett mejl i din inkorg som ser ut att komma från en budfirma. I mejlet står det att du har ett paket som är på väg, men att det finns ett litet problem: det kan inte levereras om du inte betalar en liten summa.

Mejlet kan verka väldigt trovärdigt och du kanske känner att du borde svara, men den här typen av mejl är näst intill alltid en bluff. Det handlar om bedragare som med hjälp av nätfiske försöker lägga beslag på känsliga personuppgifter som betalningsuppgifter, ditt personnummer eller lösenord till dina konton på internet. Och allt fler av den här typen av mejl dyker upp i våra inkorgar. Det uppskattas att 1,2 procent av alla mejl som skickas över hela världen är den här typen av nätfiskeattacker.

Nätfiske kan stå dig dyrt

Om du råkar falla i en av de många fällor som hackare gillrar riskerar du först och främst att installera skadlig programkod på datorn, vilket kan resultera i att du förlorar dina filer senare. Du kan också drabbas av betydligt större problem, som att få din identitet stulen eller till och med förlora hela ditt sparkapital om hackarna lyckas lura dig att lämna ut dina känsliga personuppgifter.

Hackare döljer bedrägerier bättre

Vissa bluffmejl är mer uppenbara än andra, men den tekniska utvecklingen gör att det blir allt svårare att avgöra vad som är bluff och vad som är legitimt.

I början av 2025 var Google tvungna att gå ut med en varning till sina Gmail-användare om att 2,5 miljarder konton blivit måltavlor för hackare som använde artificiell intelligens för att göra sina bedrägerier mer trovärdiga.

Lyckligtvis är inte alla hackare lika listiga. Det är inte omöjligt att upptäcka när ett mejl är en bluff, men du måste veta vilka tecken du ska hålla utkik efter för att minimera risken att bli lurad.

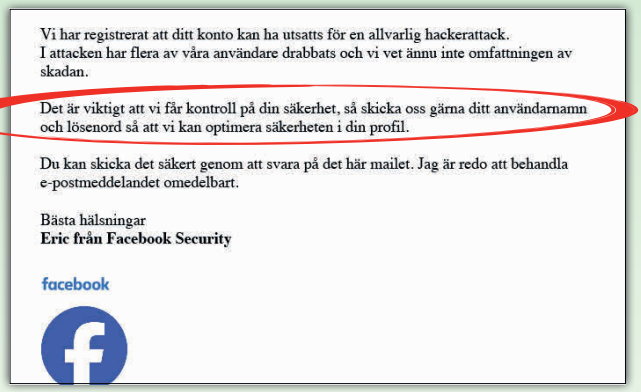
Många tecken känns igen i mobilen

Nätfiske sker inte bara via mejl utan även via sms på mobilen, ett fenomen som kallas ”smishing”. Precis som med mejl försöker bedragarna lura dig att trycka på länkar, öppna bilagor eller lämna ut olika person-uppgifter. Många av de varningssignaler som gäller för mejl bör du också hålla utkik efter i din sms-inkorg.

Mejlet ber dig att lämna ut känslig information

Det spelar ingen roll hur korrekt språket i ett mejl är och hur trovärdigt det ser ut, ska du aldrig skriva känslig information som lösenord i ett mejl. Det gäller särskilt mejl från en avsändare som ber dig att göra det utan föregående dialog.

Företag som Facebook eller Netflix, din bank eller myndigheter kommer aldrig att be dig att lämna ut dina uppgifter via ett vanligt mejl.


Vi har registrerat att ditt konto kan ha utsatts för en allvarlig hackerattack.
I attacken har flera av våra användare drabbats och vi vet ännu inte omfattningen av skadan.

Det är viktigt att vi får kontroll på din säkerhet, så skicka oss gärna ditt användarnamn och lösenord så att vi kan optimera säkerheten i din profil.

Du kan skicka det säkert genom att svara på det här mailet. Jag är redo att behandla e-postmeddelandet omedelbart.

