# Helpdeskfraude

Version PDF

## Wat is Helpdeskfraude?

U ontvangt een bericht waaruit blijkt dat u te kampen heeft met een probleem met een bepaalde dienst (bv. Microsoft, een bankinstelling, enz.) en u wordt verzocht bepaalde verrichtingen uit te voeren via de ondersteuningsdienst/klantendienst/helpdesk van deze dienstverlener.

Uw computer lijkt vast te zitten op een webbrowserpagina die suggereert dat hij met een virus is geïnfecteerd.

Soms begint dit soort oplichting met een klik op een advertentie of een link, meestal op websites die op het randje van legaal (downloadsites, streamingsites) of pornografisch zijn. De internetbrowser opent dan een venster met een bericht dat suggereert dat een virus zojuist uw computer heeft geïnfecteerd.

Het venster ziet er vaak uit als een blauw scherm van Windows of een typische Microsoft-pagina.

Je kunt de browservensters niet meer sluiten en dat kan je afschrikken.

Een bericht nodigt u uit om dringend contact op te nemen met een telefoonnummer.

Aan de telefoon biedt een nep-technicus aan om de controle over het computersysteem over te nemen:

- via een softwaredownload of via een webinterface door een login en wachtwoord in te voeren;

- door met een creditcard te betalen. De aangerekende prijs varieert tussen 100 en 200 €.

## Wat heb je nodig om klacht neer te leggen?

- Exacte URL van de bezochte website;
- Exacte datum en tijd van het incident;
- Exacte URL (adres) van de zogenaamde "helpdesk"-pagina;
- Uw e-mailadres;
- E-mailadres gebruikt door de verdachte;
- Datum en tijdstip van gesprek(ken) met de verdachte;
- Gedetailleerde beschrijving van de inhoud van het gesprek en de acties die op verzoek van de verdachte(n) zijn ondernomen.
- Inhoud van de met de verdachte uitgewisselde e-mails (bij te voegen) + volledige header;
- URL's van alle links in de verdachte e-mail, indien aanwezig;
- Het telefoonnummer van de verdachte;
- Mogelijke opnames van telefoongesprekken;
- Indien het oproepnummer niet bekend is: noteer de tijd, het oproepnummer waarop u werd gecontacteerd;
- Informatie over de betaling die u hebt verricht of had moeten verrichten

## Wat kan je nog doen?

- Verbreek onmiddellijk de verbinding met het internet.
- Als de verdachte de controle over uw apparaat heeft kunnen overnemen, kan het aangewezen zijn om het systeem opnieuw te installeren.
- Wijzig de wachtwoorden en beveiligingsvragen van uw account.

  In de meeste gevallen is de machine, in tegenstelling tot wat het lijkt, niet vergrendeld of geïnfecteerd.
  Het is louter een pop-up venster.

  Om de controle terug te krijgen, klikt u gewoon op de knop OK of de knop Sluiten (X) op het pop-upvenster dat verschijnt, soms herhaaldelijk, of dwingt u de browser te sluiten via Taakbeheer (Ctrl-Alt-Delete).

# Hoe vermijd je om opnieuw slachtoffer te worden?

- Als u twijfelt, ga dan niet in op telefoontjes van zogenaamde helpdesks.
- Wees kritisch over e-mails en telefoontjes die je krijgt
- Als het adres of de boodschap van de beller vreemd lijkt, als de beller in een andere taal spreekt of als hij aandringt op negatieve gevolgen als u niet reageert, is het waarschijnlijk oplichterij.
- Klik nooit op links die u onder deze omstandigheden worden toegestuurd.
- Geef uw persoonlijke gegevens niet per e-mail of telefoon (codes, paswoorden, klantnummer, bankgegevens, enz.).
- Als u een betaling doet met uw bankkaart, bel dan onmiddellijk Card Stop op 070 344 344 om uw kaart te laten blokkeren.
- Neem in geval van twijfel zelf contact op met het bedrijf waarvoor uw contactpersoon zegt te werken.

# Waar vind je meer informatie?

https://www.besafe.be/nl/veiligheidsthemas/cyberveiligheid/cybercriminaliteit

---

**Cybercriminalité | Besafe**

www.besafe.be

On parle de sabotage informatique pour désigner le fait de, sans y être autorisé, introduire, modifier ou effacer des données dans un système informatique ou modifier par un moyen technologique l'utilisation normale de données dans un système informa...

---