ISABEL
E-SECURITY

BEWAAK EN BESCHERM UW ONLINE BETALINGS-VERKEER.

isabel group

VEILIGER INTERNETBANKIEREN DANKZIJ ISABEL 6.

Isabel Group is vooruitstrevend in veiligheid.

Cybercriminaliteit is een reële bedreiging en de technieken en methodes evolueren voortdurend. Met Isabel Security Services zetten we voluit in op innovatie om fraudeurs een stap voor te blijven en de risico's tot een minimum te beperken.

Veilige financiële transacties garanderen we via Isabel 6, een multibancaire oplossing die professionals in één keer toegang geeft tot alle rekeningen bij hun verschillende banken:

- 30.000 bedrijven, zelfstandigen, organisaties en overheden gebruiken Isabel 6 elke dag.
- In 2015 werd via Isabel 6 voor ruim 2.600 miljard euro aan transacties uitgevoerd.
- De Isabel 6 smartcard wordt door de overheid erkend als betrouwbare toegang voor bv. Tax-on-web.

Een bijlage openen, zo simpel kan het zijn om een virus te activeren. Of zelfs gewoon een e-mail in preview bekijken.
Er bestaan jammer genoeg tal van manieren om in te breken in financieel verkeer. Vergis u niet: ook kleine ondernemingen worden geviseerd door hackers. Multinationals beschikken vaak over een professioneel uitgeruste IT-afdeling om zich te beveiligen, maar voor een KMO zijn de middelen beperkt. Gelukkig hoeft u geen expert te zijn om preventieve maatregelen te nemen: Isabel Group staat tot uw dienst als uw expert.

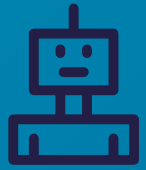
Vertrouw op onze specialisten en tools om uw bankzaken te beschermen.

CYBERCRIMINALITEIT:
VANWAAR KOMT HET GEVAAR?

De inbreuk kan voor of tijdens de transactie gebeuren via uiteenlopende technieken. Vaak bedienen criminelen zich van een andere identiteit om uw computer of de mensen achter het scherm te misleiden.

Phishing

Criminelen doen zich per e-mail voor als een betrouwbare afzender en proberen op die manier gevoelige financiële informatie of zelfs uw gebruikersnaam en paswoord te achterhalen.



BotNets

Een BotNet is een netwerk van computers dat gecontroleerd wordt door hackers. Uw pc kan hier deel van uitmaken zonder dat u zich er bewust van bent.

Factuurfraude

U ontvangt per post of per e-mail een nepfactuur op naam van één van uw leveranciers met een aangepast rekeningnummer.

Kwaadaardige software

Via virussen en andere ‘malware’ kunnen criminelen zich vanop afstand toegang verschaffen tot uw computer en systeem.

CYBERCRIMINALITEIT:
VANWAAR KOMT HET GEVAAR?

Mule Accounts

Mensen worden online gerekruteerd om gestolen geld door te sturen in opdracht van de criminelen. Vaak weten deze ‘smurfers’ niet dat ze betrokken zijn bij illegale praktijken.

Gestolen identiteit

Door iemands online identiteit te gebruiken, kunnen criminelen financiële informatie ontfutselen en zelfs kredieten aanvragen.

CEO-fraude

De aanvaller stuurt in naam van de CEO een vertrouwelijke e-mail naar een bepaalde medewerker van de financiële dienst met de vraag een som over te schrijven. Vaak vinden de criminelen de nodige informatie gewoon op de website van het bedrijf of via hun kanalen op sociale media.

Man in the Middle

Een derde partij onderschept uw communicatie met de bank door uw browser over te nemen. Zo lijkt het alsof u transacties tekent die u zelf aangemaakt heeft, maar in werkelijkheid autoriseert u valse betalingen die door de hackers opgezet worden.

MALWARE:
WAAR ZIT DE ZWAKKE SCHAKEL?

Door heimelijk kwaadaardige software te installeren op uw computer, brengen criminelen uw bankzaken in het gedrang. En dat kan u heel wat geld kosten. De beveiliging van uw pc is dus van vitaal belang.

Hoe slaat malware toe?

