Aangifte hack

“Iemand anders heeft toegang tot mijn apparaat of netwerk!”

Uw apparaat of netwerk is gehackt, wat houdt dat in?

Uw apparaat of uw netwerk is gehackt, wat betekent dat? Een derde heeft beschikking gekregen over uw wachtwoord en daarmee toegang verkregen tot uw apparaat of uw netwerk.

Gegevens 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. Vul hieronder uw gegevens in.

U kunt dit document op een *computer* invullen. Om het document in te vullen klikt u boven in beeld op “BEELD” en vervolgens op “Document bewerken”.

Gegevens aangever

- Voornaam (voluit)
- Achternaam
- Geboortedatum
- Geboorteplaats
- Adres
- Postcode
- E-mailadres
- Telefoonnummer
- Burgerservicenummer
- Welk identiteitsbewijs neemt u mee naar de aangifte? Dit kan een paspoort, identiteitskaart, rijbewijs of Nederlands vreemdelingendocument zijn.

- Documentnummer identiteitsbewijs

Vragen aangifte

Wilt u ter voorbereiding van de aangifte alvast antwoord geven op onderstaande vragen? De antwoorden vult u in onder de vraagstelling achter ‘A:’.

Algemene vragen

V: Indien bekend, op welke dag/datum/tijd heeft het misdrijf plaatsgevonden?
A:

V: Heeft u nog toegang tot uw apparaat of uw netwerk?
A:

V: 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.
A:

V: Heeft u in het verleden een verdachte sms of e-mail ontvangen van een externe organisatie, waar u op een link moest klikken of persoonlijke gegevens moest invullen? Zo ja, welke organisatie en link is dat geweest (Pas op! Niet op de link klikken)? Voeg de e-mail of SMS toe als bijlage.
A:

V: Wat zou het motief van de hack kunnen zijn?
A:

Ontdekking

V: Op welke dag/datum/tijd heeft u de hack ontdekt?
A:

V: Hoe heeft u dit ontdekt? Denk hierbij aan applicaties die u zelf niet heeft geïnstalleerd, een telefoon die ineens op regelmatige basis vastloopt, verzonden e-mails die u zelf niet heeft geschreven etc.
A:

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*.

Het account

Vermeld in de aangifte zoveel mogelijk informatie, wanneer een van uw accounts is betrokken bij de hack.

V: Is een van uw accounts betrokken bij de hack?
A:

V: Heeft u al een melding gedaan bij het bedrijf dat dit account in beheer heeft?
A:

Mogelijk is uw emailadres gekoppeld aan het gehackte account.
V: Zijn er e-mails namens u verzonden, die u zelf niet heeft verzonden? Indien u nog toegang heeft tot het e-mailaccount, kunt u dit controleren door te zoeken in de map ‘verzonden items’ of de map ‘verwijderde items’.
A:

V: Wat zijn de e-mailadressen van de geadresseerden?
A:

V: Wat was de inhoud van de e-mails? Voeg al uw relevante e-mails toe in als bijlage.
A:

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*.

V: Op welke datum en tijdstip zijn de e-mails verzonden?
A:

V: Was er een herstel e-mailadres gekoppeld aan dit account?
A:

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

V: 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 account.
A:

V: Welk telefoonnummer was gekoppeld aan dit account?
A:

V: Op welke wijze logt u in (bijvoorbeeld via de website of via de app)?
A:

V: Wat voor apparaat gebruikt u om in te loggen op het account (bijvoorbeeld computer, laptop, tablet, telefoon)? En vermeld ook welk merk en type apparaat het is.
A:

V: Hoe is uw account beveiligd? (Bijvoorbeeld met een wachtwoord en tweestapsverificatie)
A:

V: Indien bekend: hoe is de dader mogelijk aan uw inloggegevens gekomen? Mocht dit niet bekend zijn, dan kunt u bijvoorbeeld onbedoeld uw wachtwoord hebben gedeeld via een link uit een phishingmail of een virus hebben gedownload of slachtoffer zijn geworden van een datalek.
A:

Op https://www.politie.nl/informatie/checkjehack.html en op https://haveibeenpwned.com/ kunt u controleren of uw e-mailadres in datasets voorkomt.

Het apparaat

Vermeld in de aangifte zoveel mogelijk informatie over het betreffende apparaat.
V: Welk apparaat is gehackt en wat voor merk en type betreft het? Wees hierbij zo specifiek mogelijk.
A:

V: Waaruit blijkt dat het apparaat gehackt is?
A:

V: Heeft een deskundige/expert het apparaat onderzocht en wat zijn de bevindingen?
A:

V: Zijn er programma's geïnstalleerd door de verdachte of andere wijzigingen aangebracht?
A:

V: Heeft u gecontroleerd of andere apparaten van u ook zijn gehackt?

A:

Schade en impact

V: Heeft de hack voor u tot financiële schade geleid?
A:

V: Kreeg u deze schade vergoed en zo ja, door welke partij?
A:

V: Wat voor mentale en/of fysieke impact heeft dit voorval op u?
A:

Slachtofferhulp

V: 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. A:

Bijlagen

Belangrijke feitelijke informatie dient u ook letterlijk te benoemen bij Algemene vragen. 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 WhatsApp berichten toe als bijlage in de e-mail.

Voorkom misbruik van uw apparaat of netwerk

Om in de toekomst misbruik van uw apparaat of netwerk te voorkomen 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 of gestolen.
- Installeer software updates altijd op tijd. Denk hierbij ook aan uw modem (router).
- Controleer of er onbekende apparaten zijn gekoppeld aan uw accounts. 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.
- Zorg voor een back-up van apparaten en accounts. Bij een hack beschikt u dan nog over een back-up.
- Controleer wekelijks of er updates beschikbaar zijn voor uw apparaten en installeer de updates zo snel mogelijk.
- Op https://laatjeniethackmaken.nl/ vindt u nog meer tips om uzelf te beschermen tegen hackers.
- Doe een uitgebreide virusscan. Wees erg voorzichtig met het downloaden van antivirussoftware. Er zijn nepwebsites actief. Schakel indien nodig hulp in van een deskundige/expert.