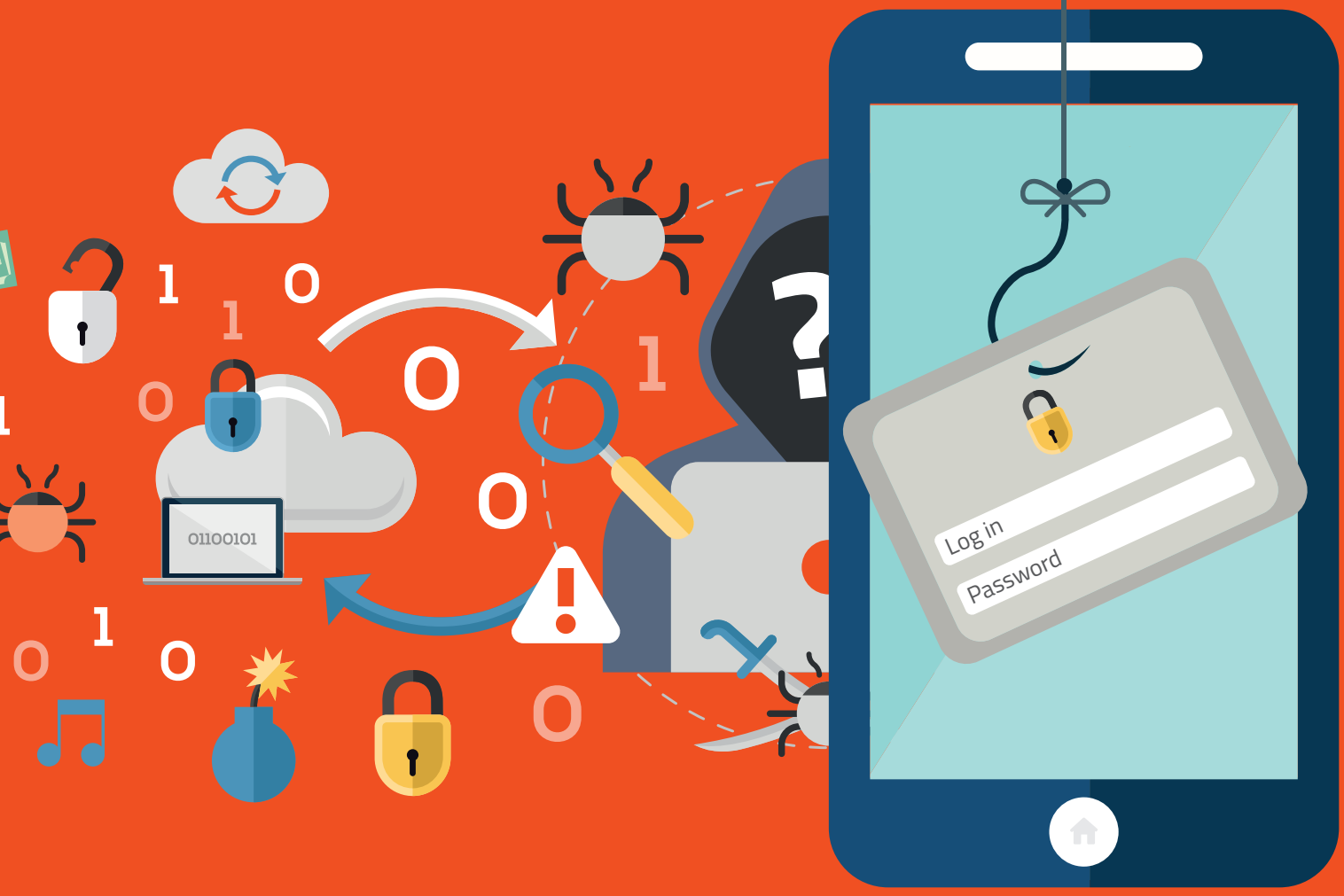
BETALINGSFRAUDE: HOE KUNNEN ONDERNEMINGEN ZICH WAPENEN?



accountant belastingconsulent iab
BeExcellent.be!

UCM

BIBF IPCF

unizo
VERSTERKT ONDERNEMERS

Instituut van de Bedrijfsrevisoren
Koninklijk Instituut

febelfin

VBO Verbond van Belgische Ondernemingen | FEB Fédération des Entreprises de Belgique

isabel
beyond banking

Meer en meer ondernemingen worden vandaag geconfronteerd met diverse vormen van betalingsfraude. Deze fraudevorm is vaak gestructureerd zoals een echt bedrijfsmodel en komt voort uit een grondige voorkennis van de beoogde ondernemingen. Voorkennis die in het algemeen opgedaan wordt via internet en social media.

