5 VEELVOORKOMENDE TRUCS

VOORKOM ONLINE OPLICHTING

Valse appjes, phishingmails en nepwebshops: cybercriminelen worden steeds gewiekster en zijn actiever dan ooit. Vijf vaak voorkomende vormen van online oplichting en hoe je je ertegen wapent.

WhatsApp-fraude

WhatsApp is populair, én toegankelijk. Iedereen kan een bericht via WhatsApp sturen. Criminelen maken er dan ook graag gebruik van. Sterk in opkomst is de tactiek waarbij de oplichter zich voordoet als een familielid of bekende. Hij heeft net een nieuw telefoonnummer en vraagt om geld. De berichtjes zijn vaak akelig realistisch. Ook bekend zijn de berichten van zogenaamde banken dat er iets mis is met je bankpas. Even inloggen en het 'probleem' is verholpen. Maar het linkje leidt naar een nagebouwde site. Wie daar inlogt, overhandigt zijn gegevens aan oplichters.
In alle gevallen waarin wordt gevraagd om geld over te maken, bestanden te downloaden of ergens in te loggen, is het goed om achterdochtig te zijn. Wantrouw altijd nieuwe telefoonnummers. Bel bij twijfel de persoon op zijn oude nummer. Neemt hij op, dan is meteen duidelijk dat het nieuwe nummer van een fraudeur is.

Phishing

Bijna iedereen ontvangt weleens phishingmail. Vaak komt die zogenaamd van een bank, provider of ander vertrouwenwekkend bedrijf, met het verzoek om ergens in te loggen of een bijlage te downloaden. Bij deze onderwerpen is de kans op phishing groot: bankzaken, incasso's, vorderingen, boetes, facturen, verlopen accounts, mislukte betalingen, gemiste pakketjes en autoschade.
De tijd dat deze mails vol spelfouten stonden, is voorbij. Ook zien ze er steeds professioneler uit. Toch kun je phishingmails meestal wel herkennen. Zo is de aanhef vaak onpersoonlijk ('Geachte klant') en klopt het e-mailadres van de afzender niet. Als KPN een mail verstuurt, eindigt het mailadres op @kpn.com. Dat van een fraudeur eindigt bijvoorbeeld op @kpn-service.com. Deze domeinnaam is niet van KPN, maar komt wel betrouwbaar over.
Klik nooit zomaar op een link in een mail als je niet zeker weet of die van een betrouwbare bron komt. Als een mailtje van ING Bank linkt naar een onlogisch webadres dat bijvoorbeeld begint met bit.ly, is er iets mis. Download ook geen bijlagen die door onbekenden zijn gestuurd. Een virusscanner kan ook veel leed voorkomen.
Meestal richten phishing-fraudeurs zich op grote groepen tegelijk. Het idee is dat er dan altijd wel iemand bij zit die erin trapt. Maar steeds vaker zoekt de cybercrimineel zijn slachtoffer gericht uit. Dit heet spear phishing. Soms volgt de oplichter daarbij iemand langere tijd via social media, om zo kennis te verzamelen die hij kan gebruiken om het vertrouwen van zijn slachtoffer te winnen.

Nepwebshops

Lage prijzen zijn verleidelijk. Criminelen spelen hier handig op in met webshops die er soms verrassend professioneel uitzien. Compleet met werkende helpdesk, keurmerklogo's, reviews van nepkopers en een inschrijvingsnummer van de Kamer van Koophandel. Maar als je iets bestelt, ontvang je niets, of een namaakproduct. Extreem lage prijzen zijn op z'n minst reden om extra onderzoek te doen. Zoek via Google en betrouwbare review- en klachtensites als Trustpilot.com, Kieskeurig.nl en Klachtenkompas.nl naar klachten over de webwinkel. Check of er een telefoonnummer, bezoekadres en normaal e-mailadres op de site staan. Neem bij twijfel eerst contact op. Vraagt een website om geld over te maken naar een buitenlands rekeningnummer, laat hem dan links liggen. De veiligste betaalmethode is via creditcard of PayPal. Hiermee krijg je je geld terug als de webshop niet levert. Bij iDeal geldt dat niet.

