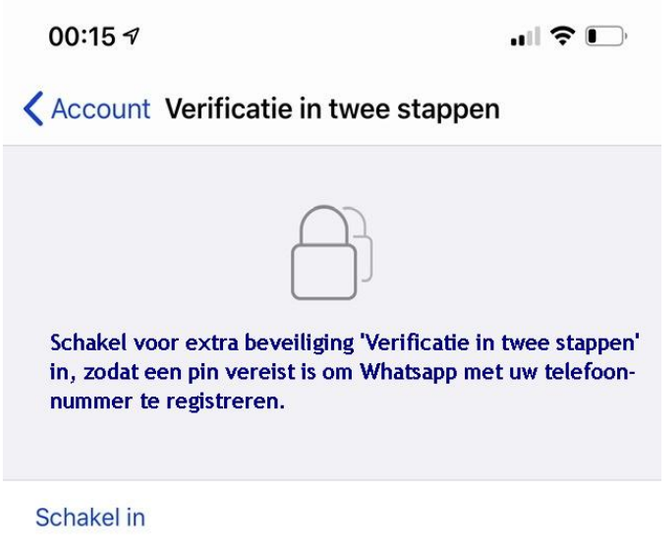
Voorkom online oplichting

Bert van Dijk

Enkele nuttige tips!

In een tijd waarin ook dieven niet graag besmet worden met corona en ook zij het ‘thuiswerken’ hebben ontdekt, zien we een enorme toename van online hulpvraagfraude. Over heel 2019 waren er 2.663 meldingen met in totaal 1 miljoen schade. In april en mei 2020 waren er al circa 3.000 slachtoffers, die bij elkaar meer dan 1 miljoen euro kwijtraakten. Omdat mensen het geld zelf overmaken, krijgen ze het niet terug van hun bank. Lees de volgende drie tips en voorkom dat je een slachtoffer van fraude wordt.

Opgepast! Nieuwe Whatsapp-fraude verspreidt zich als olievlek



Altijd terugbellen voordat je iemand helpt

Criminelen doen zich vaak voor als een familielid of vriend in nood met bijvoorbeeld autopech of een probleem in het buitenland als ze op social media hebben gezien dat die persoon op vakantie is. Ze hacken soms een WhatsApp-account. Als ze je account overnemen kunnen ze geen oude berichten lezen, maar wel zien ze met wie je contact hebt in groepsgesprekken. Daardoor kunnen ze zich bij veel mensen voor jou uitgeven en zo verspreidt deze hulpfraude zich als een olievlek. (Zie ook het filmpje op **https://youtu.be/poV3JJxUR7E**).

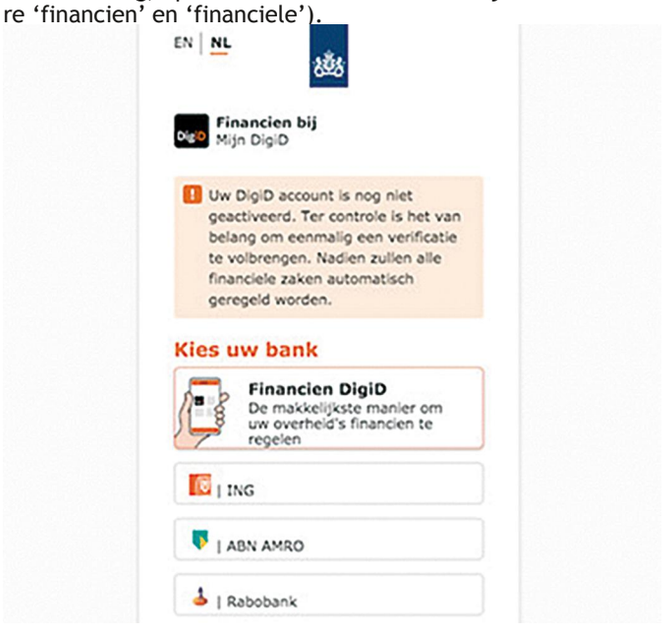
Dit voorkom je door:
a. verificatiecodes nooit door te sturen (om zogenaamd je mobiele nummer te verifiëren),
b. je voicemail te beveiligen met een code en
c. in de instellingen van WhatsApp bij Account te kiezen voor ‘Verificatie in twee stappen’.
Bij het installeren van WhatsApp op een ander toestel heb je, naast de verificatiecode uit het sms-bericht, ook de door jou ingestelde pincode nodig.
(Zie de afbeelding in de volgende kolom)

