Hvordan håndtere misbruk, phishing eller forfalsking i Outlook.com

*Outlook.com*

***Obs!:****Vi ønsker å gi deg det nyeste hjelpeinnholdet så raskt som mulig, på ditt eget språk. Denne siden er oversatt gjennom automatisering og kan inneholde grammatiske feil eller unøyaktigheter. Formålet vårt er at innholdet skal være nyttig for deg. Kan du fortelle oss om informasjonen var nyttig for deg nederst på denne siden?*[*Her er den engelske artikkelen*](https://support.office.com/en-us/article/0d882ea5-eedc-4bed-aebc-079ffa1105a3)*for enkel referanse.*

En phishingsvindel er en e-postmelding som ser ekte ut, men som egentlig er et forsøk på å få tak i personlige opplysninger eller stjele penger. Svindlerne kan også bruke en teknikk som kalles forfalsking («spoofing»), slik at det ser ut til at du har mottatt en e-postmelding fra deg selv.

Slik håndterer du misbruk, svindelforsøk, phishing og forfalsking på nettet samt søppelpost sendt til eller fra Outlook.com-kontoer.

Velg din versjon for å få instruksjoner

Instruksjonene er litt forskjellige avhengig av om du bruker betaversjonen av Outlook.com eller ikke. Du kan velge hvilken versjon av Outlook.com du bruker for å se instruksjonene som gjelder for deg.

|  |  |
| --- | --- |
| HVIS POSTBOKSEN SER SLIK UT ... | HVIS POSTBOKSEN SER SLIK UT ... |
| Et skjermbilde av øvre, venstre hjørne av beta-postboksen i Outlook.comSe [Instruksjoner for betaversjonen av Outlook.com](https://support.office.com/nb-no/article/h%C3%A5ndtere-misbruk-phishing-eller-forfalsking-i-outlook-com-0d882ea5-eedc-4bed-aebc-079ffa1105a3#bkmk_beta) | Et skjermbilde av øvre, venstre hjørne av den klassiske postboksen i Outlook.comSe [Instruksjoner for den klassiske versjonen av Outlook.com](https://support.office.com/nb-no/article/h%C3%A5ndtere-misbruk-phishing-eller-forfalsking-i-outlook-com-0d882ea5-eedc-4bed-aebc-079ffa1105a3#bkmk_classic) |

Instruksjoner for betaversjonen av Outlook.com

Rapportere phishing eller forfalskning/svindel

Hvis du mener du har blitt forsøkt svindlet med phishing eller forfalsking, må du først merke e-postmeldingen som søppelpost, og deretter merke den som phishing-svindel.

**Viktig!:** Når en melding er merket som en phishingsvindel, viser Outlook.com en advarsel øverst på siden, men du kan fortsatt åpne eventuelle koblinger i meldingen.

1. Velg meldingen du vil merke som phishing-svindel, og velg **Søppelpost** på kommandolinjen.



Du kan også høyreklikke på meldingen og velge **Marker som søppelpost**.

1. Velg Søppelpost-mappen, og velg deretter **ikke søppelpost** > **Phishing** for å rapportere avsenderen.



**Obs!:**

* + *Når du har merket en melding som phishing, rapporteres bare avsenderen. Avsenderen markeres ikke fra å sende deg meldinger i fremtiden. Hvis du vil blokkere avsenderen, må du legge til avsenderen i listen over blokkerte avsendere. For mer informasjon, kan du se*[*blokkerer avsendere eller oppheve blokkeringen av avsendere i Outlook.com*](https://support.office.com/nb-no/article/blokker-eller-fjern-blokkering-av-sendere-i-outlook-com-afba1c94-77bb-4f50-8b85-057cf52f4d5e)*.*
	+ *Du kan også rapportere phishing ved å videresende e-postmeldingen som et vedlegg til*[*phish@office365.microsoft.com*](https://go.microsoft.com/fwlink/?linkid=2003947)*.*

Instruksjoner for standardversjonen av Outlook.com

Rapportere phishing eller forfalskning/svindel

Hvis du mener du har blitt forsøkt svindlet med phishing eller forfalsking, rapporterer du e-postmeldingen ved å velge pilen ved siden av **Søppelpost** og deretter velge ett av følgende alternativer.

**Viktig!:** Når en melding er merket som en phishingsvindel, viser Outlook.com en advarsel øverst på siden, men du kan fortsatt åpne eventuelle koblinger i meldingen.



