Aangifte Diefstal cryptocurrency

Hulpmiddel bij aangifte

Versie juni 2024

« waakzaam en dienstbaar »

Diefstal van cryptocurrency

Cryptocurrency is een digitale munteenheid die bedoeld is om transacties tussen twee partijen mogelijk te maken. Hierbij wordt geen centrale partij betrokken. De bekendste munteenheid, of coin, is de Bitcoin. Wanneer een derde toegang krijgt tot de wallet waarin de crypto wordt beheerd, dan kan de crypto worden gestolen. De crypto wordt dan weggesluisd naar andere cryptowallets waarvan u niet de beheerder bent.

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 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

Algemene vragen

1. Op welke dag/datum/tijd heeft de diefstal van uw cryptocurrency plaatsgevonden?

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

Ontdekking

1. Op welke dag/datum/tijd heeft u de diefstal van uw cryptocurrency ontdekt?

2. Op welke wijze ontdekte u de diefstal?

- 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.

De cryptowallet

Vermeld in de aangifte zoveel mogelijk informatie over de betreffende cryptowallet.

1. Wat is de public key (het adres) van uw cryptowallet?

2. Heeft u zelf de wallet in beheer of verloopt het beheer via een derde partij?

3. Welk type wallet heeft u? (bijvoorbeeld: online wallet, software wallet, hardware wallet of papieren wallet)

4. Welke virtuele valuta bevat de cryptowallet? (bijvoorbeeld: Bitcoin, Ethereum etc.)

5. Wat is de waarde in euro's van de cryptovaluta in de cryptowallet?

Accountgegevens

1. Welke aanbieder van cryptodiensten is gebruikt?

2. Wat is de exacte URL van de exchange waar het delict plaats heeft gevonden?

3. Welke gegevens zijn ingevuld bij de registratie van de account?

4. Wat is de gebruikersnaam?

5. Waar heeft u de inloggegevens bewaard?

6. Is het account beveiligd met tweestapsverificatie?

7. Met welke apparaten heeft u ingelogd op het account?

8. Wie hebben er toegang tot deze apparaten/het account?

Algemene veiligheid

1. Was er sprake van ongewenst toegang van derden tot de wallet?

2. Hoe is de ongewenste toegang tot de cryptowallet vermoedelijk verkregen?

3. Indien bekend, wat is het IP-adres van de fraudeleuze inlog? (Dit is vaak te zien in een security dashboard van betreffende aanbieder cryptodiensten)

4. Is er (per ongeluk) op een phishinglink geklikt? Welke link was dat?

5. Indien er sprake was van phishing, kunt u dan de volgende vragen beantwoorden:

- Wat is uw telefoonnummer en uw emailadres?

- Van welke internetprovider maakt u gebruik?

- Welk telefoonnummer en/of emailadres gebruikte de verdachte?

- Indien van toepassing, welke URL stuurde de verdachte naar u?

6. Is er een up-to-date virusscanner en firewall geïnstalleerd op het apparaat?

7. Is het account beveiligd met tweestapsverificatie?

8. Met welke apparaten heeft u ingelogd op het account?

9. Wie hebben er toegang tot deze apparaten/het account?

Schade en impact

Vermeld in de aangifte zoveel mogelijk informatie over de betreffende transacties.

1. Vul in per cryptotransactie:

   Datum en tijdstip:
   Aantal en valuta:
   Van wallet:
   Naar wallet:
   Transactiehash:

2. Op welk site hebben de transacties plaatsgevonden?

3. Wat is het totale schadebedrag?

4. Heeft u contact gehad met een cryptodienst over de schade?

5. Wat voor impact heeft dit voorval op u?

❖ Belangrijke feitelijke informatie dient u ook letterlijk te benoemen bij *Algemene vragen*, vraag 2.

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:

- Phishinglinks
- Gegevens die de verdachte gebruikte in het contact met u. Naam, telefoonnummer, email.
- Links naar de transacties in Blockchain.
- IP-adressen waar de verdachte gebruik van maakte.
- Voeg al uw relevante e-mails, sms-berichten, en WhatsApp berichten toe als bijlage in de e-mail.

Voorkom diefstal van cryptocurrency

Om diefstal van cryptocurrency te voorkomen hebben wij de volgende tips voor u:

- Zorg voor een apparaat met up-to-date firewall en virusscan. Installeer software updates altijd op tijd. Denk hierbij ook aan je modem (router)
- Check altijd reviews op Google voordat u een account aanmaakt bij een website of cryptoplatform.
- Beveilig uw account altijd met een uniek wachtwoord en tweestapsverificatie.
- 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.
- Maak altijd gebruik van een veilige internetverbinding. Een openbaar wifi-netwerk is niet veilig.
- Controleer in uw email of er doorstuurregels zijn ingesteld. Wanneer uw mailaccount gehackt is, kan de oplichter met vooraf ingestelde woorden zoals “crypto” uw mails automatisch doorsturen en monitoren. Controleer ook de mappen “archief” en “verwijderde items”, omdat de oplichter een bepaalde actie kan hebben ingesteld om berichten te verwijderen.
- Op https://laatjeniethackmaken.nl vindt u tips om uzelf te beschermen tegen hackers.