Om deze - in toenemende mate internationaal georganiseerde - vorm van oplichting te bestrijden, hebben het VBO, UNIZO, UCM, de bankensector, de economische beroepen, en de gerechtelijke politie van Brussel (NIFO, *National and International Fraud Office*) hun krachten gebundeld.

De gevolgen kunnen dramatisch zijn: enerzijds is er de financiële impact op de onderneming die weinig kans heeft om de naar het buitenland overgedragen bedragen terug te vorderen; anderzijds is er de menselijke impact op de werknemer die de oplichting niet meteen door heeft.

MISLEIDING VAN BOEKHOUDKUNDIGE EN FINANCIËLE MEDEWERKERS IN BELGISCHE ONDERNEMINGEN

De werknemers van financiële, IT- en juridische diensten moeten prioritair worden geïnformeerd. Verhoogde waakzaamheid en een aangescherpte kritische benadering zullen hen in staat stellen om de oplichtingsscenario's te identificeren waarmee zij ooit kunnen worden geconfronteerd.

Enkele cijfers

Sinds september 2010 werden alleen al voor de zogenaamde oplichting "uit naam van de bedrijfsleiding" (cf. *infra*) 32 onderzoeken geopend bij de federale gerechtelijke politie van Brussel voor een bedrag van ruim 37 miljoen euro, waarvan meer dan 13 miljoen daadwerkelijk werd overgeschreven naar buitenlandse bankrekeningen van oplichters. De resterende 24 miljoen betrof pogingen tot overdracht.

Voor dezelfde periode bedragen de actueel gekende cijfers in Wallonië (Marche-en-Famenne, Neufchateau, Hoei, Bergen, Doornik, Nijvel, Luik en Charleroi) 31 dossiers, voor een totaal bedrag van 24 miljoen euro, waarvan iets meer dan 4 miljoen overgeschreven werd naar de rekeningen van de oplichters.

In Vlaanderen tonen de onvolledige cijfers (Antwerpen, Turnhout, Leuven, Oudenaarde en Halle) 8 geopende onderzoeken waarbij geprobeerd werd 3,5 miljoen euro over te schrijven. Daarvan kwam ook effectief een kleine 2 miljoen euro op de rekeningen van de oplichters.

Deze cijfers vormen slechts het zichtbare deel van de ijsberg: talrijke om hun imago bezorgde ondernemingen onthullen liever niet dat ze werden misleid. Daarenboven betreft het hier slechts bepaalde oplichtingsvormen gebaseerd op identiteitsmisbruik en manipulatie van medewerkers (cf. *infra*); andere oplichtingsvormen zoals vervalsing van facturen bijvoorbeeld, zijn niet in deze cijfers opgenomen – bij gebrek aan nauwkeurige statistieken hieromtrent – ook al werden er bij de politiediensten reeds duizenden gevallen gemeld.

Om welke oplichtingspraktijken gaat het?

Deze oplichting kan een oneindig aantal vormen aannemen. We onderscheiden voornamelijk twee oplichtingsvormen, de ene gebaseerd op identiteitsmisbruik en de andere op het onderscheppen van documenten.

Een derde categorie maakt gebruik van *malware* die de informaticasystemen besmet.

1. Oplichting gebaseerd op identiteitsmisbruik

Deze oplichting wordt soms voorafgegaan door een voorbereidingsfase.
Hierna volgen enkele terugkerende scenario's waarmee de oplichting kan gedetecteerd worden:

VOORBEREIDINGSFASE

Gebruikt voorwendsel:

Audit en analyse van de betaalprocessen

- De oplichter contacteert een onderneming, eventueel dochteronderneming van een internationale groep, via telefoon of e-mail.
- Hij doet zich voor als een overheidsinstelling, auditor of bedrijfsrevisor die aangesteld is om de interne betaalprocessen uit te schrijven.
- Op die manier tracht hij waardevolle informatie te verkrijgen zoals de identiteit van de medewerkers die gemachtigd zijn om betalingen uit te voeren.

Gebruikt voorwendsel: Informaticatest

- Ook hier neemt de oplichter contact op met een onderneming via telefoon of e-mail.
- Hij doet zich voor als een informaticus van het bedrijf dat instaat voor de beveiliging van de betalingen.
- Onder de dekmantel van het uitvoeren van een aanal "testen", verzoekt hij het slachtoffer om hem gevoelige informatie (betalingsprocedures, rekeningsaldi, rekeningnummers, enz.) te verstrekken.

