De psychologie achter de telefonische babbeltruc

Televisieprogramma Kassa maakte er in september een groot item over: Oplichters bellen mensen met het verhaal dat ze van de alarmlijn van de bank zijn. Gelukkig zijn we tegenwoordig een stuk alerter op dit soort telefoontjes. Dus weten we meteen wat we moeten doen! We checken het nummer in het scherm van onze telefoon. Warempel, het nummer klopt. Voor sommige mensen een reden om zich veilig te wanen en mee te gaan in het verhaal. Onterecht, want de trucs van criminelen zijn tegenwoordig zo vernuftig dat het juiste nummer in het scherm niet langer een garantie is. Via spoofing is het namelijk mogelijk om een ander nummer op de telefoon weer te geven dan waarmee daadwerkelijk gebeld wordt. Dat vraagt dus om nog meer alertheid en betere checks!

Door Inge Wetzer
Fotografie: Josina van den Bosch

Inge Wetzer is gepromoveerd in de sociale psychologie. Na 10 jaar onderzoek naar gedragsbeïnvloeding bij TNO is zij sinds 2015 gespecialiseerd in cybersecurity. Ze werkt momenteel bij Secura als sociaal psycholoog cybersecurity & compliance in het team dat zich richt op de 'menskant' van informatiebeveiliging.

In de cybercriminaliteit is een duidelijke trend zichtbaar: waar vroeger vooral technisch werd gehackt, wordt nu steeds vaker via de mens aangevallen: social hacking. Deze trend betekent niet alleen verschoven aandacht! Het betekent vooral dat er meer aandacht, voorbereiding en zorg aan deze mensgerichte aanvallen besteed wordt. Met als resultaat geavanceerdere aanvalsmethoden, die steeds moeilijker te herkennen zijn. Niet langer slecht vertaalde e-mails over ongeloofwaardige erfenissen dus. Wake up call voor mensen die nog dachten dat alleen oude mensen het slachtoffer worden van telefonische babbeltrucs…

Social hacking. Het begint pas bij spoofing. Want daarna komen de psychologische trucs. Die maken duidelijk dat deze criminelen zich goed hebben verdiept in de psychologie. Feilloos maken zij gebruik van allerlei menselijke mechanismen. Een aantal van deze mechanismen wordt in dit artikel toegelicht.

De 'bankbabbeltruc'

Even terug naar de 'bankbabbeltruc'. Het nummer in je display komt dus overeen met het nummer van de officiële crisislijn van je bank. De naam van de medewerker die je belt klopt ook, want die is door de criminelen van sociale media zoals LinkedIn gehaald. Het is overigens een vrouwelijke medewerker, spreekt perfect Nederlands en is uitermate vriendelijk en behulpzaam. Wel een beetje bezorgd, want, vertelt ze je, ze heeft net gezien dat er op dit moment €5.000 van je rekening wordt overgeschreven naar een rekeningnummer in de Oekraïne. Licht bezorgd vraagt ze of dat kan kloppen.

Inge Wetzer was afgelopen september te zien in een uitzending van televisieprogramma Kassa dat gewijd werd aan de telefonische babbeltruc.

Nee! Gelukkig hoef je niet in paniek te raken, want de vrouw vertelt dat ze de overschrijving heeft tegengehouden omdat ze hem als verdacht hadden aangemerkt.

Terwijl je aan de telefoon bent blijkt dat men probeert nog meer geld van jouw rekening af te schrijven. Best stressvol. Maar geen paniek, want de bank is je erbij aan het helpen. Er blijkt even later een nieuwe telefoon aan je rekening te worden gekoppeld, ben jij dat? Ook niet… De bankmedewerker (en haar collega's op de achtergrond) vinden het wat veel worden en hebben een plan: Voor deze avond stellen we je geld even veilig op een veilige kluisrekening. Dan kan niemand erbij en kun je morgen in je eigen filiaal met je paspoort en bankpas alles gaan regelen. Je vindt het natuurlijk spannend maar wat kun je? Op de achtergrond hoor je af en toe een andere bankmedewerker roepen dat hij weer een transactie heeft tegengehouden en de bankmedewerkers complimenteren elkaar. Ze zijn als team jou aan het helpen en zullen ervoor strijden dat jouw geld niet bij de criminelen terecht komt. Want boeven zijn het!

De psychologische mechanismen

Bovenstaande social hacking aanval zit vrij kunstig in elkaar. Het is doordrongen van psychologische mechanismen die inspelen op de emoties en natuurlijke reacties van mensen. Welke typisch menselijke mechanismen zijn in deze truc te onderscheiden?

