

Mobiele telefoons

9 vragen over sim-swapping

Het aantal gevallen van sim-swapping neemt toe: oplichters slagen erin om 06-nummers te kapen. Hoe werkt deze fraude en hoe verklein je het risico?

1 Wat is sim-swapping?

Sim-swapping is de Engelse term voor het zonder je toestemming overzetten van je 06-nummer op een ander simkaartje. Je 06-nummer wordt dus gestolen. Je kunt dan niet meer bellen, geen sms'jes meer versturen of ontvangen en niet meer mobiel internetten. Dat is erg, maar ook gevaarlijk: een crimineel kan toegang krijgen tot je accounts.

2 Wat kan een fraudeur met je 06-nummer?

Als een crimineel de controle heeft over je telefoonnummer, kan hij inloggen op je accounts, zelfs als je die extra beveiligd hebt met tweefactorauthenticatie (2FA) via sms. Die accounts kunnen van je sociale media, bank, DigiD of creditcard zijn. De crimineel ontvangt de controlesms'jes die voor jou bestemd zijn, inclusief de codes voor tweefactorauthenticatie. Zo kan hij je wachtwoorden resetten. Ten slotte kan hij fraude plegen in jouw naam, bijvoorbeeld door WhatsApp-berichten te sturen naar je familie en vrienden en om geld vragen.

3 Hoe gaan criminelen te werk?

Veel pogingen beginnen met phishing, omdat de fraudeurs persoonlijke gegevens van jou nodig hebben. Ze sturen je een e-mail of een sms waarin ze bijvoorbeeld beweren dat je simkaart verouderd is en dat je hem moet vernieuwen. Ze lokken je naar een nepwebsite en

Het aantal meldingen van deze fraudevorm is de afgelopen maanden sterk gestegen

vragen je persoonsgegevens in te vullen, waaronder je e-mailadres, telefoonnummer en soms zelfs je BSN. Het kan nog brutaler. Er zijn ook oplichters die hun slachtoffers bellen en zich voordoen als medewerker van de provider. Ze vertellen dat je sim-

kaart moet worden 'gevalideerd' of dat die moet worden omgezet naar een eSIM. Met de persoonsgegevens bellen ze de helpdesk van je telecomprovider en doen zich voor als jou. Ze zeggen bijvoorbeeld dat ze hun telefoon kwijt zijn en een nieuwe simkaart nodig hebben. De provider controleert of alles klopt en als dat zo lijkt, gaat je telefoonnummer over naar iemand anders' simkaartje. Het maakt trouwens niet uit of je een plastic simkaartje of een eSIM hebt.

4 Waarom is sim-swapping in het nieuws?

Sim-swapping is niet nieuw, maar het aantal meldingen van deze fraudevorm is de afgelopen maanden sterk gestegen. De Fraudehelpdesk kreeg in de eerste vijf maanden van dit jaar 300 meldingen. Opvallend vaak gingen die over KPN en Odido, waarbij het in totaal om duizenden euro's schade ging. De verklaring van Odido hiervoor is dat de oplichters zich vaak voordoen als (medewerker van) Odido om de benodigde gegevens voor het sim-swappen te bemachtigen.

5 Hoeveel risico loop je?

Er is geen reden voor grote zorgen. Het aantal gevallen van sim-swapping is heel laag vergeleken bij andere vormen van online fraude. Maar het probleem groeit wel. Je loopt een verhoogd risico als je sms-codes gebruikt als tweefactorauthenticatie. Gebruik daarom zo mogelijk liever een authenticator-app als tweede inlogmiddel. Zie het kader 'Verklein het risico'.

6 Hoe weet je of je slachtoffer bent?

Je zou slachtoffer van sim-swapping kunnen zijn als je plots niet meer kunt bellen of internetten met je telefoon. Of je krijgt een melding dat een wachtwoord is gereset, terwijl je dit zelf niet hebt aangevraagd. En misschien melden vrienden of familieleden dat ze verdachte berichten van je ontvangen. Als je zo'n aanwijzing krijgt, moet je direct contact opnemen met je telecomprovider. Zie vraag 9.

7 Wat doen providers om sim-swapping te voorkomen?

We vroegen het KPN, Oido en VodafoneZiggo. Klanten moeten zich bij een simwissel op verschillende manieren identificeren, bijvoorbeeld door specifieke klantgegevens te geven of controlevragen te beantwoorden. Bij verdachte situaties voeren de providers naar eigen zeggen extra controles uit en wordt het telefoonnummer en de simwissel tijdelijk geblokkeerd. De provider neemt ook contact op met de klant. Verder is voorlichting belangrijk, de providers geven tips op hun websites. Ze benadrukken dat ze geen sms'jes of e-mails sturen over verlopen simkaarten en niet bellen over simkaartvalidatie of -overstap. Desondanks lukt het fraudeurs om sims over te nemen.



8 Wat moet je doen als je denkt dat je slachtoffer bent?

Neem direct contact op met je telecomprovider en meld dat je vermoedt dat je nummer is overgenomen. Vraag of ze je nummer kunnen blokkeren. Wijzig zo snel mogelijk wachtwoorden van belangrijke accounts, die van je e-mail en bank als eerste. Bel je bank en vertel over je vermoedens. Controleer je accounts op verdachte activiteiten. Doe aangifte bij de politie als je inderdaad slachtoffer bent geworden van sim-swapping.

9 Kun je gestolen geld terugkrijgen?

Dit is lastig. Banken en verzekeraars vergoeden schade door sim-swapping lang niet altijd. Ze kijken of je voldoende beveiligingsmaatregelen hebt genomen. Is er sprake van 'grote nalatigheid' aan jouw kant (zoals simpele wachtwoorden of geen tweefactorauthenticatie), dan zal aansprakelijk worden afgewezen en draai je zelf voor de schade op. Dat gebeurt ook als je waarschuwingen van je bank of provider hebt genegeerd of niet meteen actie hebt ondernomen. ■

Verklein het risico

Je kunt sim-swapping niet helemaal voorkomen, want de fraudeur regelt die buiten jou om met je provider. En soms wordt het gedaan via een hack of contactpersoon bij de provider. Wat kun je wel doen?

- ▶ Voorkom dat een oplichter je persoonsgegevens in handen kan krijgen. Pas dus goed op voor phishing. Beperk de persoonlijke informatie die je online deelt, zoals je geboortedatum, adres en telefoonnummer.
- ▶ Klik niet op links in verdachte berichten en verwijder die berichten meteen.
- ▶ Beëindig verdachte telefoontjes, ook als iemand namens een provider belt. Bel de provider vervolgens zelf.
- ▶ Gebruik zo min mogelijk sms voor tweefactorauthenticatie, maar installeer een authenticator-app, bijvoorbeeld die van Google, Microsoft of Authy.
- ▶ Beveilig je accounts met sterke, unieke wachtwoorden met behulp van een wachtwoordmanager.

Digitaal blijblijven?

In de Digitaalguide vind je elke 2 maanden alles over digitale trends en online dreigingen. Probeer nu met korting.

Bekijk de aanbieding