UITVOERINGSFASE

- De oplichter neemt telefonisch contact op met een medewerker van de financiële dienst van de beoogde onderneming.
- Hij geeft zich uit als de CEO, de CFO of een vertrouwenspersoon van de onderneming.
- Hij eist de grootst mogelijke vertrouwelijkheid in verband met zijn oproep.
- Onder de dekmantel van bijvoorbeeld een belastingcontrole of de overname van een onderneming, zal er steeds een dringende betaling moeten worden uitgevoerd.
- Hij zal, misbruik makend van de naam van de CEO, CFO, of iedere andere vertrouwenspersoon van de onderneming, en met behulp van vleierij of agressie, eisen dat het slachtoffer de ingevoerde betalingsprocedures omzeilt.

De bedrieger zal zeer overtuigend overkomen. Zo zal hij bijvoorbeeld een "pseudo"-advocaat in het gesprek betrekken, een e-mail sturen naar het slachtoffer via een e-mailadres dat lijkt op dat van de Voorzitter, de financieel directeur, een advocaat of andere beroepsbeoefenaar, alsook, onder een vals voorwendsel, de grootst mogelijke vertrouwelijkheid eisen.

Aangezien hij vóór zijn oproep doorgaans voldoende informatie heeft ingewonnen over het slachtoffer (bijvoorbeeld met behulp van op het internet beschikbare gegevens), heeft hij nog meer invloed op het slachtoffer.

Aangezien het slachtoffer zich tot geheimhouding heeft verbonden, ondervindt deze een maximale druk.

2. Oplichting gebaseerd op het onderscheppen van documenten, en meer bepaald van facturen

Dergelijke oplichters zijn eveneens goed georganiseerd:

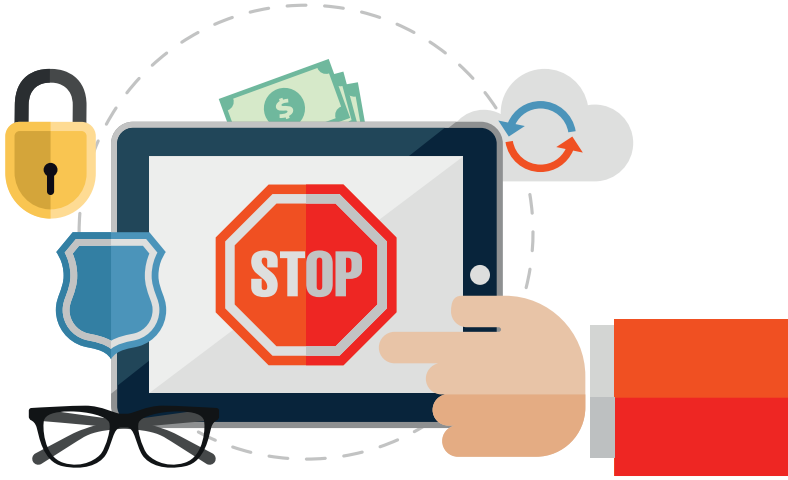
- na het onderscheppen van facturen veranderen ze het rekeningnummer van de begunstigde;
- in sommige gevallen worden de contactgegevens van de opsteller van de factuur (telefoonnummers of e-mailadres) ook aangepast zodat eventuele informatieaanvragen (met betrekking tot de geldigverklaring van de factuur) bij de oplichters zelf terechtkomen.
- in andere gevallen beweren de oplichters in kwestie dat het door het slachtoffer gehuurde pand van eigenaar is veranderd en verstrekken zij nieuwe – en valse – gegevens voor de betaling van de huur.

Wanneer de boekhoudkundige bediende denkt dat hij contact opneemt met de opsteller van de factuur om zich ervan te vergewissen dat het rekeningnummer wel degelijk werd gewijzigd, wordt hem verteld "*ja, ja, we hebben ons rekeningnummer gewijzigd*"...

3. Oplichting gebaseerd op "*malware*"

Malware is een verzamelnaam voor allerlei soorten kwaadaardige en schadelijke software. Ongevraagd en onopgemerkt slaagt die erin zich op uw computer te installeren, meestal tijdens het openen van een verdachte bijlage bij een e-mail of een hyperlink.

Malware stoort en manipuleert normale computerprocessen om onder meer informatie te stelen of frauduleuze betalingsopdrachten te genereren tijdens internetbankingsessies.



Hoe kan men zich tegen deze oplichtingspraktijken wapenen?

VOORLICHTING

Om deze oplichterij tegen te gaan, is het van fundamenteel belang dat gedetailleerde informatie wordt verspreid op alle niveaus van de onderneming.

ADMINISTRATIEVE PROCEDURES

De administratieve procedures van de onderneming moeten gericht zijn op het verlagen van het risico van onverschuldigde betalingen, bijvoorbeeld door de controle en de goedkeuring van de facturen en door de strikte naleving van de ondertekeningsbevoegdheid voor betalingen. Deze schriftelijk vast te leggen procedures moeten aan het personeel worden meegedeeld en de juiste toepassing ervan moet geregeld worden gecontroleerd.