- Een virus is een klein programma dat de werking van uw computer verstoort.
- Spyware is software die gegevens zoals paswoorden en rekeningnummers verzamelt om te verkopen op de zwarte markt. Via een Keylogger bijvoorbeeld kan men ongemerkt de aanslagen op het klavier registreren.
- Met Ransomware kunnen criminelen uw computer 'gijzelen' en u dwingen losgeld te betalen om uw toestel te ontgrendelen.

MALWARE: WAAR ZIT DE ZWAKKE SCHAKEL?

Malware kan uw persoonlijke informatie stelen, anderen toegang verschaffen tot uw systeem of zelfs uw computer onklaar maken. Wees dus waakzaam, want voorkomen is beter dan genezen.

Getuigenis

"Ik had per e-mail een factuur ontvangen van een leverancier en toen ik de bijlage opende leek het om een leeg bestand te gaan. Vreemd. Daarom keek ik de e-mail nog een keer na en toen pas zag ik dat mijn leverancier niet de echte afzender was. Ik heb het bericht dan verwijderd, maar later bleek dat de malware zich al verspreid had op mijn pc."

FRAUDE:
LAAT U NIET MANIPULEREN.

Terwijl de aanvallen op technisch vlak inventiever worden, deinzen sommige bedriegers er toch niet voor terug u persoonlijk te contacteren en te misleiden.

Social Engineering

Iemand doet zich voor als een persoon die u kent en vertrouwt en vraagt u om dringend een grote som te betalen. Deze fraudeurs informeren zich over uw bedrijf en collega's via sociale media en andere kanalen en proberen u zo te overtuigen van hun valse identiteit.

Getuigenis

"Ik kreeg een telefoontje van een 'collega' die op zakenreis was. Hij vroeg of ik snel een aanzienlijke som kon storten op een buitenlandse rekening om een contract af te sluiten met een nieuwe partner. De deal was nog niet rond, dus ik moest de transactie geheimhouden. Zo stond het ook expliciet in de bevestigingsmail die ik ontving, verstuurd van een privéadres. Ik werd bovendien nog enkele keren gebeld met de vraag om zo snel mogelijk te betalen."

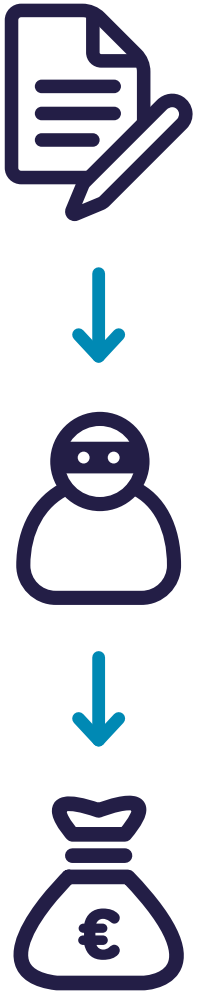
FRAUDE:
LAAT U NIET MANIPULEREN.

Uw banken en Isabel Group zullen nooit naar uw pincode of paswoord vragen. Die informatie is strikt vertrouwelijk. Als u twijfelt bij een onverwacht verzoek per telefoon of e-mail, overleg dan met een collega of uw baas. Vertel onbekenden ook niet wie binnen uw onderneming verantwoordelijk is voor de betalingen.

Vervalsing

Wanneer criminelen in uw transacties 'inbreken', schrijft u ongewild geld over naar hun **Mule Accounts**.

- Ze onderscheppen een factuur en wijzigen ongemerkt het rekeningnummer.
- Een indringer infiltreert uw boekhoudsoftware en past hier – aan de bron – rekeningnummers aan.
- Als fraudeurs aan uw betaalbestanden raken, kunnen ze ook hier hun Mule Accounts toevoegen.



PREVENTIE:
BEPERK DE RISICO'S.

U bent geen weerloos slachtoffer. Er bestaan gelukkig eenvoudige maatregelen om fraudeurs tegen te houden. Uiteraard is die waakzaamheid een gedeelde verantwoordelijkheid van boekhouding, IT, directie...

Waar kunnen u en uw collega's op letten?

OP TECHNISCH VLAK

Update uw besturingssysteem en internetbrowser.

Gebruik recente versies van antivirusprogramma's.

Zorg dat uw *firewall* permanent actief is.

Activeer *macro's* enkel indien nodig.

Installeer een *site filter* en eventueel een *ad blocker*.

PREVENTIE:
BEPERK DE RISICO'S.

Waar kunnen u en uw collega's op letten?

IN HET DAGELIJKSE GEBRUIK

Open niet zomaar bijlagen of links in een e-mail.

