Aangifte e-mail account gehackt

Hulpmiddel bij aangifte

Versie juni 2024

« waakzaam en dienstbaar »

Uw e-mailaccount is gehackt, wat is dat?

Uw e-mailaccount is gehackt, wat betekent dat? Een derde heeft beschikking gekregen over uw wachtwoord en daarmee toegang verkregen tot uw e-mailaccount. U heeft bijvoorbeeld een betalingsherinnering ontvangen voor internetbestellingen die u niet heeft gedaan of zelfs berichten van een incassobureau. Uw wachtwoord van een webshop is gewijzigd en u heeft nu geen toegang meer tot deze webshop. Uw e-mailadres is gewijzigd en u ontvangt geen e-mails van geplaatste bestellingen. Uw contactpersonen ontvangen e-mails namens u die u nooit zelf heeft verzonden. Dit kunnen bijvoorbeeld e-mails zijn met betaalverzoeken.

Belangrijk preventief advies:

Wanneer een dader toegang heeft tot het e-mailaccount van een slachtoffer - bijvoorbeeld met als einddoel om cryptovaluta buit te maken – kan de dader het ***e-mailaccount blijven monitoren door het instellen van 'forward rules' ofwel 'doorstuur regels'****. Door deze regels in te stellen worden e-mails met vooraf ingestelde woorden zoals 'factuur', 'crypto', 'invoice' of de naam van een organisatie bijvoorbeeld automatisch doorgestuurd naar de oplichter. De dader kan het e-mailverkeer op deze wijze (deels) overnemen. Daders kunnen hierdoor het e-mailverkeer blijven monitoren, ook als de gebruikersnamen en/of wachtwoorden worden gewijzigd. Naast het doorsturen van e-mails met specifieke woorden kan de dader er ook voor kiezen om kopieën van al het inkomend emailverkeer af te laten leveren in de eigen mailbox. Tijdens het monitoren van het e-mailverkeer kan de aanvaller ook facetten zoals betaalactiviteiten en taalgebruik monitoren. Wanneer er verdachte inlogpogingen zijn, is* ***het goed om de e-mailbox te controleren op eventueel ingestelde 'forward rules'.*** *Controleer dan ook de map 'verwijderde items' en "archief" omdat een dader een actie kan hebben ingesteld om bepaalde berichten te laten verwijderen. Kijk hier hoe dit moet voor bijvoorbeeld Hotmail:* ***https://support.microsoft.com/nl-nl/office/regels-voor-postvak-in-in-outlook-web-app-edea3d17-00c9-434b-b9b7-26ee8d9f5622****.*

Vragen aangifte

U maakt een afspraak voor het doen van aangifte. Voordat u de afspraak heeft, is het belangrijk dat u alle benodigde gegevens al bij de hand heeft. Wilt u ter voorbereiding alvast antwoord geven op onderstaande vragen? De antwoorden vult u in onder de vraagstelling.

U dient dit document op een *computer* in te vullen. Om het document in te vullen klikt u boven in beeld op "BEELD" en vervolgens op "Document bewerken".

Gegevens aangever

- Voornaam
- Achternaam
- Geboortedatum
- Adres
- Postcode
- E-mailadres

- Telefoonnummer

- Burgerservicenummer

Algemene vragen

1. Indien bekend, op welke dag/datum/tijd heeft het misdrijf plaatsgevonden?

2. Kunt u in chronologische volgorde vertellen wat er is gebeurd? Ook alle feitelijke gegevens zoals e-mails, rekeningnummers, telefoonnummers, IP-adressen en e-mailadressen etc. moet u hier noemen. Verwijs niet naar eventuele bijlagen die u heeft, maar benoem ze hier ook.

Ontdekking

1. Op welke dag/datum/tijd heeft u het misbruik van uw e-mailaccount ontdekt?

2. Hoe heeft u dit ontdekt? Denk hierbij aan e-mails met bestelbevestigingen, facturen of brieven van incassobureaus, verzonden e-mails die u zelf niet heeft geschreven etc.

❖ Voeg alle relevante ontvangen documenten als bijlage toe bij de aangifte aan het bureau. Belangrijke feitelijke informatie dient u ook letterlijk te benoemen bij *Algemene vragen*, vraag 2.

Het account

Vermeld in de aangifte zoveel mogelijk informatie over het betreffende account.

1. Wat is het gehackte e-mailadres?

2. Heeft u al een melding gedaan bij uw e-mailprovider?

3. Zijn er e-mails namens u verzonden, die u zelf niet heeft verzonden? Indien u nog toegang heeft tot de mailaccount, kunt u dit controleren door te zoeken in de map “verzonden items” of de map “verwijderde items”. Wat zijn de e-mailadressen van de geadresseerden?

4. Wat was de inhoud van de e-mails? Voeg al uw relevante e-mails toe in de e-mailbijlage.

5. **De e-mailheaders bevatten aanvullende verborgen informatie over een e-mail en kunnen helpen om de afzender te traceren.** De website https://internetsporen.nl/is/emailheaders/ bevat hiervoor instructies. Deze stappen kunnen vaak alleen via een computer worden uitgevoerd.
   We vragen u om de e-mailheader-tekst te kopiëren en deze te plakken in de verklaring bij algemene vragen vraag 2.

6. Op welke datum en tijdstip zijn de e-mails verzonden?

7. Was er een herstel e-mailadres gekoppeld aan dit account?

   7.1 Is het herstel e-mailadres gewijzigd, maar heeft u dat niet zelf gedaan? Zo ja, vermeld dan het gewijzigde herstel e-mailadres.