Bästa hälsningar
Eric från Facebook Security

facebook

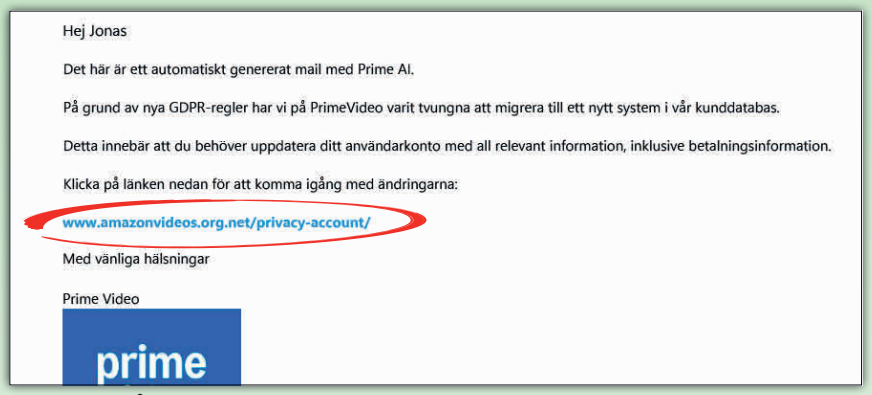
Om du blir ombedd att skicka ditt lösenord bör dina varningsklockor ringa. Ett legitimt företag skulle aldrig be om det.

Vanligtvis är det en falsk faktura som bedragare uppmanar dig att öppna så att du kan betala vad du är skyldig.

Se upp med bifogade filer

Om du får ett mejl där du uppmanas att öppna en fil som har bifogats kan det vara en bedragare som är i farten. Det är inte ovanligt att hackare gömmer virus och skadlig kod även i de vanligaste filtyperna, till exempel PDF-filer, som vanligtvis används för fakturor eller avtal.

Om du öppnar bilagan på din dator riskerar du att aktivera dold programkod som infekterar datorn med skadliga program. Det kan vara ransomware som låser dina filer och kräver betalning för att låsa upp dem, eller spionprogram som övervakar vad du gör.


Hej Jonas

Det här är ett automatiskt genererat mail med Prime AI.

På grund av nya GDPR-regler har vi på PrimeVideo varit tvungna att migrera till ett nytt system i vår kunddatabas.

Detta innebär att du behöver uppdatera ditt användarkonto med all relevant information, inklusive betalningsinformation.

Klicka på länken nedan för att komma igång med ändringarna:

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

Med vänliga hälsningar

Prime Video

prime

Länken är lång och stämmer inte överens med avsändarens domän.

Länken i mejlet matchar inte domänen

Länkar och mejladresser i mejl från bedragare använder sig ofta av konstiga domäner som inte stämmer överens med det företag eller den organisation som bedragarna utger sig för att representera.

I exemplet ovan har bedragaren försökt utge sig för att komma från streamingtjänsten Prime Video. Länken, eller URL:en, som du uppmanas att klicka på i mejlet är dock ”amazonvideos.org.net”, vilket inte stämmer överens med den riktiga domänen som är ”primevideo.com”.

Hackare kan lägga en falsk webbplats som ser ut som den äkta varan bakom länken. Du kan testa om en länk är legitim genom att kopiera länken och klistra in den i säkerhetsföretaget TrendMicros verktyg för webbplatsgranskning. Du hittar det här: **pctidningen.se/lankkoll**

Språket är märkligt

Även om artificiell intelligens gör det lättare att dölja bedrägerier kännetecknas många bluffmejl av ett språk som inte liknar det vi använder till vardags. Bedragare försöker oftast lura alla oavsett nationalitet och översättningar blir därför ofta felaktiga.

Var därför skeptisk om ett mejl innehåller språkliga fel eller har formuleringar som verkar konstiga.

Konstiga ordval och stavfel är tydliga tecken på att det är bedragare som ligger bakom ett mejl.

Du vill inte gå miste om paketet

Ett av de vanligaste bluffmejlen handlar om en leverans av ett paket som påstås ha gått fel. Mejlet, som också ofta skickas som ett sms, kommer oftast oväntat och innehåller en länk att klicka på för att ”åtgärda felet”.

Mejlet kan till exempel påstå att det är något problem med mottagaradressen eller att oväntade tullavgifter har tagits ut på paketet, som måste betalas via en länk. Om du inte svarar riskerar du, enligt mejlet, att paketet inte levereras.

Om du får ett sådant här mejl bör du alltid först kontrollera om du faktiskt har beställt något nyligen för leverans med det fraktbolag som påstås vara avsändare av mejlet.


[Postens information]:

Din försändelse har anlänt till utlämningsstället, men den kan inte levereras eftersom informationen om förpackningen är oklar.

Vänligen klicka på länken nu: http://is.gd/8yequFC?psg=olbjqei

Vi skickar igen så snart informationen har uppdaterats.