Stress

In deze aanval is een belangrijke rol weggelegd voor het stresselement: de medewerker is bezorgd en er wordt nu geld van je rekening gehaald. Stress dus, want dit vraagt om snelle actie! Het menselijk brein heeft twee manieren van informatieverwerking: beredeneerd gedrag en automatisch gedrag. Het eerste gaat over beslissingen die wij weloverwogen nemen, door rationeel verschillende argumenten af te wegen. Dit doen wij voornamelijk met belangrijke beslissingen. Omdat we echter niet de hele dag bezig kunnen zijn met het afwegen van alle argumenten voor alles wat we doen, handelen we ook deels op basis van automatisch gedrag. Dit zijn handelingen die we sneller doen, zonder zorgvuldige afwegingen. Wanneer we stress hebben, zullen we minder goed in staat zijn volledig te beredeneren wat we doen, en neigen we naar snellere acties. In dit geval gaan we sneller berusten op heuristieken.

Heuristieken

Heuristieken zijn simpele strategieën die mensen gebruiken om snel een oordeel te vormen. Door op een klein stukje informatie te focussen, trekt men gauw een conclusie en maakt men bijbehorende keuzes. In het geval van de telefoonbabbeltruc kunnen dat kleine stukjes informatie zijn op basis waarvan mensen snel (door de stress) beslissen dat ze geloven dat ze echt de bank aan de telefoon hebben. Bijvoorbeeld omdat de bankmedewerker een vrouw is, en

Inspelen op de emoties

wij de menselijke neiging hebben om vrouwen eerder te vertrouwen en ze dus minder snel als crimineel te zien. Of omdat ze zo goed Nederlands spreekt. Omdat het nummer dat in je scherm staat, daadwerkelijk het nummer van de alarmlijn van jouw bank is. Of omdat ze allemaal ingewikkelde woorden gebruikt die je alleen maar kent als je bij de bank werkt...

Legitimiteit

Doordat de beller zichzelf positioneert als bankmedewerker met verstand van zaken, word jij al snel in de positie van 'volger' gezet. De bank weet immers het beste wat je in deze situatie moet doen. Het is dan ook een zeer menselijke reactie om de expert de controle te geven en de adviezen van deze expert op te volgen. Oplichters zetten deze legitimiteit nog extra aan door allerlei moeilijke woorden te noemen; ze gaan je geld kluizen (dat werkwoord bestaat niet!), de fraudehelpdesk ziet transacties, ze zetten de protocollen in werking, ze stellen een veilige kluisrekening voor je open, etc. Nog meer reden om aan te nemen dat zij echt van de bank zijn en jou aan het helpen zijn…

Wederkerigheid

Doordat de bankmedewerker zo behulpzaam is en veel tijd voor je neemt, kan er bij jou een schuldgevoel ontstaan. Mensen hebben de natuurlijke neiging om iets terug te willen doen als iemand iets voor hen heeft gedaan. Voor je gevoel sta je dus al in het krijt bij de bankmedewerker. Ze zijn immers al een tijd alleen maar met jou en jouw rekening bezig, zelfs met meerdere mensen. Ze zijn tegelijkertijd transacties voor je aan het tegenhouden én ze stellen een kluisrekening beschikbaar. Als jou vervolgens gevraagd wordt aan een paar stappen mee te werken, ben je van nature geneigd dit te doen. Zij hebben immers al zoveel voor jou gedaan dat je het eigenlijk niet kunt maken om nu moeilijk te gaan doen…

Stress vraagt om snelle actie

Blijf alert en weet wat je moet doen

Het mag duidelijk zijn; oplichters spelen heel bewust in op deze menselijke mechanismes. Dat maakt ons dus allemaal kwetsbaar. Criminelen nemen de tijd, ze zijn vriendelijk en behulpzaam. Ondertussen zoeken ze rustig uit voor welke beïnvloedingsstrategie jij het meest kwetsbaar bent. Tenminste, als ze niet vooraf al een beeld over je hebben gevormd vanuit je social media en internet.

Als je nou zo'n telefoontje krijgt waardoor je tóch twijfelt, is het belangrijk te weten wat je moet doen. En vooral: daar niet vanaf te wijken! In dit geval: bel je bank zelf, op het bij jou bekende nummer. Vraag aan je bank of er daadwerkelijk problemen zijn met je rekening. Hoogstwaarschijnlijk niet, maar als het toch het geval is, weet je in ieder geval zeker dat je de juiste partij aan de telefoon hebt en kun je hun advies verder volgen. Dat zal overigens niet het overmaken van geld zijn… <

Wat is spoofing?

Spoofing is een truc waarmee een andere identiteit aangenomen wordt. Een bekend voorbeeld van spoofing is e-mailspoofing: er wordt een e-mail gestuurd en er staat dat deze afkomstig is van jouw e-mailadres of dat van de bank. Dit kan wanneer jouw e-mailserver niet veilig is geconfigureerd met bijvoorbeeld regels voor in het Sender Policy Framework (SPF). Een andere vorm van spoofing is telefoonnummerspoofing. Hierbij nemen de criminelen een ander telefoonnummer aan. Dit kan via verschillende trucs. Hierdoor krijg jij een ander nummer in je scherm te zien dan waar zij mee bellen. Doordat het nummer dat je ziet vertrouwd is, ben je wellicht sneller geneigd om mee te werken. Door spoofing is echter het juiste nummer in je beeldscherm dus geen garantie meer.