8. Er is er een IP-adres bekend van de hacker of zijn er gegevens bekend van het gebruikte apparaat? Het is mogelijk dat u hier een waarschuwingsbericht van heeft ontvangen van uw mailprovider. U kunt soms zelf ook onderzoeken welke IP-adressen of apparaten er gelogd zijn. Ga hiervoor naar het onderdeel “beveiliging” in uw e-mailaccount.

9. Welk telefoonnummer was gekoppeld aan dit account?

10. Op welke wijze logt u in? (Bijvoorbeeld via de website of via de app)

11. Wat voor apparaat gebruikt u om in te loggen op het account? (Bijvoorbeeld computer, laptop, tablet, telefoon.) En vermeld ook van welk merk en type dit apparaat is.

12. Hoe is uw account beveiligd? (Bijvoorbeeld met een wachtwoord en tweestapsverificatie)

13. Indien bekend: hoe is de dader aan uw inloggegevens gekomen? Mocht dit niet duidelijk zijn, u kunt bijvoorbeeld uw wachtwoord hebben gedeeld via een link uit een phishingmail, u kunt een virus hebben gedownload of ergens slachtoffer zijn van een datalek.

De verdachte handeling(en)/bestelling(en)

Wij ontvangen graag zoveel mogelijk informatie over de handeling(en)/bestelling(en) die geplaatst zijn door de verdachte. Indien er meerdere handelingen/bestellingen zijn geplaatst, geef dan elke handeling/bestelling op:

1. Op welke webshop zijn er bestellingen geplaatst?

2. Wat was de besteldatum (en -tijdstip)?

3. Wat was het bestelnummer?

4. Is het pakket op een andere naam dan die van u besteld? Zo ja, vermeld dan de naam van de begunstigde.

5. Welke producten zijn er besteld?

6. Wat was het bestelbedrag?

7. Zijn er gegevens aangepast in uw account? Zo ja, welke?

    - Wat is de gewijzigde naam van de begunstigde?

    - Wat is het gewijzigde afleveradres?

    - Wat is het gewijzigde e-mailadres?

    - Wat is het gewijzigde telefoonnummer?

- Andere aangepaste gegevens, namelijk…

8. Indien van toepassing, wat was het afleverpunt? (Bijvoorbeeld PostNL/DHL)

9. Wat waren de pakketgegevens? (Track & trace)

10. Is de aflevering van de bestelling voltooid?

11. Indien van toepassing: hebt u de bestelling(en) kunnen annuleren of retourneren?

12. Wanneer en wat was de laatste bestelling die u zelf bij deze webshop heeft gedaan?

De betaalmethode

1. Hoe is er betaald? Zijn de bestellingen op rekening geplaatst, of is er gebruik gemaakt van een andere betaalmethode zoals PayPal, creditcard, Klarna of AfterPay?

Schade en impact

1. Wat is het totale schadebedrag?

2. Kreeg u deze schade vergoed en zo ja, van welke partij? (Bijvoorbeeld van de webshop)

3. Heeft het misbruik verdere gevolgen voor u, op welk vlak dan ook?

Slachtofferhulp

Heeft u behoefte aan slachtofferhulp of nazorg? (Zie informatie op https://www.politie.nl/informatie/ik-ben-slachtoffer-wat-nu.html)

- Deze vraag graag met **ja** of **nee** beantwoorden. Antwoord:

Bijlagen

Belangrijke feitelijke informatie dient u ook letterlijk te benoemen bij Algemene vragen, vraag 2. Voeg alle relevante bijlages bij de aangifte. Denk hierbij aan:

- □ E-mails met bestelbevestigingen
- □ Track & trace nummers
- □ Facturen of brieven van incassobureaus etc.
- □ Als u contact heeft gehad met een betrokken bedrijf/webshop, voegt u de correspondentie hiervan dan bij.
- □ Voeg al uw relevante e-mails, sms-berichten, en WhatsAppberichten toe als bijlage in de e-mail.

Voorkom misbruik van uw e-mailaccount

Om in de toekomst niet nog eens slachtoffer te worden van misbruik van uw e-mailaccount hebben wij de volgende tips voor u:

- Het misbruik vindt vaak plaats doordat criminelen proberen in te loggen met gegevens die eerder elders zijn uitgelekt.
- Onderzoek welke apparaten zijn gekoppeld aan uw account. Verwijder de apparaten die u niet bekend zijn.
- Wijzig uw wachtwoorden naar nieuwe sterke en unieke wachtwoorden. Gebruik voor wachtwoorden bijvoorbeeld een onsamenhangende zin, die alleen u weet en/of gebruik een wachtwoordmanager.
- Wijzig uw beveiligingsvragen en zorg ervoor dat het antwoord op de vragen zo uniek mogelijk is.
- Gebruik nooit hetzelfde wachtwoord voor meerdere websites.
- Stel tweestapsverificatie in voor accounts waar dit mogelijk is, door bijvoorbeeld bij het inloggen op uw account een bevestiging met de mobiele telefoon te moeten geven.
- Op de website https://haveibeenpwned.com kunt u uw e-mailadres invullen om te kijken of uw inloggegevens in het verleden gelekt zijn. Op https://scatteredsecrets.com/ kunt u zien welke van uw wachtwoorden gelekt zijn.
- Schakel opties voor achteraf betalen uit op uw webshop accounts.
- Op https://laatjeniethackmaken.nl/ vindt u nog meer tips om uzelf te beschermen tegen hackers.
- Indien van toepassing, vraag kredietbureaus om uw rekening in de gaten te houden de komende maanden.
- Doe een uitgebreide virusscan. Wees erg voorzichtig met het downloaden van antivirussoftware. Er zijn nepwebsites actief. Schakel indien nodig hulp in van een bekende.