ISABEL
E-SECURITY

SUIVEZ ET PROTÉGEZ VOS TRANSACTIONS EN LIGNE.

isabel group

Il ne faut pas grand-chose pour activer un virus : ouvrir une pièce jointe ou lire un e-mail en prévisualisation suffit. Il existe malheureusement de multiples manières de s'introduire dans des transactions financières. Ne vous y trompez pas : les hackers visent aussi les petites entreprises. Les grandes multinationales peuvent souvent compter sur un département IT professionnel pour assurer leur sécurité, mais les petites et moyennes entreprises ne disposent que de ressources limitées. La bonne nouvelle ? Il ne faut pas être un expert pour agir préventivement : Isabel Group est l'expert à votre service.

Faites confiance à nos spécialistes et à nos outils pour protéger vos transactions bancaires.

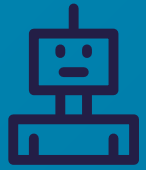
INHOUD

CRIMINALITÉ INFORMATIQUE : QUELS SONT LES DANGERS ?

L'intrusion peut se produire avant ou pendant une transaction financière et les techniques utilisées sont multiples. Les criminels utilisent souvent une identité différente pour tromper votre ordinateur ou la personne qui l'utilise.

Hameçonnage

Un criminel peut se faire passer pour une personne de confiance en vous envoyant un e-mail pour vous demander des informations financières sensibles, voire votre nom d'utilisateur et votre mot de passe.



BotNets

Un botnet est un réseau d'ordinateurs contrôlés par des cybercriminels. Votre ordinateur peut avoir été associé à ce réseau à votre insu.

Fausse facturation

Vous recevez, parfois par e-mail, une facture factice qui semble avoir été envoyée par l'un de vos fournisseurs, mais sur laquelle apparaît un autre numéro de compte bancaire.

Logiciel malveillant

Les criminels utilisent des virus ou d'autres logiciels malveillants pour accéder à distance à votre ordinateur et à votre système.

CRIMINALITÉ INFORMATIQUE : QUELS SONT LES DANGERS ?

Comptes mules

Des personnes sont recrutées sur Internet pour transférer de l'argent volé pour le compte de criminels. Souvent, ces mules sont impliquées dans des pratiques illégales à leur insu.

Usurpation d'identité

Les criminels usurpent l'identité d'un tiers pour détourner des informations financières voire pour faire des demandes de prêts.

L'arnaque au PDG

L'agresseur envoie un e-mail confidentiel à un membre de l'équipe Finance au nom du PDG dans lequel il demande à l'employé de transférer des fonds. Très souvent, les criminels trouvent très facilement les informations dont ils ont besoin sur le site web de l'entreprise ou sur les réseaux sociaux.

« Man in the Middle »

Un tiers intercepte vos communications avec la banque en prenant le contrôle de votre navigateur. Vous aurez l'impression de signer des transactions créées par vous, mais en réalité, vous autoriserez de faux paiements créés par des hackers.

LOGICIEL MALVEILLANT : OÙ EST LE MAILLON FAIBLE ?

En installant discrètement des logiciels espions sur votre ordinateur, les criminels mettent en péril la sécurité de vos opérations bancaires sur Internet. Cela peut vous coûter une fortune. La sécurité de votre ordinateur est donc extrêmement importante.

Comment les logiciels malveillants sont-ils utilisés ?

- Un virus est un petit programme qui perturbe le fonctionnement de votre ordinateur.
- Un logiciel espion est un logiciel qui collecte des données sensibles (comme les mots de passe et les numéros de compte) qui sont ensuite revendues sur le marché noir. Un enregistreur de frappe (« keylogger »), par exemple, est capable d'enregistrer toutes les touches enfoncées sur votre clavier.
- Un rançongiciel s'installe discrètement sur votre ordinateur et vous demande de payer une rançon pour débloquer votre machine.

LOGICIEL MALVEILLANT : OÙ EST LE MAILLON FAIBLE ?