Neptelefoontjes

Cybercriminelen zoeken ook contact via de telefoon. Ze doen zich bijvoorbeeld voor als helpdesk- of bankmedewerker en vertellen dat er iets dringends mis is. Meestal moet er snel gehandeld worden. Er klopt natuurlijk niets van het verhaal, maar ga je erin mee, dan zijn de gevolgen niet te overzien.
Berucht zijn de telefoontjes uit naam van Microsoft. De medewerker meldt dat er dringende problemen zijn gesignaleerd. Voor een paar tientjes helpt hij je zogenaamd overal vanaf. Soms blijft het daarbij, maar het komt ook voor dat hij meekijkt tijdens de internetbetaling en je bank- of creditcardgegevens steelt. Of hij installeert ransomware of andere schadelijke software op je pc. Ga hier dus niet in mee. Microsoft belt nooit ongevraagd klanten. Net als een bank ook nooit belt met het verzoek om geld over te maken. Bij twijfel: hang op en neem zelf contact op via het officiële nummer van de bank of het bedrijf.
Ben je gebeld door een onbekend nummer, bel dan niet terug. Zeker niet als het een buitenlands nummer is. Dit is een bekende truc, die wangirifraude heet. Criminelen bellen met een onbekend nummer, laten de telefoon twee keer overgaan en hangen op. In de hoop dat je terugbelt, want dan gaat de teller lopen. Het nummer is namelijk gekoppeld aan een dure betaaldienst. Hoe langer je aan de lijn blijft, des te meer de crimineel verdient.
Tip: veel telefoons kun je zo instellen dat ze onbekende nummers automatisch afwijzen of naar de voicemail doorschakelen.

31.000

MELDINGEN OVER ONLINE FRAUDE KREEG DE FRAUDEHELPDESK IN 2019, DAT IS 63% MEER DAN IN 2018

Marktplaatsoplichting

Ook bij online marktplaatsen als Marktplaats, eBay en Speurders ligt oplichting op de loer. Vaak gaat het om malafide (ver)kopers die een product niet opsturen of weigeren te betalen. Maar criminelen gebruiken de verkoopsites ook om identiteitsbewijzen te stelen. Ze vragen om een kopie, zogenaamd om te controleren of je te vertrouwen bent. En vervolgens sluiten ze er leningen of telefoonabonnementen mee af. Stuur dus nooit een kopie van je identiteitsbewijs aan een koper of verkoper.
Berucht is ook Tikkiefraude. Een fraudeur vraagt je om 1 cent over te maken 'om je identiteit te controleren'. Vervolgens stuurt hij een nep-betaallink. Dat gaat meestal via Tikkie, vandaar de naam. Maar ook andere betaaldiensten, zoals Payconiq, iDeal en de 'Gelijk Oversteken'-dienst van Marktplaats worden ervoor misbruikt. Gebruik je de link, dan overhandig je je bankgegevens aan de crimineel. Doe dus nooit 1-cent-betalingen aan particulieren. Beperk de communicatie zo veel mogelijk tot het eigen berichtensysteem van de verkoopsite en schakel niet over naar bijvoorbeeld WhatsApp. Stuurt de verkoper via een ander kanaal een betaallink, controleer dan heel goed of die klopt.

MEER LEZEN?

In het boek Voorkom online oplichting lees je hoe cybercriminelen te werk gaan. Waar liggen de gevaren? En hoe voorkom je dat je slachtoffer wordt van online oplichting? Het boek kost €22 voor leden en €27,50 voor niet-leden. Het e-book kost €14 voor leden en €17,50 voor niet-leden. Te bestellen via consumentenbond.nl/webwinkel of telefonisch: 070-445 45 45.

Consumenten bond

Smaakt dit naar meer?

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

Ja, vertel me meer