Presentatie Computer Vereniging Bollenstreek/Haarlemmermeer
Veiligheid, Randsomeware en andere vormen van oplichting

Phishing

Phishing is een vorm van fraude waarmee fraudeurs proberen om u persoonlijke informatie te ontfutselen. Met deze informatie kan fraude met internetbankieren, pinpassen, creditcards of uw identiteit worden gepleegd. Phishing is vaak gericht op een grote groep personen, maar kan ook specifiek op één persoon of een kleine groep zijn gericht. Hierbij wordt gebruik gemaakt van informatie die al van de persoon of groep bekend is, zoals het e-mailadres, de naam of de functie.
Voorbeelden van Phishing mails zijn bij alle banken beschikbaar. Zoals hier bij de ING https://www.ing.nl/de-ing/veilig-bankieren/herken-fraude-en-oplichterij/fraude-via-uwcomputer/bescherming-tegen-phishingberichten.html
En bij de Rabobank https://www.rabobank.nl/images/pdf_valse_email_versie_2015_29714425.pdf
En de ISC (International Card Services) https://www.icscards.nl/ics/info/overzicht-phishing-email

Werkwijze crimineel
Phishing gebeurt zowel **via internet, per telefoon als per e-mail**. Hierbij doet de crimineel zich voor als betrouwbare instantie. Zo kunt u een e-mail of een SMS krijgen die van uw bank afkomstig lijkt, met het verzoek om voor controle persoonlijke gegevens, zoals uw naam, adres, telefoonnummer, rekeningnummers en beveiligingscodes in te voeren op een website. De website lijkt echt, maar is volledig nagemaakt.
In sommige gevallen kan de crimineel met deze gegevens al misbruik maken van uw rekening. Ook kan u worden gevraagd een telefoonnummer te bellen, omdat anders uw rekening geblokkeerd wordt.
In andere gevallen kan de crimineel met de verkregen informatie u later bellen en zich voordoen als bankmedewerker. Hij of zij vraagt dan bijvoorbeeld om uw beveiligingscodes, omdat er problemen zouden zijn met uw rekening en de medewerker wil controleren of alles in orde is.

Wat doet de bank?

Om phishing tegen te gaan, proberen banken phishingmails en -websites te traceren en deze websites zo snel mogelijk uit de lucht te halen. Daarnaast zal uw bank u zo goed mogelijk informeren en waarschuwen voor grote phishingaanvallen.
Uw bank vraagt u **nooit** per telefoon (e-mail of SMS) om:

- Uw verificatiecode voor internetbankieren of bankieren via de bank app.
- Uw pincode
- Uw creditcardnummer, CVC-code of geldigheidsdatum van uw creditcard.
- In te loggen op internetbankieren.
- Een update van internetbankieren, een nieuwe website te testen of de veiligheid van uw computer te testen.
- Uw betaalpas of inlogapparaat naar uw bank terug te sturen. U krijgt automatisch een nieuwe betaalpas toegestuurd. Uw oude pas moet u doorknippen door de chip en door de strip en kunt u vervolgens gewoon weggooien. Krijgt u zo'n verzoek? Ga hier dan niet op in, maar meld het bij uw bank. Twijfelt u aan de echtheid van een e-mail? Bel uw bank via het nummer dat bij u bekend is en vraag het de medewerker.
- Klik niet op een link in de e-mail.
- Stuur de e-mail door naar het meldpunt van de bank die geïmiteerd wordt.
- Verwijder de e-mail.

Heeft u toch op een link in een e-mail geklikt? Bel dan uw bank via het nummer dat u bekend is en vertel de medewerker wat er precies is gebeurd.

Wat kunt u doen?

Wees u ervan bewust dat criminelen op uw gegevens uit kunnen zijn. Wees altijd heel kritisch voor u (persoonlijke) gegevens afgeeft. Weet wat alarmbellen zijn om phishing mails te herkennen (zie hieronder). Bedenk dat uw bank u nooit zal vragen om beveiligingscodes op onverwachte momenten of plekken, dus nooit per e-mail en nooit per telefoon. U kunt valse e-mails melden bij de bank die geïmiteerd wordt. Zo draagt u bij aan veilig bankieren.

U kunt ook de Fraudehelpdesk raadplegen https://www.ing.nl/de-ing/veiligbankieren/herken-fraude-en-oplichterij/fraude-via-uw-computer/bescherming-tegen-phishingberichten.html
Daarnaast is het verstandig gebruik te maken van een spamfilter. E-mails waarover u twijfelt moet u meteen verwijderen. Heeft u onverhoopt toch persoonlijke gegevens gegeven aan een phisher of stuit u op onverwachte zaken bij het internetbankieren? Meld dit dan direct bij uw bank.

Zo kunt u phishing onder andere herkennen

- Het is een onverwachte e-mail. Zogenaamd verzonden door:
- uw eigen bank
- een andere bank
- Een betaalmethode zoals iDEAL
- CJIB, Belastingdienst Betaalvereniging Nederland of andere organisatie
- De e-mail is niet aan u persoonlijk gericht, bijvoorbeeld “Geachte klant”. Is de e-mail wel persoonlijk naar u gericht, dan kan het alsnog phishing betreffen.
- Kijk naar de afzender van de mail (bovenin de mail). Staat er na ‘@’ wel de juiste naam van uw bank, dus de naam van de site waar u altijd op inlogt? Dus bijvoorbeeld abnamro.nl, rabobank.nl of ing.nl? Nee? Stuur de mail door naar de bank die wordt geïmiteerd en gooi direct daarna de valse e-mail weg.
- Kijk ook naar het daadwerkelijk e-mailadres van de afzender. Dit kunt u bekijken door met muis op het e-mailadres te gaan staan zonder er op te klikken. Is het e-mailadres niet logisch? Dan gaat het waarschijnlijk om een valse e-mail.
- (Soms) zijn het slecht geschreven e-mails. Denk aan slechtlopende zinnen en spel- en grammaticafouten of woorden in een andere taal.
- De aanleiding van de e-mail is meestal een actueel onderwerp, bijvoorbeeld het aanvragen van een nieuwe betaalpas waarmee u contactloos kunt betalen.
- Door paniek te zaaien hopen criminelen dat u impulsief reageert en de door hen gewenste informatie verstrekt.
- In de e-mail vraagt de beveiligingsafdeling van bijvoorbeeld uw bank of Betaalvereniging Nederland u iets te doen.