Les logiciels malveillants sont en mesure de voler vos informations personnelles, de donner accès à votre système à des tiers et même de neutraliser votre ordinateur. Soyez vigilant : mieux vaut prévenir que guérir.

Témoignage

« J'ai reçu par e-mail une facture d'un fournisseur. Lorsque j'ai ouvert la pièce jointe, j'ai trouvé un fichier vierge. Étrange, j'ai donc vérifié une seconde fois l'e-mail, puis je me suis rendu compte que l'expéditeur n'était en fait pas mon fournisseur. J'ai donc supprimé le message, mais j'ai constaté plus tard que le logiciel malveillant avait déjà pris le contrôle de mon ordinateur. »

LA FRAUDE :
ÉVITER DE SE FAIRE MANIPULER.

Quoique les attaques informatiques fassent preuve de techniques de plus en plus innovantes, certains hackers n'hésiteront pas à vous contacter personnellement pour vous duper.

Ingénierie sociale

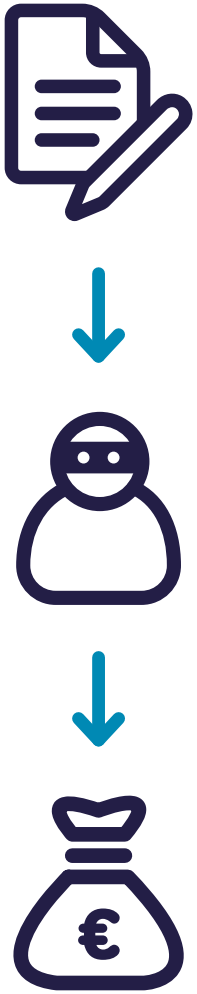
Une personne se fait passer pour quelqu'un que vous connaissez et en qui vous avez confiance. Elle vous demande de payer rapidement une grosse somme d'argent. Pour essayer de vous convaincre de sa fausse identité, le fraudeur est allé récolter des informations sur votre société et sur vos collègues sur les réseaux sociaux et d'autres canaux.

Témoignage

« J'ai reçu un appel d'un "collègue" en voyage d'affaires. Il me demandait de transférer rapidement une importante somme d'argent vers un compte étranger pour qu'il puisse conclure un contrat avec un nouveau partenaire. L'accord n'étant pas encore conclu, je devais garder cette information confidentielle. C'est également ce qui était inscrit mot pour mot dans l'e-mail de confirmation que j'ai reçu d'une adresse privée. La personne m'a aussi téléphoné à plusieurs reprises, me demandant de payer le plus rapidement possible. »

LA FRAUDE :
ÉVITER DE SE FAIRE MANIPULER.

Vos banques et Isabel ne vous demanderont jamais de donner votre code pin ou votre mot de passe. Ces informations sont strictement confidentielles. Si vous hésitez quant à l'authenticité d'une demande inattendue par e-mail ou par téléphone, parlez-en à un collègue ou à votre supérieur. Ne révélez par ailleurs jamais à des inconnus l'identité de la personne responsable des paiements au sein de votre entreprise.



Contrefaçon

Quand des criminels « s'introduisent » dans vos transactions, vous transférerez involontairement de l'argent vers leurs **comptes mules**.

