Phishing

In de vorige editie heeft het Meldpunt Ongebruikelijke Transacties (MOT) negatieve gevolgen voor de maatschappij die voortvloeien uit malafide praktijken van criminelen belicht. In deze editie gaat het MOT in op het fenomeen phishing . Met dit onderwerp is zij belandt op het terrein van de typologieën. Bij typologieën gaat het om trends waarbij methoden en technieken die door de crimineel zijn bedacht worden beschreven of uitgewerkt..

Money laundering is het verrichten van handelingen, waardoor een voor de wet verzwegen vermogensaanwas ogenschijnlijk een legale oorsprong krijgt. Met de voortschreidende technologische ontwikkelingen worden door de criminelen methoden en technieken bedacht om de nieuwe technologische producten te beheersen. Deze methoden en technieken die de criminelen toepassen worden pas duidelijk na observatie, analyse en onderzoek. Ingevolge artikel 11 van de Wet Identificatieplicht Dienstverleners dienen dienstverleners een adequaat beleid uit te voeren en te beschikken over adequate procedures die gericht zijn op de voorkoming van misbruik van nieuwe technologische ontwikkelingen en instrumenten ten behoeve van Money Laundering en Terrorisme Financiering.

Het is algemeen bekend dat zowel bonafide als malafide individuen dan wel groepen gebruik of misbruik maken van de technologische of communicatie systemen. Phishing is een oplichtingsmethode, waarbij misbruik wordt gemaakt van communicatie systemen (internet en mobiel). Degene die zich daaraan schuldig maken worden aangeduid als fraudeurs of oplichters.

Vormen van phishing via mobiel zijn: aanbiedingen, lotterij- en terugbelfraude en via internet is dat emailberichten.

Phishing via mobile zijn:

- **Aanbiedingen**

  Verschillende aanbiedingen worden via de telefoon gedaan . De variatie loopt van goedkope leningen tot een deelname aan een loterij. De oplichters laten geen ruimte om na te denken over het voorstel. Ze streven naar een positieve reactie en dat men meegaat met hun verhaal. Sommige fraudeurs verwijzen hun slachtoffers zelfs door naar websites, bijvoorbeeld met reviews van ‘tevreden klanten’. Die site en de klanten zijn waarschijnlijk net zo nep als de intenties van de fraudeurs.

- **Loterijfraude**

  Slachtoffers worden via hun mobiel op de hoogte gesteld van een gewonnen loterij prijs, terwijl zij nooit eerder hebben meegedaan aan een loterij. Door op dit bericht te reageren kunnen de oplichters toegang krijgen tot persoonlijke informatie van slachtoffers ten einde deze voor hun eigen doeleinden te gebruiken.

- **Terugbelfraude**

  Het slachtoffer ziet een gemiste oproep van een nummer dat niet bekend is. Hij belt terug. Het telefoontje komt echter van oplichters die via een auto-dialer duizenden telefoontjes naar willekeurige mobiele nummers plegen. Wanneer de telefoon één keer is overgegaan verbreken zij de verbinding, in de hoop dat er terug gebeld wordt. Indien het slachtoffer daartoe overgaat wordt zijn nummer door de fraudeur gebruikt om gesprekken te voeren waarvan de rekening door de service provider aan het slachtoffer wordt gepresenteerd.

Vormen van phishing via internet zijn:

- **Phishing via email**

  Het slachtoffer ontvangt een email waarin gevraagd wordt zijn account bij een bank te verifiëren en te bevestigen. Er volgt dan een email verzoek waarin er gevraagd wordt om persoonlijke (financiële) gegevens te verstrekken. De fraudeurs gebruiken deze informatie voor hun malversaties.

Wanneer fraudeurs ertoe overgaan het illegaal verkregen vermogen in de legale sfeer te brengen zijn zij bezig wit te wassen.

www.fraudehelpdesk.nl

www.politie.nl

www.veiligbankieren.nl

MOT (FIU Suriname)

E-mail: motsur@sr.net

Website: www.mot.sr