- Er wordt gevraagd naar beveiligingscodes en/of persoonlijke gegevens.
- Het gaat vaak om een dringend verzoek. Er wordt gedreigd met gevolgen als u niet direct reageert. Bijvoorbeeld: als u voor een bepaalde datum een nieuwe betaalpas aanvraagt dan betaalt u niets, anders moet u wel voor de pas betalen.
- U wordt gevraagd op een link te klikken naar een vreemde website. Of u wordt geleid naar een website die bedrieglijk veel op het origineel lijkt. Als u met uw muis op het webadres gaat staan, kunt u meestal ergens in uw scherm het webadres zien waar de link naar verwijst. Kijk kritisch naar dit webadres, klik liever niet op de link. Soms is er maar een kleine onopvallende fout. www.bedrijv.nl of bijvoorbeeld www.bedrijf.net in plaats van www.bedrijf.nl. Wanneer u twijfelt of de e-mail echt van uw bank komt: Bel uw bank!

- Uw mail provider of spamfilter heeft een indicatie van ‘spam’ gegeven.
- In plaats van mailtjes met tekst, versturen de internetcriminelen de phishing mails vaak met plaatjes met tekst. Dit wordt gedaan om spamfilters te omzeilen. Deze mails zijn te herkennen doordat u de tekst (afzonderlijke woorden) niet kunt selecteren met de muis.
- Uw bank stuurt u hoogst zelden mails voorzien van bijlagen. Ontvangt u dan ook een mail met bijlagen zogenaamd van uw bank, open deze dan niet en zeker geen bijlagen met de extensie ‘*.exe’*.

Zelf goed opletten blijft altijd belangrijk. Bij twijfel: Bel uw bank!

Let op!
Internetcriminelen bellen u ook op om pincodes en inlogcodes te achterhalen. Deze criminelen kunnen zich aan de telefoon voordoen als een bankmedewerker die uw gegevens wil controleren, bijvoorbeeld omdat er problemen zijn met uw rekening. Ook hier geldt: uw bank vraagt u nooit naar beveiligingscodes via de telefoon of e-mail. Houd uw beveiligingscodes voor u zelf. **Neptelefoontjes. Daar trapt u ook niet in.**

Bent u slachtoffer van phishing? Twee zaken zijn het belangrijkst:

- Informeer direct uw bank en/of creditcardmaatschappij en volg de aanwijzingen van de bankmedewerker.
- Meld de fraude bij de politie via telefoonnummer 0900-8844 (lokaal tarief).

Presentatie Computer Vereniging Bollenstreek/Haarlemmermeer
Veiligheid, Randsomeware en andere vormen van oplichting

Mails met malware

Deze e-mails bevatten een bijlage of een link waarmee, meestal met slechts één muisklik, schadelijke software op de computer gedownload en geïnstalleerd kan worden. Van deze malware zijn verschillende varianten die vaak voorkomen: spyware, ransomware en cryptoware.
Malware is een verzamelnaam voor software die vervelende dingen met je pc of telefoon doet, zoals een virus, wormen en Trojaanse paarden. Maar ook software die ongevraagd advertenties injecteert op uw computer en verder in principe geen negatieve gevolgen heeft, wordt bestempeld als malware.

Spyware

Spyware is software die (onopgemerkt) op een computer wordt geïnstalleerd, gegevens over de gebruiker verzamelt en doorstuurt naar een externe partij. Alles wat u op uw computer kunt zien, kan de crimineel ook zien. Zij kunnen zelfs volgen welke toetsen u gebruikt. Dus ook al ziet u ****** op de plek van uw wachtwoord. Doordat u het wachtwoord in heeft getypt komt de crimineel toch in het bezit van uw wachtwoord.

Als extra veiligheid kunt u, voor het inloggen ook het schermtoetsenbord gebruiken.

Ransomware/Cryptoware

Deze varianten van malware gijzelen en versleutelen uw bestanden. U kunt hierdoor niet meer bij uw bestanden. Criminelen vragen geld, vaak in de vorm van bitcoins, in ruil voor het vrijgeven van uw bestanden. Betaal niet! U weet namelijk niet of de bestanden na betaling daadwerkelijk worden vrijgegeven. Neem contact op met een deskundige om de ransomware/cryptoware te verwijderen en uw computer te herstellen. De experts van de club kunnen u hierbij helpen.

Misleidende e-mails

Heeft u een prijs gewonnen zonder dat u meedeed aan een wedstrijd? Grote kans dat u een misleidende e-mail heeft ontvangen. Veel namen van bestaande bedrijven worden voor de e-mails misbruikt. In werkelijkheid heeft u niets gewonnen. De crimineel probeert uw gegevens te ontfutselen en te misbruiken. U zit bijvoorbeeld vast aan een duur SMS-abonnement of u moet een duur telefoongesprek voeren. De bedrijven die achter deze e-mails zitten, bedenken steeds weer wat nieuws waardoor het lastig is deze misleiding te stoppen.
Zit u vast aan zo'n SMS-abonnement? Ga dan naar payinfo.nl en vul hier uw telefoonnummer in. Hiermee wordt het abonnement stopgezet.

Identiteitsfraude

Identiteitsfraude is frauderen door iemands identiteit over te nemen. In uw naam shopt de crimineel bijvoorbeeld online. Hij krijgt de spullen, u krijgt de rekening.
Bij identiteitsfraude misbruiken criminelen persoonlijke gegevens die ze bemachtigen via een online advertentie, social engineering of met een phishing e-mail. Hiermee worden bijvoorbeeld bankrekeningen geopend op uw naam, waarnaar crimineel geld kan worden doorgesluisd. Of de crimineel gebruikt uw gegevens om bijvoorbeeld aankopen op krediet te doen.
Gelukkig nemen veel organisaties maatregelen tegen identiteitsfraude. De banken werken bijvoorbeeld aan een nieuwe online identificatiedienst genaamd iDIN, waarmee u met de veilig en vertrouwde inlogmiddelen van uw eigen bank uzelf bekend kunt maken bij overheidsinstanties, verzekeringsmaatschappijen of webwinkels. Naar verwachting is deze nieuwe dienst vanaf 2016 beschikbaar voor instellingen en consumenten.
U kunt zelf ook veel doen om identiteitsfraude te voorkomen. Lees dat hieronder onder de kop "Wat kunt u doen?" https://www.veiligbankieren.nl/fraude/identiteitsfraude/

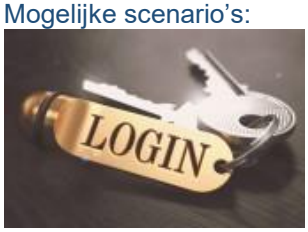
Bent u slachtoffer van identiteitsfraude of is er door de overheid een fout gemaakt met uw identiteit, meld dit dan altijd bij het Centraal Meldpunt Identiteitsfraude en -fouten (CMI) en vraag hen om hulp. In de folder Geef oplichters geen kans: een veilig ID staan de vormen van identiteitsfraude en hoe u uw schade kunt beperken.