* **Søppelpost** Bruk dette alternativet for rutinemessig uønskede e-postmeldinger.
* **Phishingsvindel** Bruk dette alternativet for e-postmeldinger som prøver å lure deg til å oppgi personlige opplysninger, for eksempel passord, bankkontoinformasjon eller personnummer.

**Obs!:**

* + *Når du har merket en melding som phishing, rapporteres bare avsenderen. Avsenderen markeres ikke fra å sende deg meldinger i fremtiden. Hvis du vil blokkere avsenderen, må du legge til avsenderen i listen over blokkerte avsendere. For mer informasjon, kan du se*[*blokkerer avsendere eller oppheve blokkeringen av avsendere i Outlook.com*](https://support.office.com/nb-no/article/blokker-eller-fjern-blokkering-av-sendere-i-outlook-com-afba1c94-77bb-4f50-8b85-057cf52f4d5e)*.*
	+ *Du kan også rapportere phishing ved å videresende e-postmeldingen som et vedlegg til*[*phish@office365.microsoft.com*](https://go.microsoft.com/fwlink/?linkid=2003947)*.*
* ***Vennen min har blitt hacket****Bruk dette alternativet hvis du har begynt å motta søppelpost eller forsøk på phishing-svindel fra en avsender du vanligvis stoler på.*

Flere måter å håndtere misbruk, phishing eller forfalsking på

Beskyttelse mot phishingsvindel

En phishingsvindel er en e-postmelding som ser ekte ut, men som egentlig er et forsøk på å få tak i personlige opplysninger eller stjele penger.

* Aldri svar på en e-postmelding som ber deg om å sende personlige opplysninger eller kontoinformasjonen.
* Hvis du mottar en e-postmelding som ser mistenkelig ut eller som ber deg om denne typen informasjon, må aldri klikke på koblinger som gir seg ut for å være koblinger til et firmanettsted.
* Aldri åpne vedlegg inkludert i mistenkelige e-postmeldinger.
* Hvis e-postmeldingen ser ut til å komme fra et selskap, kan du kontakte selskapets kundestøtte via telefon eller en nettleser for å se om e-postmeldingen er legitim.
* Søk etter e-postens emnelinjen på nettet, etterfulgt av ordet «hoax», for å se om andre har rapportert denne svindelen.

Fem vanlige typer nettsvindel

Her er noen av de vanligste typene nettsvindel, sammen med flere tips om hvordan du gjenkjenner dem.

***«Bekreft kontoen din nå, ellers stenger vi den!»***

***«En stor sum penger kan bli din, bare send din personlige informasjon eller kontanter.»***

***«Du er vår store vinner!»***

***«Hjelp! Jeg er strandet!»***

***«Hvis du (ikke) videresender denne e-postmeldingen, vil noe godt (dårlig) skje med deg!»***

Gjenopprette kontoen når den er blitt hacket

Hvis noen har hacket/kommet seg inn i kontoen din i Outlook.com, eller du har en e-postbekreftelse for endring av passord du ikke har godkjent, kan du gjenopprette kontoen din. For mer informasjon, kan du se [Min Outlook.com-kontoen har blitt Hacket](https://support.office.com/nb-no/article/outlook-com-kontoen-min-har-blitt-hacket-35993ac5-ac2f-494e-aacb-5232dda453d8).

Rapportere misbruk

* Hvis du utsettes for trusler, må du ringe lokale politimyndigheter.
* Hvis du vil rapportere sjikane, representasjon, barnemisbruk, barnepornografi eller andre ulovlige aktiviteter mottatt via en Outlook.com-konto, videresender du den støtende e-postmeldingen som et vedlegg til abuse@outlook.com. Inkluder all relevant informasjon, for eksempel hvor mange ganger du har mottatt meldinger fra kontoen og tilknytningen, hvis det er en tilknytning mellom deg og avsenderen.

**Obs!:** Hvis du vil lære hvordan du legger til en melding som et vedlegg, kan du se [legge ved en e-postmelding til en annen e-posten](https://support.office.com/nb-no/article/legge-ved-filer-i-outlook-com-8d7c1ea7-4e5f-44ce-bb6e-c5fcc92ba9ab#bkmk_attachmessagetomessage).

* Hvis du vil rapportere misbruk mottatt fra en ikke -Outlook.com-konto, kan du gå til [https://www.abuse.net](https://go.microsoft.com/fwlink/p/?linkid=859121) til å identifisere adressen for rapportering av riktig misbruk.