TEKST DAAN VERMEER

Oplichting en misleiding

Wie belt er eigenlijk?

Met allerlei trucs proberen bedrijven en oplichters je telefonisch geld uit de zak te kloppen. Helaas zegt het telefoonnummer waarmee ze bellen niet alles.

● Winkelen, werken, bankzaken doen en contacten onderhouden. Dit gaat vaak telefonisch en via internet. Dat heeft veel voordelen, hebben we het afgelopen jaar wel gemerkt. Maar niet iedereen kan de digitalisering goed bijbenen. Dat geeft kwaadwillenden een voorsprong. Zij kunnen eenvoudig, anoniem of met een vervalste identiteit, contact met slachtoffers leggen. Via websites en e-mail, maar ook via sms, WhatsApp en telefonisch. Soms gaat het om vervelende telemarketing, waarbij lastig na te gaan is welk bedrijf er belt. Maar het kan ook een crimineel zijn die technische trucs gebruikt om zich voor te doen als iemand anders. Bijvoorbeeld met een gemanipuleerd e-mailadres of telefoonnummer. Dat heet *spoofing*. Bekende voorbeelden zijn bancaire fraude en helpdeskfraude, we hebben er al vaker over geschreven. Die trucs gaan vaak hand in hand met *phishing*. Daarbij hengelen criminelen naar persoonlijke informatie, zoals inloggegevens en pincodes. Al deze vormen van oplichting hebben enorme financiële gevolgen. Zo bedroeg de totale schade door telefoonnummerspoofing in het betalingsverkeer het afgelopen jaar bijna €27 miljoen. Goed opletten wie er belt dus. Maar helaas zegt het telefoonnummer niet alles.

Telemarketing via 088 en 085

Telemarketeers die consumenten bellen, doen dat soms vanaf nummers die beginnen met 085 of 088. In tegenstelling tot netnummers als 010, 020 en 030, zijn zulke telefoonnummers niet aan een locatie gebonden. Dat maakt ze aantrekkelijk voor bedrijven die landelijk werken. Ook nummers die beginnen met 0800, 087, 090, 091, 116, 14 en 18 zijn niet aan een locatie gebonden. Word je gebeld door zo'n nummer, dan weet je dus niet waar de beller vandaan belt.

Ook particulieren kunnen tegenwoordig voor enkele euro's zo'n telefoonnummer aanvragen. Iemand met kwade bedoelingen kan dus zo'n nummer kopen en weer snel overstappen op het volgende. De kosten zijn immers verwaarloosbaar.

Nummerspoofing is kinderlijk eenvoudig, merkten we toen we het zelf probeerden

Anonieme nummers

Een netnummer dat wél locatiegebonden is, zegt ook niet alles. Vroeger gaf KPN lokale netnummers uit. Die hoorden bij een specifieke regio, omdat ze verbonden waren met de fysieke telefooncentrale. Nu verstrekt de toezichthouder Autoriteit Consument & Markt (ACM) netnummers met 1000 tegelijk. Net als bij de 088-

nummers, kunnen bedrijven die kopen, ongeacht waar ze in Nederland ingeschreven staan. Alleen verstrekt de ACM die telefoonnummers in bulk en niet direct aan eindgebruikers. Vaak koopt een telecombedrijf een volledige reeks nummers en verhuurt een deel daarvan aan een ander bedrijf. En dat bedrijf leent individuele telefoonnummers weer uit aan particulieren en bedrijven. Die nummers verschijnen niet in een (online) telefoongids of register. En de locaties die smartphones laten zien bij een bepaald netnummer, kloppen dus ook niet. Dat maakt netnummers, inmiddels net zo anoniem als 085-nummers. Terwijl ze dus wel vertrouwd overkomen.

Namens KPN?

