

# E-MAIL VERSLEUTELLEN

PGP KEY

## INHOUDSOPGAVE

Beleid voor responsible disclosure.....	1
E-mail versleutelen met PGP key .....	2
Download & install GPG4win .....	2
Verstuur bevindingen via Outlook .....	2

### Uitgangspunten

Wij beschouwen de veiligheid van onze systemen als een topprioriteit, maar hoeveel moeite we ook steken in systeembeveiliging, er kunnen nog steeds kwetsbaarheden aanwezig zijn.

Als u een kwetsbaarheid ontdekt in onze systemen, willen we dat graag weten, zodat we maatregelen kunnen nemen om deze zo snel mogelijk te verhelpen. We willen u vragen om ons te helpen onze klanten en onze systemen beter te beschermen.

Doe a.u.b. het volgende:

- E-mail uw bevindingen naar [security@vhict.nl](mailto:security@vhict.nl). Versleutel uw bevindingen met onze PGP-sleutel om te voorkomen dat deze kritieke informatie in verkeerde handen valt.
- Maak geen gebruik van de kwetsbaarheid of het probleem dat u heeft ontdekt, bijvoorbeeld door:
  - Meer gegevens te downloaden dan nodig is om de kwetsbaarheid aan te tonen.
  - Door gegevens van anderen te verwijderen of aan te passen.
  - Het plaatsen van gegevens.
  - Het plaatsen van malware.
- Vertel het probleem niet aan anderen voordat het is opgelost.
- Voer geen aanvallen uit met behulp van:
  - Social engineering.
  - (Gedistribueerde) denial of service.
  - Brute force aanvallen.
  - Spam.
- Geef voldoende informatie om het probleem te reproduceren, zodat we het zo snel mogelijk kunnen oplossen. Meestal zijn het IP-adres of de URL van het getroffen systeem en een beschrijving van de kwetsbaarheid voldoende, maar bij complexe kwetsbaarheden is wellicht meer uitleg nodig.

Wat we beloven:

- We zullen binnen 3 werkdagen op uw melding reageren met onze evaluatie van de melding en een verwachte datum voor een oplossing.
- Als u bovenstaande instructies heeft opgevolgd, zullen we geen juridische stappen tegen u ondernemen met betrekking tot de melding.
- Wij behandelen uw melding strikt vertrouwelijk en geven uw persoonlijke gegevens niet zonder uw toestemming door aan derden.
- We houden u op de hoogte van de voortgang bij het oplossen van het probleem.
- In de openbare informatie over het gemelde probleem vermelden we uw naam als de ontdekker van het probleem (tenzij u anders wenst).
- Als blijk van dank voor uw hulp bieden wij een beloning aan voor elke melding van een beveiligingsprobleem waarvan wij nog niet op de hoogte waren. De hoogte van de beloning wordt bepaald op basis van de ernst van het lek en de kwaliteit van de melding. De minimale beloning is een cadeaubon van € 50.

We streven ernaar om alle problemen zo snel mogelijk op te lossen en we willen graag een actieve rol spelen in de uiteindelijke publicatie over het probleem nadat het is opgelost.

## E-MAIL VERSLEUTELLEN MET PGP KEY

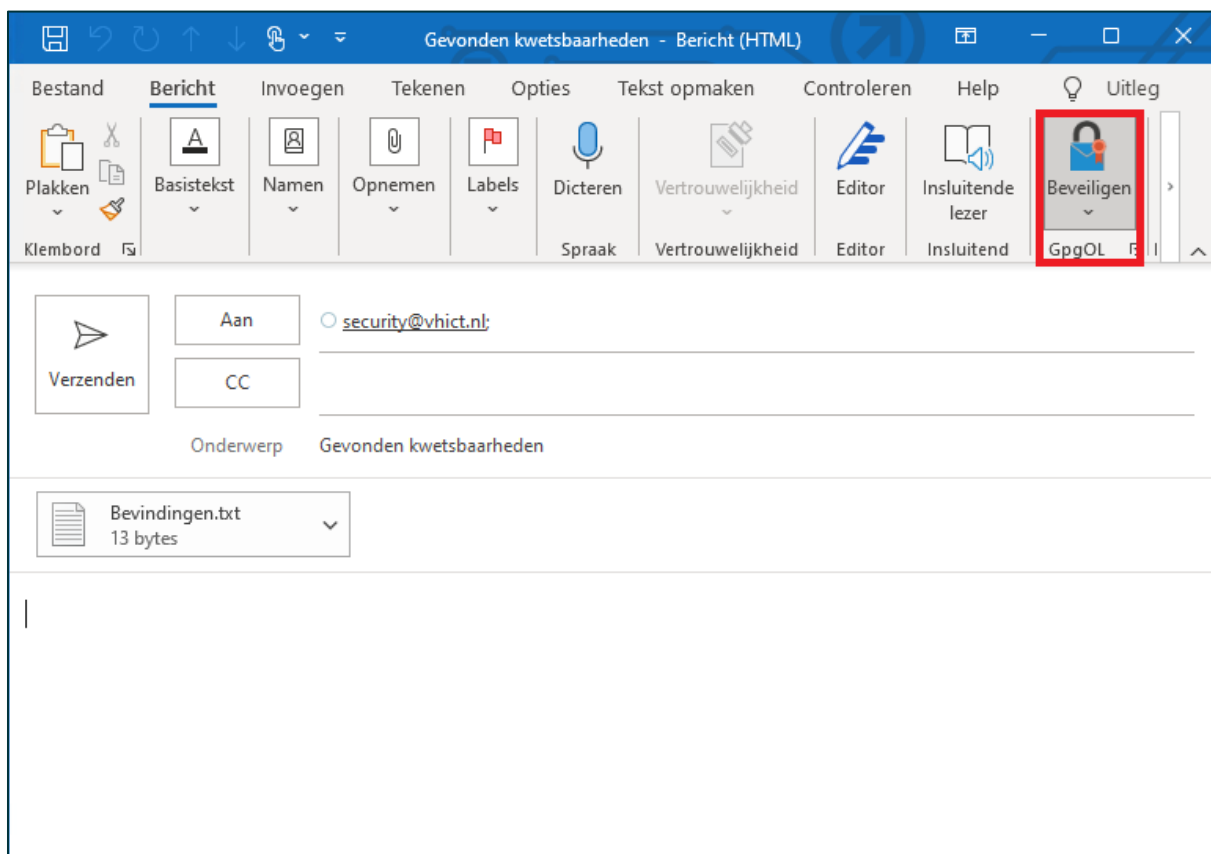
Hieronder staat één van de mogelijke tools Gpg4win (GNU Privacy Guard for Windows) beschreven om uw bevindingen veilig per e-mail te versturen.

## DOWNLOAD & INSTALL GPG4WIN


- Download en installeer de tool via: <https://gpg4win.org>
- Importeer het public certificaat te vinden in deze zipfile.
- Controleer het e-mailadres en de geldigheidsduur van het certificaat.

## VERSTUUR BEVINDINGEN VIA OUTLOOK



- Maak een nieuwe e-mail met uw bevindingen.
- Zorg ervoor dat beveiligen via GpgOL aan staat en verzend de e-mail.





- Maak waar nodig een eigen PGP-sleutel aan en verstuur de e-mail.

 **Goedkeuring beveiliging** ✕



Identiteit  bevestigen als:

  ▼ 

Versleutelen naar uzelf  :

  ▼ 

Versleutelen naar anderen:

  ▼ 

Genereren Cancel