Werkwijze crimineel

Criminelen verdiepen zich in de werkwijze die bedrijven en individuen hanteren om de identiteit van klanten vast te stellen. Zij proberen deze werkwijze te manipuleren of te misbruiken door gebruik te maken van informatie van klanten en/of valse identiteitsbewijzen.

- Diefstal van gegevens en documenten. Uit uw huis, tas, of waar u het in bewaring geeft, uit uw brievenbus, computer of mobiele telefoon.
- U wordt verleidt tot het delen van gegevens. Via phishing e-mails, online advertenties of babbeltruc aan de telefoon of aan de deur. In sommige gevallen kunt u verleidt worden om een kopie van een geldig legitimatiebewijs toe te sturen.
- De oplichter vindt uw gegevens. In slecht beveiligde administraties, in uw afval of via het internet en sociale media.

Mogelijke scenario's:



- De crimineel opent rekeningen op uw naam met de bedoeling betalingen te ontvangen voor zogenaamde verkopen via advertenties op websites en internetforums. Lees meer over identiteitsfraude via advertenties
- De crimineel opent rekeningen op uw naam met de bedoeling om schulden aan te gaan op uw naam.
- De crimineel fingeert uw verhuizing. Zo probeert hij van u als rekeninghouder aan uw beveiligingscodes en authenticatiemiddelen (wachtwoord, DigiD, bankpassen etc.) te komen.
- De crimineel vraagt uit uw naam een vervangend authenticatiemiddel en/of beveiligingscode aan en 'hengelt deze vervolgens uit de brievenbus'.

- De crimineel doet bestellingen bij webwinkels uit uw naam.
- Uw identiteitsbewijs komt op de zwarte markt. Een oplichter kan daar een identiteitsbewijs kopen van iemand die op hem lijkt. Bij identiteitscontroles kan deze 'lookalike fraude' moeilijk te herkennen zijn.
- Naast zaken rond veilig bankieren, zijn er ook andere gebieden waar de crimineel uw identiteit kan misbruiken. U leest hierover in de folder Geef oplichters geen kans: een veilig ID.

Wat doet de bank?

In de strijd tegen identiteitsfraude doen banken het volgende:

- Bij het openen van een rekening wordt gevraagd om een geldig identiteitsbewijs en wordt nagegaan of deze als gestolen is gerapporteerd.
- Beveiligingsmiddelen en -codes zoals passen, pincodes en wachtwoorden worden los van elkaar opgestuurd of moeten persoonlijk worden afgehaald.
- Van transacties en wijzigingen in persoonlijke informatie wordt vaak een bevestiging gestuurd die de klant kan controleren.
- Banken informeren u zo goed mogelijk over identiteitsfraude en waarschuwen u voor actuele aanvallen via de bankenwebsite.

Wat kunt u doen?

Er is een aantal zaken waar u op kunt letten om identiteitsfraude te voorkomen:

- Oplichters zijn meesters in het winnen van uw vertrouwen. Lees hierover in de folder Geef oplichters geen kans: een veilig ID. Trap niet in babbeltrucs aan de telefoon of aan de deur, wees alert bij online advertenties en e-mails waarin u op links moet drukken. Bij twijfel of uw bank de afzender van een bericht is, kunt u altijd eerst uw bank bellen.
- Ga zorgvuldig om met uw identiteitsbewijzen. Geef geen identiteitsbewijzen of kopieën aan mensen of partijen die u niet kent of niet vertrouwt. U kunt uw identiteitsbewijs ook versleuteld en met watermerk toesturen. Gebruik daarvoor de KopieID app van de Overheid.

- Zorg dat uw brievenbus goed is beveiligd. Het moet niet mogelijk zijn eenvoudig informatie uit uw brievenbus te vissen. Denk hierbij aan een door de oplichter aangevraagde nieuwe betaalpas op uw naam, aan brieven van de Belastingdienst, loonstrookjes, jaaropgaven of verzekeringspapieren.
- Zorg dat iemand uw brievenbus leegt als u langere tijd niet thuis bent.
- Sla alarm als een beveiligingsmiddel en/of beveiligingscode niet aankomt.
- Klik in e-mails nooit op een link naar een inlogpagina. Surf zelf naar het juiste webadres. De pagina waar de link naar verwijst kan een namaak website van de crimineel zijn.
- Beveilig uw digitale accounts zoals DigiD, iDIN of social media met twee-staps-authenticatie: u ontvang dan een extra controle per sms of u genereert deze code met een app. Een oplichter kan dan niets beginnen zonder uw telefoon, tablet of computer.

- Controleer regelmatig uw persoonlijke gegevens en transacties op al uw rekeningen.
- Meld verlies of diefstal van bankpassen, creditcards e.d. direct bij uw bank.
- Meld verlies of diefstal van uw identiteitsbewijs direct bij de politie en uw gemeente.
- Alarmeer uw bank bij vreemde transacties en fouten in persoonlijke gegevens.

Enkele veel voorkomende aanwijzingen van identiteitsfraude:

- Er is persoonlijke informatie gewijzigd zonder dat u hiervoor opdracht gegeven heeft.
- U kunt geen geld meer opnemen.
- Er staan transacties op uw rekeningafschrift waarvoor u geen opdracht gegeven hebt.
- U kunt niet meer inloggen op internetbankieren.

Bent u slachtoffer van identiteitsfraude?

