

# ● Criminelen zijn sneller dan wij! ●

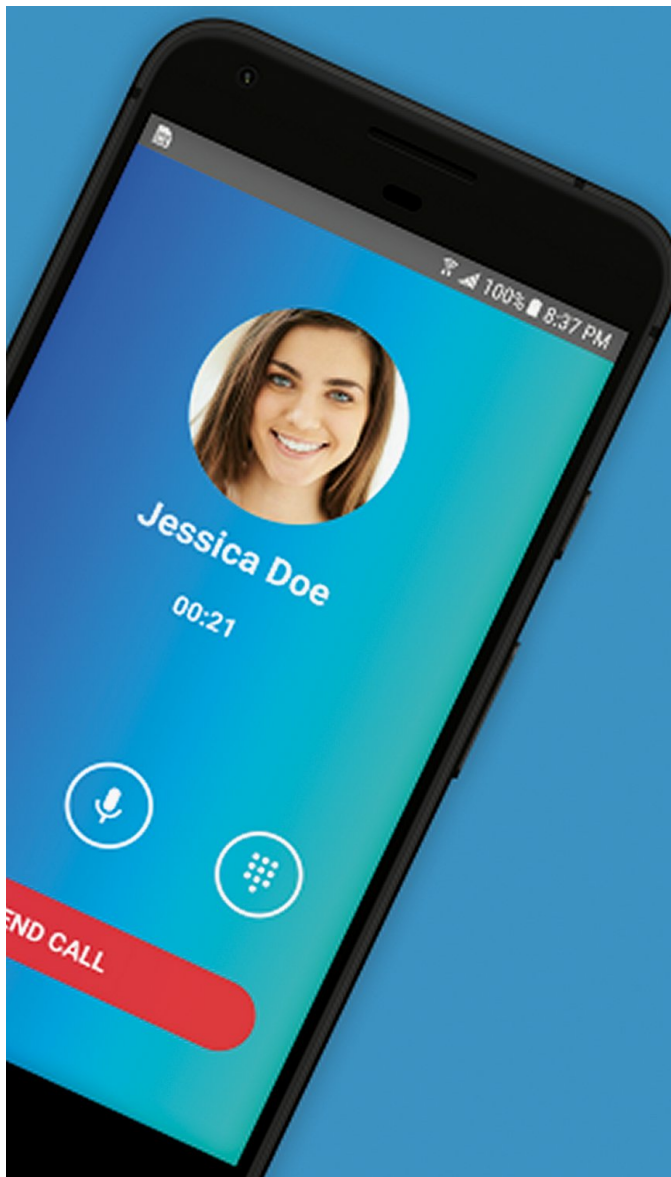
Ruud Uphoff

*We zijn intussen wel genoeg gewaarschuwd voor phishing mails. Nee, daar trappen we niet meer in. En om een bedrag over te kunnen maken, wordt tegenwoordig verificatie met je mobiel gedaan. Voortaan veilig dus? Nou en of! Voortaan zal het crapuul dus iets anders moeten bedenken, hier trappen we niet meer in. Goed nieuws dus?*

**Nou, niet echt.** ‘Iets anders bedenken’ is al lang gedaan hoor. Eigenlijk gaat het om mogelijkheden die al lang bestaan, maar het geboefte gebruikte die nog niet omdat eerdere gemakkelijkere methoden nog werkten.

## Welke waarde hechten we aan nummerherkenning?

Je mobiel begint een bekend deuntje te spelen en de foto van je zoon of dochter verschijnt. Maar bij opnemen klinkt de stem van iemand anders. ‘Niet schrikken, het is niet ernstig, maar uw dochter heeft een ongelukje gehad en ligt nu in het ziekenhuis, niet ernstig, maar ze mag een paar dagen niet praten en daarom heeft ze mij gevraagd even te bellen met haar telefoon...’



Het is echt haar nummer, dus dat moet vertrouwd zijn?

**Nou nee!** Vergeet dat maar! Er zijn nog steeds veel mensen die denken dat je aan nummerherkenning kunt zien wie er belt. Dat was zo in de dagen van de vaste lijn, helemaal onder beheer van KPN, maar tegenwoordig kan elke crimineel een centrale installeren. En dan bepaal je gewoon met welk nummer je uitbelt.

Daarvoor worden trouwens al apps voor Android aangeboden. Als APK-bestandje, dus nee, niet via de Play Store en nee, zeker niet door mij aanbevolen. Het is dat je maar weet waar je mee te maken hebt. Als je geld overmaakt zal de bank dat niet vergoeden. Er is geen sprake van een hack. Je hebt het helemaal zelf gedaan! Dus altijd zelf terugbellen naar ‘bekend nummer’.

Gebruikers van services zoals VoipBuster zullen zich herinneren dat het nummer, dat ze als ID wilden gebruiken, eerst werd geverifieerd. Netjes natuurlijk want ze staan niet toe dat u stoute dingen gaat doen. Ik had ooit vier vaste nummers, je weet wel, ISDN, maar daarvan heb ik er drie al in 2008 opgezegd. Ha, je snapt ‘m al! Met die nummers kan ik nog steeds uitbellen.