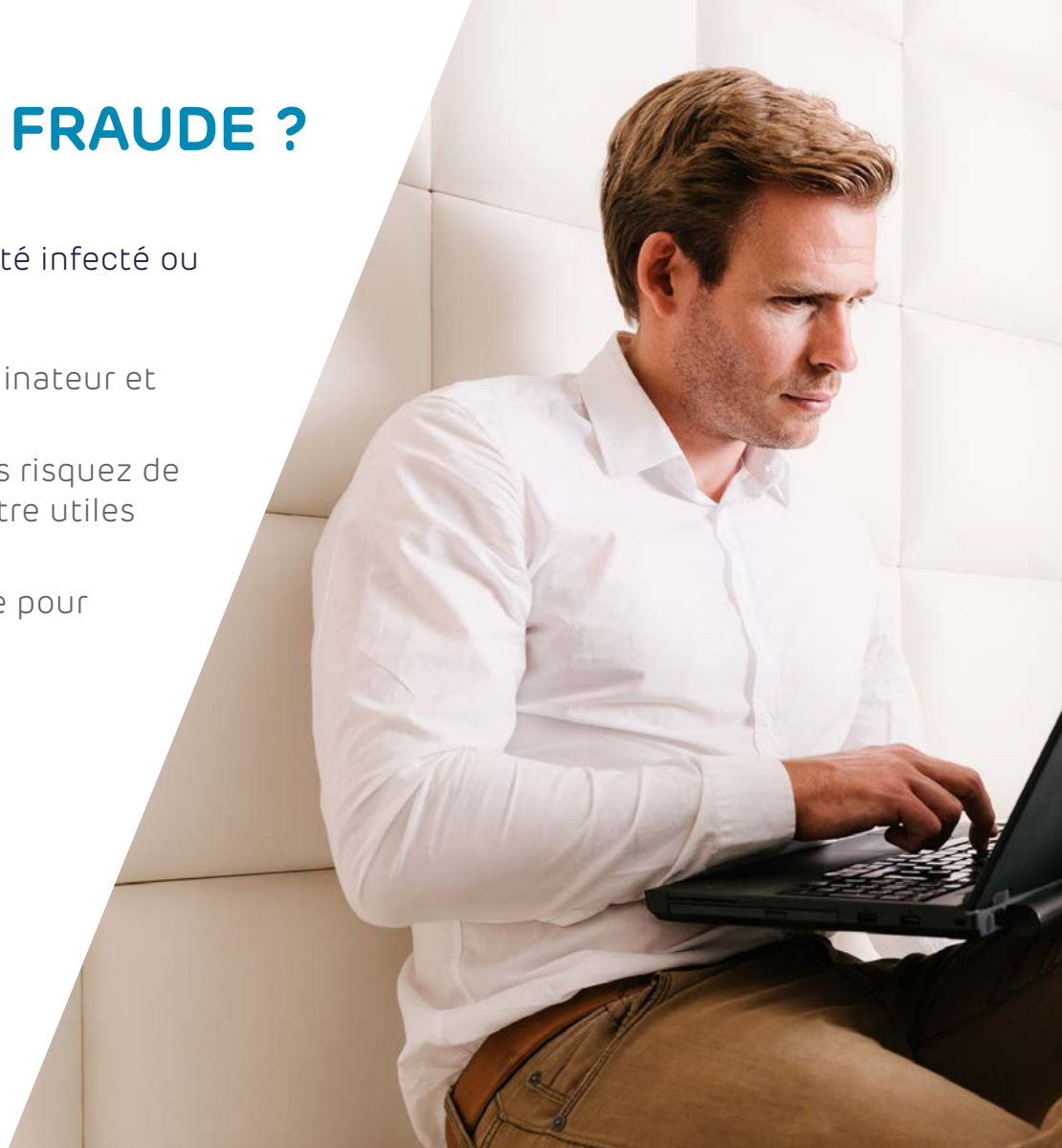
- Ils interceptent une facture et modifient le numéro de compte sans que vous vous en rendiez compte.
- Un intrus s'infiltre dans votre logiciel comptable et y modifie les numéros de compte à la source.
- Si les fraudeurs parviennent à accéder à vos fichiers de paiements, ils pourront aussi y ajouter leurs comptes mules.

QUE FAIRE EN CAS DE FRAUDE ?

Si vous remarquez que votre ordinateur a été infecté ou piraté, suivez ces recommandations :

1. Débranchez le câble réseau de votre ordinateur et coupez le Wi-Fi de votre ordinateur.
2. N'éteignez pas votre ordinateur, car vous risquez de supprimer des données qui pourraient être utiles pour l'enquête.
3. Contactez immédiatement votre banque pour annuler toute transaction frauduleuse.
4. En tant que client Isabel 6, vous pouvez contacter notre service clientèle de 8 h à 18 h.
5. Signalez l'incident à la police fédérale.