- Meld de identiteitsfraude bij uw bank.
- Meld de identiteitsfraude bij het Centraal Meldpunt Identiteitsfraude van de Rijksoverheid.
- Neem contact op met de betrokken instanties.
- Leg een logboek aan van de gebeurtenissen en bewaar alle relevantie correspondentie. Verzamel zoveel mogelijk bewijs waaruit blijkt dat er sprake is van identiteitsfraude. Denk hierbij aan kopieën van bankafschriften, brieven van incassobureaus of aanvragen van abonnementen.
- Vermoedt u (als slachtoffer of getuige van) een strafbaar feit, dan kunt u aangifte doen bij de politie. Neem zoveel mogelijk documenten mee om uw verhaal te ondersteunen. Zonder aangifte kan de politie geen opsporingsonderzoek instellen en zonder aangifte kunt u de schade niet op de dader of de verzekering verhalen.
- Wijzig wachtwoorden van uw accounts regelmatig. Gebruik sterke en verschillende wachtwoorden. Een sterk wachtwoord is lang en bestaat uit een combinatie van gewone letters en cijfers, kapitalen en bijzondere leestekens. Dit kan ook een korte zin zijn.
- Als er op uw naam een profiel is aangemaakt op Facebook, andere sociale media of Marktplaats, dien dan bij betreffende organisatie het verzoek in om dit profiel te laten verwijderen.
- Overweeg of het in uw situatie verstandig is om uw privé en/of zakelijke contacten te informeren dat u slachtoffer bent van identiteitsfraude.

Phishing via de telefoon

Wordt u gebeld door uw bank, of door een medewerker van bijvoorbeeld Microsoft? Wees alert! Er is een mogelijkheid dat u een oplichter aan de lijn heeft. Vertrouwd u het niet? Bel dan zelf terug. Bel niet het nummer dat u van de beller krijgt of dat u in het display van uw telefoon ziet, maar zoek zelf het telefoonnummer op via de website van de organisatie. De algemene telefoonnummers van de banken staan ook op www.veiligbankieren.nl.
Geef nooit uw pincode of inlogcodes. Banken vragen daar nooit om.

Telefonisch

Criminelen bellen u op en zeggen dat zij voor uw bank werken. Ze spreken u persoonlijk aan zodat het lijkt alsof ze u kennen. Ook proberen ze op uw gevoel in te spelen door bijvoorbeeld aan te geven dat weten dat u uw inlogcodes niet mag geven. Vervolgens leggen ze u uit waarom u aan hen wél uw inlogcodes kunt geven. Soms vragen criminelen u om naar een website te gaan waar u zelf uw inlogcode in moet toetsen. Doe dit nooit! En hang direct op.
Uw bank vraagt u **nooit** per telefoon (e-mail, WhatsApp of SMS) om:

- Uw verificatiecode voor internetbankieren of bankieren via de bank app.
- Uw pincode
- Uw creditcardnummer, CVC-code of geldigheidsdatum van uw creditcard.
- In te loggen op internetbankieren.
- Via een link naar een nieuwe website te gaan.
- Een update van internetbankieren, een nieuwe website te testen of de veiligheid van uw computer te testen.

- Uw betaalpas naar uw bank terug te sturen. U krijgt automatisch een nieuwe betaalpas toegestuurd. Uw oude pas moet u doorknippen door de chip en door de strip en kunt u vervolgens gewoon weggooien.

Twijfelt u of u echt een medewerker van uw bank aan de telefoon heeft? Noteer dan de naam van de medewerker en hang op. Bel uw bank via het nummer dat bij u bekend is en vraag naar deze medewerker.
Heeft u uw inlogcodes telefonisch doorgegeven? Meld het direct bij uw bank en volg de instructies van de medewerker op.

E-mail, WhatsApp, SMS

Naast de traditionele e-mails worden ook mensen per WhatsApp of per SMS benaderd, met als doel om de verificatiecodes van internetbankieren te ontvreemden.

Werkwijze crimineel

- U ontvangt een WhatsApp bericht of SMS met een oproep om een beveiligingsupdate voor internetbankieren te installeren. U moet hiervoor de gebruikersnaam en wachtwoord invoeren. In werkelijkheid wordt een virus op de mobiele telefoon geïnstalleerd, wat alle SMS-berichten doorstuurt.
- U wordt benaderd in verband met een geplaatste advertentie op bijvoorbeeld Marktplaats of advertentiesites. Het kan ook andersom, als u biedt op een (valse) advertentie. Met een op het eerste gezicht overtuigend verhaal wordt gevraagd om:
  - allerlei gegevens af te geven, waarmee de fraudeur toegang tot internetbankieren of mobiel bankieren krijgt.
  - een betaling te doen van € 0,01 via een valse betaallink. Hiermee ontvreemd een crimineel de inloggegevens van internetbankieren.
    Let op: Niet iedere betaallink is vals. Consumenten kunnen een betaallink ontvangen van ondernemers én van consumenten. Ook WhatsApp mag gebruikt worden voor echte betaallinks. Controleer de betaalpagina goed.
- U ontvangt een WhatsApp bericht of SMS met de melding dat er een blokkade op uw mobiel bankieren app zit. Achter de phishing-link zit een pagina waarop wordt gevraagd om gebruikersnaam en wachtwoord. Gevolgd door een instructie om de zogenaamde update te installeren. Dit betreft in werkelijkheid een valse app die al uw SMS-berichten doorstuurt naar de fraudeur.

Wat kunt u doen?

- Installeer geen apps op uw telefoon die zogenaamd van een bank zijn. De apps van banken worden alleen via Google Playstore, Apple Appstore of Windows Store aangeboden.
- Bescherm uw codes: vul uw gebruikersnaam en wachtwoord voor internetbankieren alleen in op de pagina van uw bank. Klik nooit op een link in e-mail, WhatsApp of SMS om op deze pagina te komen, maar type zelf het internetadres van uw bank in uw browser en klik bovenin op ‘Inloggen’. Of gebruik de bank app.
- Wanneer u koopt of verkoopt op Internet (bv via een advertentiesite) en geld wil overmaken of ontvangen van een (ver)koper, dan is alleen het IBAN-nummer van de ontvanger nodig voor de persoon die wil betalen. Wanneer u om andere gegevens gevraagd wordt, kan het zijn dat u wordt opgelicht.

- Stuur nooit een foto van uw betaalpas of identiteitsbewijs naar andere personen of instellingen. U leest hierover in de folder Geef oplichters geen kans: een veilig ID.
- Bij twijfel: bel uw bank.