Een telefoonnummer op het scherm zegt dus niets over de locatie van de beller. En je weet dus ook niet zeker of je een bedrijf of individu aan de lijn hebt. Als de beller beweert namens een bepaald bedrijf te bellen, is dat dus lastig te achterhalen. Zo kregen wij twee keer hetzelfde bedrijf aan de lijn dat aangaf 'namens KPN' te bellen. De ene week eindigde het nummer op 209 00 88, een week later op 209 00 87. Toen we terugbelden naar deze nummers, hoorden we dat we de 'Servicedesk van de acquisitie namens KPN' aan de lijn hadden. Maar KPN zegt dat het consumenten nooit met aanbiedingen belt. En dat het bedrijf daar ook nooit callcenters opdracht toe geeft. Bovendien is er bij de Kamer van Koophandel geen bedrijf ingeschreven dat Servicedesk heet. Wie hadden we nu eigenlijk écht aan de lijn?
We achterhaalden dat deze telefoonnummers afkomstig zijn uit een reeks van 1000 die ACM vorig jaar toekende aan een internationaal telecommunicatiebedrijf. Dat leende een deel van die nummers weer uit aan een Fins techbedrijf met software voor callcenters. En een van hun klanten gebruikte deze telefoonnummers. Dat bedrijf heet niet Servicedesk en zit ook niet in de buurt van de plaats waar het netnummer vandaan leek te komen.
Ook zo'n netnummer is eenvoudig aan te vragen en te gebruiken. Zo kwamen we een 015-nummer op het spoor waarmee

€5

kost het aanvragen van een 085-nummer

dit voorjaar duizenden consumenten gebeld werden. Het bedrijf dat het nummer ooit registreerde, was in oktober 2020 al uitgeschreven bij de Kamer van Koophandel. In de tien maanden dat het wél ingeschreven was, veranderde het liefst viermaal van naam. De persoonsgegevens die dit bedrijf buitmaakte, verkocht het via Instagram en Facebook. Een lekker verdienmodel. Dit alles kun je niet weten als een vertrouwd ogend 015-nummer je belt.

Neptelefoonnummers

Criminelen gaan vaak nog een flinke stap verder. Zij verschuilen zich niet achter een anoniem nummer, maar vervalsen het nummer waarmee ze bellen. Zij kunnen zo elk zelfgekozen nummer gebruiken, ook als dat al in gebruik is. En juist daarin schuilt het gevaar. Het bekendste voorbeeld van nummerspoofing is bankspoofing. Daarbij helpt een zogenaamde bankmedewerker je telefonisch om geld veilig te stellen (zie het kader hieronder).
Hoe kinderlijk eenvoudig nummerspoofing is, ontdekten we toen we het zelf eens probeerden. Binnen een kwartier en tegen betaling van nog geen €10 aan een Bulgaars bedrijf, kregen we toegang tot een website die nummerspoofing faciliteert. We hoefden ons niet te legitimeren en konden met een virtuele creditcard betalen. Dat is een digitale betaalkaart die direct na de betaling weer verdwijnt. Via die site probeerden we collega's te bellen namens een telefoonnummer dat wij vooraf kozen. Toen we hen belden, verscheen in hun scherm het telefoonnummer van de BelastingTelefoon of de Alarmlijn van ING. Voor hen was het alsof onze oproep van die instanties afkomstig was.
Onze test legt het grote gevaar van nummerspoofing bloot: de techniek is eenvoudig toegankelijk voor iedereen met kwade bedoelingen. En een bekend telefoonnummer wekt vertrouwen. Als je gebeld wordt door 020-2288800, herken je dat nummer misschien niet direct. Maar als je het op internet natrekt, zie je dat het de Alarmlijn van ING is. Oppassen dus, want je hebt mogelijk niet de ING aan de lijn als dat nummer op je scherm verschijnt. Alleen door het nummer zelf terug te bellen, weet je zeker dat je met ING – of welk bedrijf dan ook – spreekt. Dus welk nummer er ook op je scherm staat, het blijft een raadsel wie er belt. ■

Bank moet standaard vergoeden

Vorig jaar werden duizenden Nederlanders slachtoffer van bankspoofing: via het telefoonnummer van de bank beroofden nepmedewerkers hun slachtoffers van hun spaargeld. Deze fraude was in 2020 goed voor ruim €26 miljoen schade. Mede dankzij onze druk op de politiek hebben banken de schade vergoed, uit coulance zeiden ze zelf. Maar we zijn er nog niet. Wij willen af van die 'coulance'. Banken moeten bij dergelijke doortrapte fraudevormen de schade standaard vergoeden. Hiervoor blijven we druk uitoefenen op de sector en de politiek. Zie ook consumentenbond.nl/vergoed-bankspoofing.

Consumenten bond

Smaakt dit naar meer?

Word lid en krijg direct toegang tot alle onafhankelijke tests en informatie.

Ja, vertel me meer