Tack

DHL

Klicka aldrig på länken. Kontakta istället fraktbolaget via deras officiella hemsida och ta reda på vad som hänt.


Avast

WARNING

STOR RISK UPPTÄCKT

Varning: Skadlig aktivitet har upptäckts på din dator.

Allvarlighetsgrad: Hög
Tid: 12:42 - 10/03/2025
Aktivitet: Skydd
Detaljer: En obehörig inloggning på Windows tillhörande: Jonas Svensson

Tack,
Avast

Istället för att skyddas blir din dator infekterad om du gör det som mejlet ber dig att göra.

Antivirusprogrammet skickar varningar via mejl

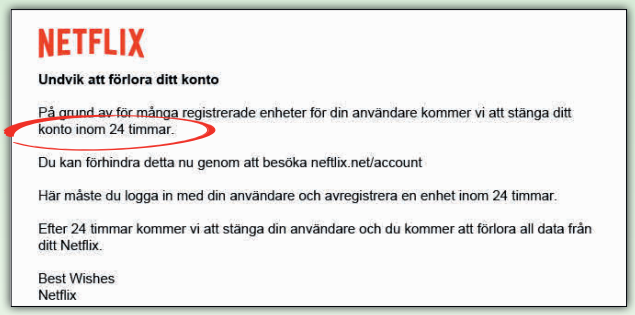
Om du inte har registrerat dig för ett nyhetsbrev hör du sällan något från ditt antivirusprogram via mejl, och särskilt inte om hot på din dator. Den typen av varningar visas direkt på din dator.

Om du får ett mejl som påstår sig komma från ditt antivirusprogram kan du lugnt radera det. Öppna istället antivirusprogrammet direkt på din dator och kör en genomsökning.

Mejlet försöker stressa dig med en panikartad ton

Vi fattar förhastade beslut när vi är stressade. Det är därför bluffmejl ofta har en lite alarmistisk ton. De kan till exempel hävda att du förlorar ett användarkonto om du inte följer instruktionerna i mejlet, som vanligtvis innehåller en länk till en falsk webbplats som ser ut som den officiella. Om du matar in dina inloggningsuppgifter där överlämnar du dem till hackarna.

Om du är osäker kan du alltid kontrollera ditt konto för den tjänst som nämns i mejlet genom att besöka företagets officiella webbplats eller öppna motsvarande app och logga in för att se om allt är som det ska.


NETFLIX

Undvik att förlora ditt konto

På grund av för många registrerade enheter för din användare kommer vi att stänga ditt konto inom 24 timmar.

Du kan förhindra detta nu genom att besöka neftlix.net/account

Här måste du logga in med din användare och avregistrera en enhet inom 24 timmar.

Efter 24 timmar kommer vi att stänga din användare och du kommer att förlora all data från ditt Netflix.

Best Wishes
Netflix

Du får veta att något har gått fel med ditt konto och att du måste skynda dig att göra ändringar inom en viss tidsram.


CONGRATS!
YOU'VE WON!

Hej Jonas

Grattis! Du har vunnit huvudvinsten som är en MacBook Air i vår tävling "Anniversay Giveaway".

Så här gör du för att göra anspråk på ditt pris:

1. Skicka ett e-mail till jordanstarr@applecontestwin.com och bekräfta att du har vunnit.
2. Bekräfta att det är OK för oss att publicera ditt förnamn på våra sociala medier och på vår webbplats.
3. Detta är valfritt, men om du är lika glad över att vinna som vi är, ta en selfie och skicka den till oss.

Om du har några frågor är det bara att svara på det här mejlet så hjälper jag gärna till.

Bästa hälsningar från Jordan

Om du plötsligt får ett mejl där det står att du har vunnit en tävling är det tyvärr knappast ett äkta mejl.

Du behöver bara bekräfta något

Det är alltid trevligt att få goda nyheter, till exempel att man ärver en massa pengar från en okänd släkting eller vinner något stort. Det enda du behöver göra är att bekräfta något innan du kan göra anspråk på ditt pris.

Enligt avsändaren kan det göras snabbt och enkelt, men tyvärr är det ofta bedragare som ligger bakom sådana mejl. När du tror att du bekräftar mottagandet av ett pris kan du ge bedragare tillgång till personlig information och hamna i stora problem.

Om du får ett mejl av den här typen bör du kontrollera om du har deltagit i tävlingen. Kontakta avsändaren om det behövs, men utan att klicka på något här.