Microsoft scam Werkwijze crimineel
Wanneer u wordt gebeld door een Microsoft medewerker, dan zal hij u willen overtuigen dat u een probleem met uw computer heeft. De medewerker zal aandringen op snelle maatregelen om het bestaande probleem te verhelpen en grote(re) problemen te voorkomen. Daarvoor zijn wel wat aanpassingen op uw computer nodig. De beller is snel bereid om tegen betaling de zogenaamde problemen te verhelpen:

- uw virusscanner is niet up-to-date
- uw computer bevat een virus
- uw computer is gehackt
- uw Microsoft-software is niet up-to-date
- uw Microsoft-licentie is verlopen
- via uw computer zou er naar kinderporno gekeken worden
- u heeft nog geen recente Windows Upgrade

Hier is sprake van oplichting / phishing. De beller is op uw geld uit en wil u ertoe verleiden om tegen betaling onveilige software (een virus) op uw pc te installeren. Hiermee krijgt de crimineel toegang tot uw pc en uw bestanden. Daarnaast wordt het bedrag dat u voor de telefonische hulp moet betalen tijden het betaalproces bijna altijd (ongemerkt) verhoogd. Hier komt u vaak pas later achter wanneer u onraad ruikt of uw bankafschrift onder ogen krijgt.

Luister naar een voorbeeld van een gesprek van deze vorm van oplichting.

Slachtoffers lijken willekeurig te worden gekozen. Cybercriminelen maken gebruik van telefoonboeken en/of databases waar uw gegevens in zijn opgenomen. Meer informatie leest op de website van de politie.
Wat kunt u doen?

- Installeer geen illegale software op uw telefoon of computer.
- Houdt uw telefoon en computer up-to-date met behulp van updates en patches.
- Maak gebruik van een antivirusprogramma en een firewall.

Microsoft zal u nooit bellen met informatie omtrent de veiligheid van uw computer en of de wel/niet verlooptijd van uw Microsoft-licentie. Microsoft zal ook nooit naar uw beveiligingsinstellingen en/of wachtwoorden vragen. Verbreek daarom direct de verbinding. Schrijf zo mogelijk namen en het telefoonnummer op waarmee de oplichter naar u heeft gebeld. De oplichter is afhankelijk van de toegang tot uw pc. Als u niet inlogt en niets installeert, kan hij niets doen.

Mobiele malware

Mobiele apparaten zoals smartphones en tablets zijn inmiddels diep geworteld in ons dagelijkse leven. Door de hoge populariteit van deze apparaten, is de interesse van cybercriminelen ook toegenomen. Tot nu toe zijn de mobiele apps van de banken veilig. Het risico van mobiele malware is echter wel reëel. Hackers kunnen gevoelige informatie stelen, de apparaten inzetten als botnetwerk en activiteiten van de gebruiker volgen. Helaas realiseren de meeste mensen zich niet wat het belang is van het beschermen van hun mobiele apparaten tegen dergelijke aanvallen.

Meer informatie vindt u in de verschillende infographics.
Bovenstaande materialen maken onderdeel uit van een internationale campagne van Europol. In Nederland wordt de campagne ondersteund door de Nationale Politie, Alert Online en Betaalvereniging Nederland.

Social Engineering

Social engineering is het misbruiken van menselijke eigenschappen zoals nieuwsgierigheid, vertrouwen, hebzucht, angst en onwetendheid. Social engineering is zo oud als de mensheid en kent vele vormen.

Werkwijze crimineel
Criminelen proberen vertrouwelijke informatie van u te verkrijgen. Zij proberen u een bepaalde handeling te laten verrichten, zoals het afgeven

van persoonlijke gegevens (phishing), beveiligingscodes of creditcardgegevens of het installeren van malware.

Voorbeelden van social engineering zijn:

- Iemand biedt concertkaarten te koop aan op internet en deze wilt u graag hebben. Deze verkoper wil graag zeker weten dat u betaalt en en vraagt daarom ter controle een kopie van een geldig legitimatiebewijs per e-mail te sturen en een symbolisch bedrag over te maken. Lees meer

Shouldering

Pinnen. Het bestaat pas 25 jaar en toch is het niet meer weg te denken uit ons dagelijks leven. Sinds 1990 toetsten we ruim 30 miljard keer onze pincode in op een betaalautomaat. De manier waarop we de pincode intoetsen is daardoor een ingesloten gewoonte geworden. Doordat we ons zeer veilig voelen tijdens het afrekenen of bij een geldopname staan we er niet meer bij stil dat we het intoetsen van de pincode moeten afschermen.
Voor criminelen is het een kwestie van geduld tot ze zien hoe we onze pincode intoetsen. Ze proberen bij de kassa mee te kijken, of staan vlak achter u bij een geldautomaat. Met alleen een pincode kunnen criminelen niets. Toch worden ieder jaar duizenden mensen slachtoffer van deze vorm van fraude. Criminelen weten precies hoe zij uw betaalpas te pakken moeten krijgen. Zij halen direct geld van uw rekening. Het leed is al geschied nog voordat u merkt dat uw betaalpas weg is. Hoewel de Nederlandse banken de schade bij shouldering meestal vergoeden, is voorkomen van fraude altijd beter dan genezen.

- Zorg dat anderen niet mee kunnen kijken als u uw pincode intoetst.
- Gebruik uw vrije hand of portemonnee om het intoetsen van de pincode af te schermen.
- Staat iemand te dicht achter u, vraag dan om meer privacy.
- Laat u niet afleiden. Een crimineel heeft maar kort de tijd nodig om uw betaalpas om te wisselen.
- Bewaar uw betaalpas op een veilige plaats.
- Geef uw pincode nooit aan een ander.
- Meld verlies of diefstal van uw betaalpas onmiddellijk bij uw bank.
- Meld onveilige omstandigheden bij een betaalautomaat. Landelijk meldpunt: (088) 385 65 55.

Voorkom dat anderen met u mee kunnen kijken: houd uw pin privé.

Bankrekeningfraude

Steeds meer jongeren worden slachtoffer van criminelen die via de bankrekeningen van deze jongeren geld witwassen. Met een financiële beloning in het vooruitzicht geven de scholieren toestemming grote bedragen tijdelijk op hun rekening te zetten. De geldezel sluist hierbij frauduleus verkregen geld door naar criminelen. Door gebruik van zo'n 'tussenstation' is de identiteit van de crimineel moeilijker te achterhalen.
Zodra de bank merkt dat de jongere als geldezel is ingezet, moet het slachtoffer (geldezel) het vaak alweer verdwenen geld terugbetalen. Met een enorme schuld tot gevolg. Ook hangt de jongere een zware straf boven het hoofd wegens fraude.