Tevens is de menukeuze Beveiliging boven de ‘Verificatie in twee stappen’ een aanrader. Als je daar ‘Toon beveiligingsmeldingen’ aanzet, krijg je een seintje als een contactpersoon WhatsApp op een nieuw toestel installeert. Als je snel daarna een hulpvraag krijgt, dan ben je alvast gewaarschuwd.

Ook maken fraudeurs soms een nepaccount met een foto die ze van je social media afhalen. Je moet ook oppassen als iemand je een nieuw telefoonnummer doorgeeft. Dit gebeurt dan vaak met een smoes dat zijn telefoon is gestolen. Na een tijdje krijg je dan wat berichten en een link om geld over te maken. Om het extra overtuigend over te laten komen bellen ze dan soms via WhatsApp en breken dan af voordat er opgenomen kan worden. Komt zo’n verzoek onverwacht of moet het snel, laat ze dan altijd naar jou bellen. Zo check je eenvoudig van wie dat verzoek echt komt.

Negeer onverwachte sms-berichten met linkjes

Pas vooral op bij sms-berichten die verzonden lijken te zijn door Apple of je bank. Voor boetes of belastingbetalingen en teruggaven worden geen linkjes verzonden. Een ander recent voorbeeld is een sms-nepbericht van DigiD: ‘Uw digitale sleutel voor toegang tot DigiD is nog niet geactiveerd. Activeer je digitale sleutel voor ...’
Een link brengt je naar een nagemaakte DigiD-site met allerlei links naar nagemaakte inlogpagina’s van tien banken (zie de afbeelding; opvallende taalfouten daarin zijn onder andere ‘financien’ en ‘financiele’).



De oplichters willen op deze manier zoveel mogelijk gegevens buitmaken voor hun kwa-lijke praktijken. Klik daarom nooit op links die je niet verwacht. Gebruik bij voorkeur de app van dat bedrijf of ga zelf naar hun website.

3. Neem zelf contact op met een bedrijf

Ook worden vaak mensen in een telefoongesprek bang gemaakt, met de bedoeling ze over te halen iets te installeren op de computer, of een QR-code te scannen met hun bank-app, waarmee de beller bij een bepaalde bank jouw bank-app op zijn toestel kan registreren, en zo snel veel geld weg kan boeken. Het komt zelfs voor dat het lijkt of men belt vanaf een officieel telefoonnummer van dat bedrijf.

Bedenk dat bedrijven nooit ongevraagd individuen bellen om iets te installeren of je geld in veiligheid te brengen. Als er iets bij-zonders is, vraag dan de naam van de persoon die jou belt en neem daarna zelf telefonisch contact op met dat bedrijf via het juiste telefoonnummer en vraag naar die persoon.

4. Tot slot

Toevoeging door de redactie van de SoftwareBus
Ga nooit in op verzoeken om een QR-code te scannen of geld over te maken via een link die je is toegestuurd vanaf een 'betrouwbare' bron, ook al gaat het maar om een cent. Gebruik bij bankieren via smartphone of pc altijd de tweetraps authenticatie, dus met wachtwoord (pincode) en je vingerafdruk of de identifier van de bank.

Zie ook het artikel '***Wat weet de browser (Edge, Chrome, FireFox) van jou?***' op de website van Rein de Jong over hoe je kunt nagaan wat betrouwbaar is:
https://www.reindejong.nl/.

Bert van Dijk verstuurt elke maand een iPhone- en iPad-tip-lijst via **apple.hcc.nl**