Hetzelfde geldt natuurlijk voor sms en WhatsApp: dat nummer zegt niets. Op z’n Vlaams: ‘Laat u niet doen hè!’

## Doorgeknijpte betaalpas of credit card ongeldig?

Een ander praktijkgeval is de e-mail van de bank die je vertelt dat je betaalpas is gekraakt. Of je die maar naar het in de mail genoemde adres wilt sturen. U krijgt een nieuwe pas met een nieuwe pincode. Graag voor het politieonderzoek de oude pincode met stift op de pas zetten, en natuurlijk niet vergeten de pas onbruikbaar te maken (met plaatje van doorgeknijpte pas). Dat laatste zorgt ervoor dat het helemaal OK lijkt. Weet de arme ziel veel? De chip in die doorgeknijpte pad doet het prima hoor!



Degene die dit overkwam was echt niet dom! Wat kon er nu gebeuren? Die mail kwam duidelijk van haar bank: [service@ing.nl](mailto:service@ing.nl); dus werd de schaar gepakt en het pasje met pincode aan het opgegeven adres verzonden.

Toch zat het haar achteraf niet lekker en daarom belde ze toch even met haar vriendin. Ze liet de pas toch door de bank blokkeren en één ding in de mail was juist: ze heeft nu inderdaad een nieuwe pas met een andere pincode.

## Het gezag van Internet? Weg er mee!

Het is eigenlijk ongelooflijk hoeveel waarde mensen hechten aan mededelingen uit totaal niet geverifieerde bronnen. 'Waar heb je dat vandaan?' 'Nou, het staat op internet, hè!' Mijn eerste kennismaking daarmee was ooit, jaren geleden, in een nieuwsgroep van XS4ALL. Bij het reageren op een artikel wist iemand mij te vertellen dat ik helemaal verkeerd omging met het citeren van tekst, het zogenaamde 'quoten'. Ik moest toch maar eens gaan leren hoe dat moest en hij was zo aardig mij een link te geven naar een site: 'Kijk, daar staat het!' Natuurlijk even gekeken, dat wel. En de brave borst gevraagd waaraan het persoonlijk meninkje van een zekere meneer X wetskracht ontleende.

Die vent heeft een echte boevenkop, dus sorry als ik hem niet vertrouw. Of het was toch echt een keurige dame, daar zoek je toch geen oplichtster achter? Het is ongelooflijk moeilijk totaal geen waarde te hechten aan het uiterlijk. Die mail van je bank die er toch helemaal echt uit ziet, en als je probeert 'm te beantwoorden, (b)lijkt ie wel degelijk van *service@ing.nl* te komen.

Jou een e-mail sturen met een willekeurig adres als afzender, bijvoorbeeld *service@ing.nl* is maar een koud kunstje. De enige manier om te achterhalen waar het vandaan komt, is in de header te kijken van welk IP-adres het afkomstig is.

Op de site van ARIN of onderliggend NCC (Network Coordination Center, hier voor Europa is dat Ripe NCC) kun je dan zien aan welke firma het betreffende sub-net is uitgereikt en dan kan oom agent met een briefje van de rechter naar de betreffende ISP om te vragen wie de stouterik was die oma haar spaarcentjes heeft afgetroggeld. Simpel? Ik vrees dat het internationaal wat ingewikkelder ligt. Het geboefte opereert meestal vanuit een omgeving waar justitieel onderzoek enig smeergeld vereist.

## Gemakkelijk gemaakt door Thunderbird

De software uit de stal van Mozilla hecht erg aan gebruikers-gemak, iets wat soms vloekt met veiligheid.

Wat wel mogelijk is, maar diep verstopt, is het klikken op links blokkeren. Er zijn twee instellingen, maar je kunt wel een belangrijke maatregel nemen:

- In Thunderbird: ga in het menu naar *Extra* → *Opties* → *Geavanceerd*.
- Klik onderaan op de knop *Configuratie-editor*.
- Wijzig achter *network.protocol-handler.external.default* de instelling *true* in *false*.

Deze instelling zorgt ervoor dat een klik op een link naar een website niet werkt. Wil je die link toch openen, omdat je de afzender volledig vertrouwt, klik er dan op met de rechter muisknop en kies voor *Koppelingslocatie kopiëren*. Ik hou ervan in Windows 10 de regel uitvoeren op de taakbalk vast te pinnen, zodat ik de URL daar meteen in kan plakken. Klinkt dom? Nou, deze extra handeling dwingt je nu juist tot het maken van een bewuste keuze, in plaats van per ongeluk op een malafide link klikken.

De regel *Uitvoeren* op de taakbalk zetten: klik met de rechter muisknop op *Start*, en kies *Uitvoeren*. Als het venster is verschenen klik je ook nog met de rechtermuisknop op het bijbehorend pictogram en kies je *Aan taakbalk vastmaken*.

En ik hoor het commentaar al: 'Je kunt ook gewoon op *Start* klikken of de zoekbalk (die ik weggedaan heb) gebruiken. Bezwaar? Als jij, de grote godheid over je computer, hebt besloten dat Firefox of Chrome of Brave, of welke dan ook, de standaard browser is, dan gelieve Microsoft dat te respecteren en dus niet tegen jouw wil Edge te starten.