Wat gebeurt er als een jongere op fraude wordt betrapt?

De gevolgen voor de jongeren en hun ouders zijn ingrijpend. De pakkans vanuit de banken is namelijk ontzettend hoog. De jongeren draaien op voor de schade, die vaak oploopt tot duizenden euro's. Ook worden de jongeren strafrechterlijk vervolgd. Met als gevolg: een forse schuld met bijbehorende afbetalingsregeling en een strafblad. Verder kunnen deze jongeren acht jaar lang geen gebruik maken van de financiële diensten van banken. Ze kunnen dan bijvoorbeeld geen lening afsluiten of een nieuwe rekening openen. Dat laatste is bijvoorbeeld lastig als de jongeren geld gaan verdienen en hun werkgever het salaris niet kan overmaken.

Schadelijke software

Schadelijke software (malware; malicious software) staat voor een veelheid aan vormen van vijandige, schadelijke of irritante software. Malware kan de computer binnenkomen via e-mail, afbeeldingen, of links op websites, USB-sticks, etc. Criminelen ontwerpen speciale software die op een computer komt zonder dat de eigenaar dat merkt, laat staan daar toestemming voor geeft. De malware stelt criminelen in staat om met u mee te kijken en dingen op uw computer te veranderen. Het komt zelfs voor dat criminelen uw hele computer blokkeren. De crimineel wil dat u betaalt om hem uw computer weer op te laten schonen. In dit geval spreken we over ransomware. Betaal geen boetes of herstelkosten, dat heeft vaak geen zin. Doe aangifte en laat uw computer opschonen door een expert.

Werkwijze crimineel

Een computer kan op diverse manieren besmet raken. De meest voorkomende wijze van besmetting verloopt via besmette hyperlinks of attachments in valse e-mails. Slachtoffers die deze mails openen besmetten op deze manier ongewild hun eigen computer. Een andere manier die criminelen inzetten is het omleiden van gebruikers naar een gehackte website, advertentie of pop-up. De gehackte pagina zoekt vervolgens naar zwakheden in de software van het slachtoffer. Hier merkt de gebruiker in eerste instantie niets van. Veelgebruikte zwakheden zitten in Java, Flash en PDF. Tot slot wordt er gebruik gemaakt van botnets. Dit betekent dat cryptoware verspreid wordt via de malware die zich reeds op de computer van het slachtoffer bevindt.

Malware

Bij internetbankieren gebruiken criminelen malware vooral voor het beïnvloeden van normale processen en het stelen van informatie.
Malware kan de routes die u op internet aflegt zo veranderen dat u terechtkomt op de servers van criminelen. Met malware wordt het proces van internetbankieren veranderd. Bij het internetbankieren kunt u bijvoorbeeld onmerkbaar worden doorgelinkt naar een andere site dan die van uw bank. Deze site lijkt echt, maar is in werkelijkheid een goed nagemaakte kopie waarop de crimineel informatie kan verwijderen, wijzigen of toevoegen. Zo kunnen transactiegegevens, zoals rekeningnummer, bedrag en ontvanger worden gewijzigd om gestolen geld te verbergen, of om uw betaling naar een andere rekening te verzenden.

Voor het stelen van informatie zijn er verschillende soorten malware:

- Met spyware wordt uw surfgedrag ‘bespioneerd’.
- Zogeheten *keyloggers* verzamelen alle sleuteltermen zoals wachtwoorden, creditcardnummers en inlogcodes die u op sites invoert.
- *Screenscrapers* verzamelen alle gegevens die u op uw scherm ziet.
- Met *rootkits* wordt het besturingssyteem van uw computer overgenomen. De crimineel kan precies volgen wat u op de computer doet en ziet alle gegevens die u op uw computer achterlaat.

Ransomware en cryptoware

Ransomware betekent letterlijk: gijzelingssoftware. Criminelen maken uw computer, of een deel hiervan, ontoegankelijk. Dit doen zij via ransomware, cryptoware en scareware. Zij kunnen bestanden in alle formaten op de harde schijf van de computer blokkeren, maar ook een virtual (cloud) disk, externe harde schijf en usb-sticks kunnen tijdens een besmetting worden vergrendeld. Ook (gedeelde) bestanden die zijn opgeslagen in bedrijfsnetwerken kunnen worden versleuteld.

Na betaling zou de computer ontgrendeld worden.

Niets is minder waar. Het bericht is afkomstig van criminelen en betalen heeft vaak geen zin. Kijk op de website No More Ransom, decrypter.emsisoft.com en ID-ransomware om te zien of er een sleutel gevonden is voor het type ransomware dat uw apparaat geblokkeerd heeft. Schakel een expert in als u zelf de computer niet kunt ontgrendelen.

De versleuteling van de bestanden is een onomkeerbaar proces. Antivirussoftware kan de schadelijke software wel van de computer verwijderen, maar de bestanden niet terugzetten. De versleuteling is niet te doorbreken. Het zeer regelmatig maken van complete back-ups is de enig bekende tegenmaatregel.

Wat doet de bank?
Omdat malware direct op uw computer terechtkomt, kan uw bank hier weinig aan doen. Wel werken banken samen met professionals om malware te ontdekken en deze informatie door te spelen aan de leveranciers van antivirussoftware.

Wat kunt u doen?
Computers worden vaak besmet tijdens het surfen op internet, via e-mail of zelfs telefonisch door u te verleiden naar een bepaalde webpagina te gaan. Een besmetting is nooit helemaal te vermijden. De mogelijke maatregelen na besmetting zijn zeer beperkt, daarom is preventie des te belangrijker.
U verkleint de kans op besmetting met door twee gebruikersaccounts aan te maken. Eén die u gebruikt om zelf software op uw computer te installeren en één met minimale privileges voor dagelijks gebruik. Hoe hoger de privileges, hoe groter de kans op schadelijke software op uw computer.

Vergroot uw weerbaarheid tegen malware-aanvallen. Opgelicht?! geeft tips voor de windows gebruikers. Neem ook maatregelen om, zo nodig, direct weer te herstellen. Hiervoor is een tijdige investering noodzakelijk.

Maak regelmatig back-ups van uw bestanden en zorg dat deze back-ups niet direct verbonden zijn met uw computer. Op deze manier weet u zeker dat u ook na een besmetting nog over uw bestanden kunt beschikken.

