Nederlanders zetten eigen digitale veiligheid op een laag pitje

Cybersecurity Bewustzijnsonderzoek 2018: driekwart getroffen, helft komt niet in actie na cybercrime

Den Haag, 1 oktober 2018 – Nederlanders maken zich nog steeds zorgen om hun online veiligheid thuis. De mate van deze bezorgdheid is stabiel gebleven ten opzichte van vorig jaar. In 2017 maakte 46% zich zorgen over hun online veiligheid, in 2018 ligt dit percentage op 44%. Men schat de kans om zélf slachtoffer van cybercrime te worden laag in, terwijl een grote meerderheid van de Nederlanders weleens te maken heeft gehad met cybercrime. Eenmaal geconfronteerd met een vorm van cybercrime wordt mondjesmaat actie ondernomen. Dit en meer blijkt uit het Nationaal Cybersecurity Bewustzijnsonderzoek 2018, een trendonderzoek in opdracht van de NCTV en het initiatief Alert Online.

Minister Grapperhaus van Justitie en Veiligheid: “Het is zorgwekkend dat veel mensen zich nog steeds niet écht bewust zijn van de risico’s in de digitale wereld. De gevaren online zullen de komende jaren alleen maar toenemen, dus we moeten onszelf ook beter beveiligen. Mensen mogen van mij als minister verwachten dat ik, samen met al mijn collega’s en het bedrijfsleven, er voor zorg dat de Nederlandse maatschappij digitaal op orde is. Maar sterke wachtwoorden verzinnen, updates draaien, back-ups maken, dat moeten mensen echt zelf doen. Mijn boodschap is simpel: draai de digitale achterdeur op slot!

Bijna driekwart van de Nederlanders heeft weleens te maken gehad met cybercrime

Meer dan een kwart van de Nederlanders denkt weinig gevaar te lopen thuis. Zo maakt 45% zich nooit zorgen om identiteitsfraude en is 39% niet bezorgd om een cyberaanval. Dat deze relatieve onbezorgdheid niet terecht is, blijkt uit het feit dat 74% van de Nederlanders thuis weleens te maken heeft gehad met een vorm van cybercrime (in 2017 was dit nog 65,6%).

De drie meest voorkomende vormen van cybercriminaliteit zijn: een poging tot phishing (56%), benaderd worden met een socialmediabericht met de vraag om een onbekende link aan te klikken (37%), het ontvangen van een zakelijke uitnodiging via social media en malware (beide 20%). De grootste risico’s worden door Nederlanders gezien in het openen van een (foute) hyperlink of bijlage in een e-mail, het downloaden van bestanden op internet en het gebruikmaken van een openbare computer.

Slechts helft Nederlanders neemt maatregelen

Nederlanders zijn tamelijk hardleers als het gaat om het nemen van maatregelen om zichzelf online te beveiligen. De helft van de getroffen Nederlanders geeft aan helemaal niets te hebben gedaan nadat ze thuis zijn getroffen door cybercriminaliteit. De drie meest populaire beveiligingshandelingen die men onderneemt zijn: antivirussoftware installeren (43%), wachtwoorden complexer maken (31%) en het controleren van websites op HTTPS (31%). Nederlanders hebben niet de wil om hun online veiligheid te verbeteren: bijna vier op de tien willen dit niet. Bijna driekwart (71%) acht zichzelf hier trouwens wel verantwoordelijk voor, zo blijkt uit het onderzoek.

Nieuwe cybergevaren: Internet of Things

Erik Jan Koedijk, voorzitter van de Raad van Advies van Alert Online: “Er liggen veel nieuwe vormen van cybercriminaliteit op de loer. Denk aan de steeds populairder wordende apparaten en apps die via internet met elkaar communiceren zoals smart tv’s, slimme lampen, camera’s en thermostaten. Hier zijn nog veel gaten in de beveiliging doordat deze apparaten vaak nog de makkelijk te raden wachtwoorden vanuit de fabriek hebben. De wachtwoorden zijn niet uniek en

je vindt ze vaak op het internet terug. Uit ons onderzoek blijkt dat nog niet eens de helft van de Nederlanders zo'n wachtwoord aanpast."

Eenvoudige handelingsperspectieven
Waarom ondernemen 'we' relatief weinig actie na slachtofferschap? Reint Jan Renes, lector en gedragswetenschapper van de Hogeschool Utrecht, erkent het hardnekkige probleem onder Nederlanders: "We weten stiekem wel dat we het anders zouden moeten doen. We willen wel online veilig zijn, maar die wil is vaak tegenstrijdig met wat we er concreet voor moeten doen of laten. We gaan onszelf dan vragen stellen. Heeft het echt zin? Hoe erg is het nu eigenlijk? Belangrijk is dat Nederlanders moeten weten wat zij zélf makkelijk kunnen doen om zichzelf beter te beveiligen tegen cybercriminaliteit. Ook moeten we blijven werken aan het besef dat er concrete gevaren om de hoek liggen."

Oktober: Europese Maand van de cyberveiligheid
Het verbeteren van het cybersecuritybewustzijn van Nederlanders staat centraal tijdens de Europese Maand van de cyberveiligheid. Deze maand wordt door het initiatief Alert Online en andere partijen aangegrepen om aandacht te vragen voor veilig online gedrag. Zo opent Voorzitter van de Tweede Kamer Khadija Arib vandaag 1 oktober om 10.00 uur een Cybersecurity Escape Room voor Tweede Kamermedewerkers. Op 15 oktober start een voorlichtingscampagne om Nederlanders te wijzen op de risico's in hun online handelen en hoe zij internetcriminaliteit kunnen voorkomen.

========