Bezoek geen onbetrouwbare websites.

Gebruik geen geïnfecteerde USB-sticks.

Deel niet teveel (professionele) informatie via sociale media.

Kijk uit voor vreemde meldingen of schermweergaven.

Wees extra waakzaam tijdens vakantieperiodes.

PREVENTIE:
BEPERK DE RISICO'S.

Waar kunnen u en uw collega's op letten?

BIJ TRANSACTIES

Beperk de toegang tot de boekhoudingsoftware.

Controleer de afzender van de betalingsaanvraag.

Ga niet meteen in op een uitzonderlijk verzoek.

Raadpleeg altijd een collega in geval van twijfel.

Kijk betalingen twee keer na alvorens te tekenen.

Bewaar betaalbestanden op een veilige plaats.

PREVENTIE: VERHOOG UW VEILIGHEID MET ISABEL 6.

Wij helpen u om proactief in te grijpen en uw financiële transacties af te schermen van criminelen. We hebben daarvoor Isabel 6 ontwikkeld, een solide tool die complementair is met uw huidige boekhoudpakket.

Isabel 6: meer overzicht, meer controle

Zodra u over verschillende professionele rekeningen beschikt of met twee of meer banken werkt, kunt u Isabel 6 gebruiken om al uw transacties te bundelen en te verwerken in één overzichtelijke omgeving.

Dankzij Isabel 6 kunt u zich bovendien wapenen met enkele componenten die uw gebruikersidentificatie gevoelig verbeteren:

- uw eigen smartcard met persoonlijke pincode
- een directe, veilige verbinding tussen uw kaartlezer en pc
- een kaartlezer met toetsenbord (geen kans voor **Keyloggers**)

PREVENTIE:
VERHOOG UW VEILIGHEID MET ISABEL 6.

Isabel 6: meer mogelijkheden, meer zekerheid

Extra overzicht betekent ook extra controle. Dankzij de synchronisatie tussen uw boekhouding en Isabel 6 wordt alle informatie nauwkeurig overgedragen, zowel intern als naar de banken toe. Zo beperkt u het risico op manipulatie van gegevens.

De slimme functionaliteiten maken het ook mogelijk om interne procedures te optimaliseren:

- Deel geverifieerde begunstigden en bewaar ze in één lijst.
- Controleer gericht dankzij een gedetailleerd betalingsoverzicht.
- Krijg telefonische meldingen van verdachte transacties.
- Bepaal in overleg met uw bank(en) de bevoegdheden van elke medewerker via mandaten.
  - Wie ziet welke informatie?
  - Wie mag betalingen aanmaken?
  - Wie mag betalingen tekenen?
  - Wat is de limiet voor betalingen?

PREVENTIE:
VERHOOG UW VEILIGHEID MET ISABEL 6.

Isabel 6 MultiSign: nog meer zekerheid

Vier ogen zien meer dan twee. Via MultiSign kunt u nog eenvoudiger een collega of vennoot uitnodigen om belangrijke transacties na te kijken en te ondertekenen. Om het risico op fouten en fraude extra te beperken, vraagt u best voor elke ondertekenaar een persoonlijke Isabel 6-kaart aan.