Antivirusprogramma's en een firewall helpen voorkomen dat lekken kunnen worden misbruikt. Deze programma's waarschuwen u als vreemde zaken worden waargenomen en voorkomen de installatie van malware. Malware en ransomware kunnen makkelijker worden geïnstalleerd als de software op uw computer een lek bevat. Stel uw computer zo in dat updates automatisch worden geïnstalleerd. Wees kritisch en alert als u onverwacht wordt gevraagd programma's te installeren.

Houd uw computer veilig, zorg dat u op de echte website van uw bank bent en controleer nauwkeurig de betaling die u wilt doen. Voor meer informatie doe de test. Negeer spam en verdachte e-mails, bezoek geen duistere websites en gebruik een USB-stick niet zomaar op elke computer.
Wees u ervan bewust dat aanvallen vooral gericht zijn op:

- Het midden- en kleinbedrijf. Deze bedrijven zijn interessant voor de crimineel omdat zij beschikken over voldoende financiën, zij hebben toegang tot hun bestanden nodig om hun bedrijfsprocessen op gang te houden en willen imagoschade voorkomen. Het grootste verschil met grote organisaties is dat het MKB minder geld kan besteden aan beveiliging. Ze beschikken niet altijd over ICT-beheer, een back-up beleid of autorisatiebeheer. Hierdoor vormen ze een aantrekkelijk doelwit.

Is uw computer besmet met schadelijke software?

Is uw computer toch geïnfecteerd met malware of ransomware of vermoedt u dat dit het geval is? Gebruik deze dan direct niet meer voor internetbankieren. En controleer vanaf een andere computer de transacties op uw rekeningen. Pas nadat u er zeker van bent dat u geen schadelijke software meer op uw computer heeft, kunt u weer op uw computer internetbankieren.
Surf op een andere computer (of bijvoorbeeld een smartphone of tablet) naar de website van de Fraude Helpdesk. Op deze site vindt u instructies en stappenplannen over hoe ransomware eenvoudig verwijderd kan worden. Komt u hier niet verder mee, neem dan contact op met een erkend computerreparateur.

Betaal de crimineel niet. U heeft geen enkele zekerheid dat de crimineel de schadelijke software (volledig) verwijderd. Bovendien heeft u ook andere mogelijkheden om uw computer schoon te krijgen. Als u of uw organisatie slachtoffer bent geworden van cryptoware, dan kunt u hiervan aangifte doen bij de politie. Aangifte zal niet leiden tot een oplossing voor uw probleem, maar geeft de politie en het Nationaal Cyber Security Centrum wel meer inzicht in de omvang van het probleem. Kijk op de website No More Ransom, decrypter.emsisoft.com en ID-ransomware om te zien of er een sleutel gevonden is voor het type ransomware dat uw apparaat geblokkeerd heeft. Meer informatie leest u op de website van de politie.

CEO- en factuurfraude **Wat is factuurfraude?**

Bij factuurfraude sturen (cyber)criminelen valse facturen in de hoop dat de ondernemer deze gaat betalen. Dit gebeurt op verschillende manieren. Ten eerste sturen zij massaal nepfacturen naar willekeurige e-mailadressen. Het lijkt alsof dit facturen zijn van bekende en vertrouwde partijen als Ziggo, UPC, KPN en CJIB. Omdat het vaak om relatief kleine bedragen gaat en de e-mail lijkt te komen van gangbare partijen, betalen veel ontvangers deze nepfacturen. Dit gebeurt ook als de onderneming helemaal geen klant van de zogenaamde afzender is. Het slachtoffer gaat ervan uit dat de factuur correct is.
De tweede vorm van factuurfraude betreft de gepersonaliseerde nepfacturen. De ondernemer krijgt een vervalste factuur uit naam van een bestaande zakelijke relatie. In veel van deze gevallen onderschept de fraudeur de originele factuur (fysiek of digitaal). Vervolgens wordt enkel het rekeningnummer gewijzigd naar het rekeningnummer van de crimineel. De onderneming betaalt de rekening die hij verwachtte, maar het geld wordt overgemaakt naar het rekeningnummer van de oplichter.
Een andere vorm van factuurfraude is de zogenoemde CEO-fraude. Hoe groter een organisatie, hoe groter de kans op dat een oplichter een valse betaalopdracht verstuurt. De betaalopdracht komt veelal via e-mail binnen bij een potentieel slachtoffer. Het is ook mogelijk dat de criminelen via telefonisch contact druk uitoefenen om de betaling te verrichten. Fraudeurs doen zich voor als een belangrijke manager of bestuurder van uw bedrijf. Zij hebben zich in de onderneming verdiept, om zo werknemers te kunnen verleiden grote sommen geld over te boeken op hun rekening. Het proces van deze betaalopdracht wijkt vrijwel altijd af van de normale regels in uw bedrijf. Door de kennis van de structuur van de onderneming weten de oplichters veel slachtoffers te maken. Zij maken gebruik van het gegeven dat werknemers elkaar niet altijd persoonlijk kennen en er vaak geen contact is met het management.
Wie wordt slachtoffer van factuurfraude?
In principe kan iedereen slachtoffer worden van factuurfraude. In het mkb krijgen ondernemers voornamelijk te maken met de gerichte vervalste facturen afkomstig van bestaande zakelijke relaties. De bedragen die worden gestolen zijn geheel in overeenstemming met het type doelwit: bedrijven die grotere facturen betalen, lopen ook tegen fraude op met hogere bedragen dan kleinere bedrijven. In een enkel geval bedraagt de vervalste factuur vrijwel het hele werkkapitaal van de ondernemer en komt hierdoor de continuïteit van het bedrijf ernstig in gevaar.

Kunnen banken factuurfraude voorkomen?