BELANGRIJKSTE KNIPPERLICHTEN:

- **ongebruikelijke transacties** op grond van de aangehaalde redenen, het bedrag, de omstandigheden, enz.;
- **geheimhoudingsplicht** (vertrouwelijkheidsvereiste, gebruik van een geheime code, verzoek om de gesprekspartner te contacteren via zijn gsm of persoonlijk e-mailadres);
- **hoogdringendheid** (dringende behoefte aan liquide middelen);
- **ongewone druk** om gevoelige informatie of een betaling (ongebruikelijke contactname door de CEO of CFO, tussenkomst van een advocaat) te verkrijgen;
- transacties naar **buitenlandse bankrekeningen** (binnen of buiten Europa);
- overdracht van liquide middelen op een **vrijdag** of de **dag vóór een feestdag** (waardoor het geld niet door de bank kan worden geblokkeerd);
- **wijziging van de betalingsgegevens** van een vaste leverancier;
- Een e-mail met een **link naar de website van uw bank** en waarin gevraagd wordt om je persoonlijke code in te voeren.

PRAKTISCHE PREVENTIEADVIEZEN:

- Pas de **veiligheidsregels** en **betalingsprocedures** strikt toe; leef in het bijzonder de regels na met betrekking tot de **taakverdeling** en de uitoefening van de **ondertekeningsbevoegdheden**, en dat **onder alle omstandigheden**. Het systeem waarbij betalingen vanaf een bepaald bedrag door meerdere personen moeten worden ondertekend, biedt een betere bescherming;
- **Beveilig** je computer voldoende (o.a. via een up-to-date antivirusscanner en een goed beveiligde WIFI-verbinding);
- Verspreid geen interne bedrijfsinformatie (hiërarchische structuur, bevoegdheden, afwezigheden, beschikbare liquide middelen, enz.) wanneer deze wordt opgevraagd via telefoon of e-mail;
- Controleer de identiteit van de **gesprekspartner** bij het geringste vermoeden;
- Controleer **de oorsprong van telefoongesprekken**;
- Controleer de **juistheid van de e-mailadressen, en in geval van twijfel, de IP-adressen** van waaruit de e-mails worden verzonden (www.whois.com);
- Neem contact op met de opdrachtgever via een **ander telefoonnummer** of e-mail dan deze meegedeeld door de opbeller;
- Contacteer systematisch de leverancier wanneer de **betalingsgegevens** worden gewijzigd (opgelet: het telefoonnummer op de factuur kan ook gewijzigd zijn en het is heel goed mogelijk dat een oproepnummer dat bijvoorbeeld het netnummer "02" gebruikt, in werkelijkheid op duizenden kilometers van Brussel terechtkomt);
- Wees extra voorzichtig wanneer een betaling moet worden verricht op een rekeningnummer dat nog niet in het gebruikelijke **betalingssysteem** werd aangemaakt;
- Aarzel niet om de rekening- en telefoonnummers van een onderneming te controleren via de **internetzoekmachines**;
- Met betrekking tot de federale **belastingen** (waaronder de btw), ga na of de rekeningnummers wel degelijk beginnen met BExx679x...;
- Laat u niet onder druk zetten;
- **Overleg** met uw leidinggevende of een collega, zelfs wanneer de grootst mogelijke discretie vereist is (zonder u niet af);
- Stel een **vertrouwenspersoon** aan binnen de onderneming waarnaar de werknemer zich zal kunnen richten bij het geringste fraudevermoeden;
- Klik nooit op een **bijlage of link in een e-mail** die je niet helemaal vertrouwt;
- Surf nooit via een link in een e-mail naar de website van je bank om vervolgens **persoonlijke codes** in te voeren;
- Indien bij het openen van een bijlage in een email die je niet helemaal vertrouwt, in een pop-up scherm wordt gevraagd om de uitvoering van een **«macro»** toe te laten, ga daar dan niet op in.

BIJ OPLICHTINGSPOGINGEN:

- Waarschuw de **politie**;
- Waarschuw de ondernemingen of beroepsbeoefenaren van wie de identiteit vervalst lijkt te zijn of waarvan de gegevens vervalst zijn onder meer op de facturen.

INDIEN DE BETALING WERD UITGEVOERD:

- Neem onmiddellijk **contact op met uw bank**, die zal proberen het overgeschreven geld te recupereren
- Dien een **klacht** in.

CONTACTPERSOON

Federale gerechtelijke politie van Brussel
National and International Fraud Office (NIFO)
Vervangen door: pjfgp.bru.dirops@police.belgium.eu
HINP LECROART (02/223.93.54) en CP LECOMTE Serge (02/223.93.69)