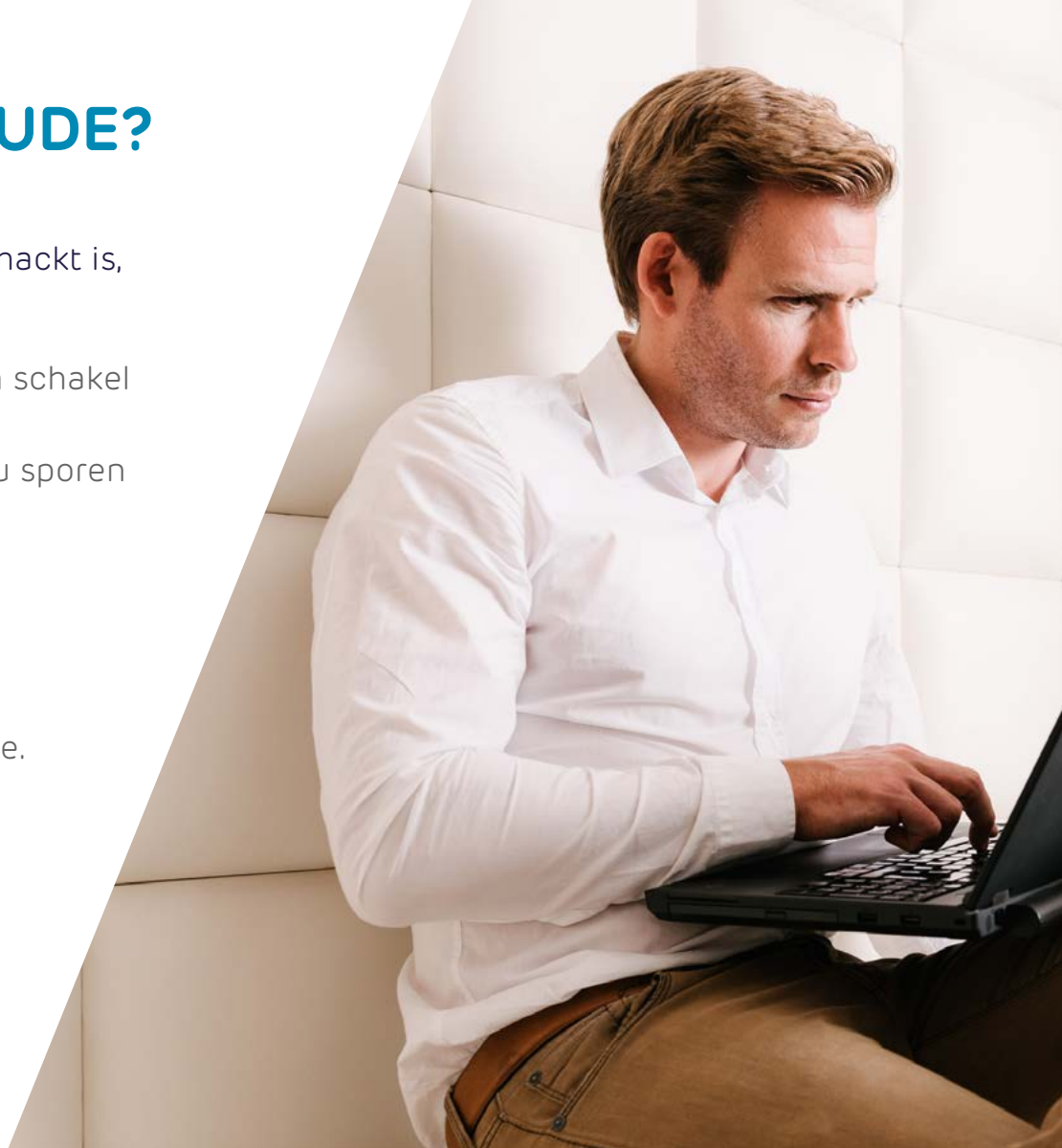
Wist u trouwens dat u meer dan twee ondertekenaars kunt aanduiden voor grote betalingen? Contacteer uw bank om de mogelijkheden te bespreken.

WAT TE DOEN BIJ FRAUDE?

Als u merkt dat uw computer besmet of gehackt is, volg dan deze aanbevelingen:

1. Koppel de netwerkkabel van uw pc af en schakel WiFi uit.
2. Zet uw pc niet uit, want anders verliest u sporen voor later onderzoek.
3. Contacteer onmiddellijk uw bank om frauduleuze transacties te annuleren.
4. Als Isabel 6-klant kunt u ook terecht bij onze klantendienst van 8 tot 18 uur.
5. Leg een klacht neer bij de federale politie.

Bankkaart verloren of gestolen?
Bel Card Stop op 070 344 344.



We maken het u graag gemakkelijk. Dankzij 20 jaar ervaring en ruime expertise op het vlak van veilige multibanking kunnen wij u op maat begeleiden en adviseren.

Uw behoefte

- Uw computer beschermen tegen kwaadaardige software
- De veiligheid van uw financiële transacties optimaliseren
- De meest recente updates en ontwikkelingen volgen

Onze oplossing

- Installeer Isabel 6
- Registreer voor onze nieuwsbrief

SAFE INTERNETBANKING .BE

CONTACTEER ONS.
Bespreek vrijblijvend alle mogelijkheden op **02 290 55 90**.

U bent een professional. Wij ook.

VEILIGER INTERNETBANKIEREN DANKZIJ ISABEL 6.

Ontdek ons aanbod en alle voordelen
op **www.isabel.eu**

isabel group