Het Laatste Nieuws | Het Laatste Nieuws | NEWSPAPER | 02/05/2023

HLN ONDERZOEK | Nieuwe onlinefraude: swipen | Cybercriminelen shoppen met uw gestolen gegevens - Niets besteld, maar plots Zalando-factuur van 1.000 euro

Je hebt niets besteld, maar toch krijg je een factuur van honderden euro's van Bol.com, Zalando of Amazon. Dat overkomt steeds meer Vlamingen, door een nieuwe soort cybercriminaliteit: 'swipen'. Daders hacken je gegevens, bestellen dure spullen en geven aan dat ze pas na de levering willen betalen. Dat gaat verbazend makkelijk.

Deze klant komt uit Willebroek. Met zijn account bestelde ik voor 400 euro, sneakers en andere shit. We praten anoniem met Lars (17)*. Hij is één van de vele jongeren in heel Vlaanderen die swipen heeft ontdekt. Niet het soort swipen dat je doet op datingapps: deze vorm betekent simpelweg 'stelen' in straattaal en kost nietsvermoedende klanten van webshops soms honderden euro's. Alleen maar omdat ze net iets te slordig zijn omgesprongen met hun digitale wachtwoorden — door die bijvoorbeeld niet vaak genoeg te veranderen of te makkelijke paswoorden te kiezen, zoals een reeks opeenvolgende cijfers.

Als je het slachtoffer wordt, krijg je plots een mail met de melding dat je bestelling is verstuurd — alleen heb je helemaal niets besteld. Het kan om phishing gaan, waarbij criminelen een valse mail versturen, maar soms komen de mails ook écht van een grote webshop. Bij onder meer Zalando, Bol.com en Amazon kan je er namelijk voor kiezen om pas na een bestelling te betalen, via overschrijving. Makkelijk, maar ook een open deur voor cybercriminelen. Zij hacken accounts en kopen dure spullen. De rekening belandt bij de eigenaar van het account. Zo kreeg de 38-jarige Bert* een factuur van net geen 1.000 euro, voor onder meer een trui van Lacoste, onderbroeken van Calvin Klein en schoenen van Nike. De kleren waren afgeleverd op een postpunt in Molenbeek. Een tijd later kreeg hij een mail van een incassobureau: De kosten waren al opgelopen naar 1.200 euro. Bert moest een klacht indienen bij de politie — alleen dan zou hij de rekening niet meer moeten betalen. Ook bij andere slachtoffers bleek dat de enige oplossing (zie kaders).

Draaiboek

Deze vorm van internetfraude is populair op sociale media als Telegram, Snapchat en TikTok. Dat ontdekte onze onderzoekscel door wekenlang mee te lezen in chatkanalen en accounts te volgen. Jongeren, zelfs minderjarigen, verdienen grof geld door elektronica of kledij te bestellen met gehackte accounts en die daarna door te verkopen. Ik kan rond de 750 euro aan kledij swipen per keer, vertelt Lars (17) uit Antwerpen. Bij een hoger bedrag kan hij op de webshop in kwestie niet meer kiezen voor 'achteraf betalen'. We spreken hem aan op Telegram. Lars koopt regelmatig de gegevens van gehackte accounts via sociale media. Hij stuurt ons een voorbeeld van een hoop bestelde kleren. We kiezen een

account met een bestelgeschiedenis, anders kan je niet achteraf betalen. We laten de pakketjes leveren in een automaat en vragen andere jongeren om ze te gaan halen. Soms kiezen we ook een adres uit — meestal geven de mensen het pakje gewoon mee.

We verkopen ook methodes, vult Ben* aan. Daarmee leren we anderen hoe je moet swipen. Ook dat stellen we vast in de groepen: er worden draaiboeken en scripts aangeboden om gehackte accounts te gebruiken. Ook hulpmiddelen om accounts van webwinkels te hacken zijn te koop — zogenaamde 'configs'. Dat is een bestand dat ingeladen kan worden in een programma waarmee je accounts kan hacken, vertelt Wesley Neelen van cybersecuritybedrijf Zolder. De oplichter moet het programma gewoon laten draaien en krijgt de inloggegevens als een juiste combinatie gevonden is. Soms passen webwinkels hun instellingen aan, om zulke hacking tegen te gaan, maar dan herwerken de hackers hun programma ook.

Pech

Webwinkels als Zalando en Bol.com maken deze vorm van misbruik deels zélf mogelijk, zegt professor Roel Gevaers, expert in e-commerce aan de Universiteit Antwerpen. Volgens hem zou tweestapsverificatie dit mee kunnen oplossen. Daarbij moet je niet alleen je paswoord ingeven, maar daarna nog eens je identiteit bevestigen, bijvoorbeeld met een code die je krijgt via sms of een extra pincode. Maar dat gebeurt dus niet. De webshops willen het hun klanten zo makkelijk mogelijk maken: elke extra klik bij een aankoop kan ervoor zorgen dat een klant afhaakt. Het fraudebedrag zal niet groot genoeg zijn tegenover de totale omzet om zwaar in te grijpen. De klant die ermee te maken heeft, heeft dan maar pech.

De overheid zou ook kunnen tussenkomen, zegt professor Gevaers. Als die bij een fraudegeval de verantwoordelijkheid meteen bij de webshops zou leggen, zouden er wellicht sneller maatregelen genomen worden. Maar als de overheid zich niet bewust is van dit soort fraude, is het moeilijk om er wetgeving rond te maken.

Hoeveel Vlamingen al slachtoffer zijn geworden van de praktijk, weet de federale politie niet — er zijn nog geen aparte cijfers over. De politie waarschuwt wel voor dit soort internetfraude: Bescherm je gegevens goed, door bijvoorbeeld een sterk wachtwoord te maken en dat vaak genoeg te wijzigen. Als je account toch gehackt wordt, of als je een pakje aan de deur krijgt waar een andere naam op staat, neem het dan niet aan en doe aangifte bij de politie. Bol.com laat weten dat het continu bestellingen monitort op zoek naar mogelijke fraude. Bij Zalando was niemand bereikbaar.

*Lars, Ben en Bert zijn schuilnamen.

JOPPE NUYTS