De banken doen er alles aan wat ze redelijkerwijs kunnen om dit soort situaties te voorkomen voor hun klanten. Dat doen ze enerzijds door de klant veelvuldig te waarschuwen op dit soort risico's en anderzijds door gebruik te maken van diverse systemen voor monitoring en detectie. Voor de banken is het echter moeilijk om factuurfraude te herkennen en te stoppen. Het gaat hier immers om een betaling die de ondernemer zelf uitvoert en ondertekent; tenzij het rekeningnummer van de begunstigde bekend is als zijnde in gebruik door fraudeurs, zal de bank hier niet snel een afwijking in kunnen waarnemen. Dat de naam op de factuur wellicht niet de naam is van de begunstigde zal niet ontdekt worden; banken controleren wel of een rekeningnummer geldig is, maar de combinatie van rekeningnummer en naam van de begunstigde wordt niet gecontroleerd.
Hoe voorkomt u factuurfraude?
Hoewel fraudeurs zeer gehaaid zijn in hun pogingen om u geld afhandig te maken kunt u veel doen om factuurfraude te voorkomen. Het is belangrijk om te zorgen dat alle lagen van de organisatie deze vorm van fraude kennen. Vooral op afdelingen waar betaalopdrachten worden verwerkt. Maak factuurfraude daarom bespreekbaar in uw bedrijf. Als uw medewerkers twijfels durven uiten, krijgt CEO-fraude minder kans. Let ook goed op hoeveel informatie u op het internet vrijgeeft over uw organisatie, de bestuurders en medewerkers; deze informatie wordt door de fraudeur gebuikt om hun misleiding kracht bij te zetten.
Geef tot slot uw medewerkers deze concrete tips:

- Controleer het e-mailadres van de afzender van de opdracht of factuur, is dit werkelijk het e-mailadres van uw eigen onderneming of van uw relatie?
- Controleer altijd het rekeningnummer van de ontvanger met uw eigen administratie
- Verifieer de betaling door de (genoemde) opdrachtgever te bellen. Gebruik hiervoor het nummer dat bij u bekend is; niet het nummer dat bij het betaalverzoek staat. Dat nummer kan immers van de oplichter zijn
- Wees alert op smoesjes waarom een betaling urgent is en moet afwijken van normale procedures
- Wees alert op telefoontjes met een dwingend karakter

- Stel duidelijk richtlijnen op voor facturatie, met daarin beschreven wie een betaalopdracht mag uitvoeren als er geen goedgekeurde factuur is. Probeer uitzonderingen te vermijden en zorg dat er altijd meerdere handtekeningen moeten worden gezet bij een betaalopdracht functiescheiding of dubbele autorisatie). Twee mensen zien namelijk altijd meer dan één.
- Overleg bij twijfel altijd met een collega of leidinggevende.

Wat moet u doen als u toch slachtoffer bent geworden van factuurfraude?
Bel zo snel mogelijk uw bank als u een betaling deed aan een fraudeur. Hoewel de kans klein is, is mogelijk nog te voorkomen dat een (deel) van het geld verdwijnt. Daarnaast is het zaak om – ook bij een eventuele buitenlandse begunstigde – aangifte te doen. Er is immers een misdrijf gepleegd en wellicht kunnen politie en justitie met de aangifte actie tegen de criminelen ondernemen. Bovendien kan dit bij eventuele geschillen met degene die het geld wel had moeten ontvangen een belangrijk element in de afhandeling zijn.
In veel gevallen blijkt het via de bovenstaande weg onmogelijk om geld terug te krijgen. In tegenstelling tot bij een automatische incasso, kan de bank een eenmalige, door u ondertekende betalingsopdracht niet terugdraaien. De bank zal proberen contact op te nemen met de (buitenlandse) bank van de begunstigde om daar de transactie te laten stoppen. Zodra een fraudeurs het geld contant heeft opgenomen is terugdraaien van de betalingsopdracht niet meer mogelijk. Snelheid is dus van belang.
Wat kunt u doen als u pogingen ziet van factuur en/of CEO-fraude?
Als u pogingen tot deze fraudes ontdekt kunt u een paar zaken doen om te voorkomen dat de fraudeurs binnen uw organisatie (of die van anderen) succesvol zijn:

- Laat het valse domein direct blokkeren op uw mailserver
- Monitor uw e-mailverkeer op valse domeinen
- Stuur valse e-mail door naar de fraudeafdeling van de geïmiteerde organisatie.

Aangifte doen van factuurfraude

Aangifte doen van het criminele feit (of feiten) bij de politie is van groot belang. De politie maakt een proces-verbaal op. De beslissing of daarna ook daadwerkelijk vervolging wordt ingesteld ligt bij het Openbaar Ministerie (OM). Aangifte doen van deze vorm van criminaliteit kan bij elk politiebureau. Meldt de fraude ook bij uw bank, zodat de banken deze de informatie kunnen gebruiken bij de monitoring en detectie van toekomstige pogingen tot fraude.

Waarom is aangifte doen van belang?
Succesvol onderzoek doen naar daders begint met informatie van aangiftes. Daarbij is het van belang dat gegevens die herleidbaar zijn tot de criminele feiten ongewijzigd worden toegevoegd aan de aangifte (b.v. de valse factuur, al dan niet digitaal). De aangiftes geven inzicht in de wijze van handelen van de crimineel of organisatie van criminelen. Als elk benadeeld bedrijf aangifte doet wordt meer informatie verzameld en gecombineerd. Hoe meer informatie, hoe groter de kans dat op basis daarvan succesvol onderzoek kan worden gedaan naar de daders.
Aangifte doen is ook van belang voor het herkennen van nieuwe vormen van factuurfraude. De informatie uit de aangifte kan leiden tot aanpassingen in beveiligingssoftware, antivirusprogramma's en in updates van systemen. Dit maakt het voor alle mkb-bedrijven weer een stuk veiliger.
Tot slot: de verzekeringsmaatschappij zal een kopie vragen van de aangifte (mits verzekerd tegen cybercrime).

Voorbereid aangifte doen!
Vraag bij het maken van een afspraak om aangifte te doen altijd om de aanwezigheid van een digitaal rechercheur, dat helpt bij het formuleren van de aangifte en zorgt dat deze zo compleet mogelijk wordt opgenomen. Bij het opnemen van de aangifte zal om informatie worden gevraagd die gebaseerd is op de wettekst en dus op de elementen van het strafbare feit, zoals:

- Betreft het een aangifte tegen een particulier of een bedrijf?
- Zijn er beveiligingsmaatregelen genomen?
- Wat is de geschatte schade (uren in geld, immateriële schade) en wat zijn de herstelkosten?
- Is er al een verdachte bekend?

Ten slotte; de bank zal dit type fraude niet vergoeden en de ontstane schade wordt doorgaans ook niet door uw verzekeraar vergoed. U heeft immers zelf de betaling uitgevoerd naar het rekeningnummer van de crimineel en deze ondertekend als zijnde correct. Het is daarom ook in uw eigen belang om de in deze brief genoemde preventieve maatregelen te treffen en bij een geslaagde fraudepoging zo snel mogelijk actie te ondernemen.

Andries Vermeulen