Carte bancaire perdue ou volée ?
Appelez Card Stop au 070 344 344.



PRÉVENTION : LIMITEZ LES RISQUES.

Vous n'êtes pas une victime sans défense : il existe heureusement des moyens simples pour contrer les fraudeurs. Bien entendu, la vigilance est une responsabilité qui doit être partagée par vos départements comptabilité, IT, management…

À quoi devez-vous veiller, vous et vos collègues ?

SUR LE PLAN TECHNIQUE

Mettez à jour votre système d'exploitation et votre navigateur.

Utilisez des versions récentes des programmes antivirus.

Assurez-vous que votre pare-feu soit actif en permanence.

N'activez les macros qu'en cas de nécessité.

Installez un logiciel de filtrage de sites et, si possible, un bloqueur de publicités.

PRÉVENTION :
LIMITEZ LES RISQUES.

À quoi devez-vous veiller, vous et vos collègues ?

AU QUOTIDIEN

Soyez prudent avant d'ouvrir les pièces jointes aux emails ou les liens internet.

Ne visitez aucun site web non fiable.

N'utilisez pas de clés USB infectées.

Ne partagez pas trop d'informations (professionnelles) sur les réseaux sociaux.

Méfiez-vous des messages ou écrans suspects.

Redoublez de vigilance pendant les vacances.

PRÉVENTION :
LIMITEZ LES RISQUES.

À quoi devez-vous veiller, vous et vos collègues ?

LORS DE VOS TRANSACTIONS

Limitez l'accès à votre logiciel comptable.

Vérifier toujours l'expéditeur de la demande de paiement.

Ne répondez pas d'emblée aux demandes inattendues.

En cas de doute, demandez toujours l'avis d'un collègue.

Vérifiez vos paiements deux fois avant de les signer.

Conservez vos dossiers de paiements en lieu sûr.

SÉCURISEZ VOS TRANSACTIONS BANCAIRES EN LIGNE AVEC ISABEL 6

Isabel Group vous offre une sécurité innovante.

La criminalité informatique est une menace réelle. Ses méthodes et techniques sont en constante évolution. Isabel Security Services mise sur des évolutions innovantes permettant de toujours garder une longueur d'avance sur les fraudeurs et de minimiser les risques.

Isabel 6 garantit la sécurité des transactions financières. Cette solution multibancaire donne aux professionnels l'accès à tous leurs comptes dans différentes banques sur un seul écran :

- 30 000 entreprises, indépendants, organisations et institutions publiques utilisent Isabel 6 au quotidien.
- En 2015, plus de 2 600 milliards d'euros ont été transférés par le biais d'Isabel 6.
- La smartcard Isabel 6 est accréditée par le gouvernement pour l'accès sécurisé à des applications telles que Tax-on-Web.

PRÉVENTION : AMÉLIOREZ VOTRE SÉCURITÉ AVEC ISABEL 6.

Nous avons développé Isabel 6 pour vous aider à agir de manière proactive et à protéger vos transactions financières des criminels. Isabel 6 est un outil puissant qui vient compléter votre logiciel comptable.

Isabel 6 : visibilité améliorée, contrôle accru

Si vous avez plusieurs comptes professionnels ou si vous travaillez avec deux banques ou plus, utilisez Isabel 6 pour combiner et effectuer toutes vos transactions dans un environnement unique et clair.

Avec Isabel 6, vous pouvez aussi vous protéger grâce à des composants améliorant significativement votre identification utilisateur :

- Votre smartcard strictement personnelle avec code PIN.
- Une connexion directe et sécurisée entre votre ordinateur et votre lecteur de carte.
- Un lecteur équipé d'un clavier (pour lutter contre les enregistreurs de frappe).

PRÉVENTION : AMÉLIOREZ VOTRE SÉCURITÉ AVEC ISABEL 6.

Isabel 6 : plus de possibilités, plus de sécurité

Une vue d'ensemble supplémentaire va de pair avec une surveillance accrue. La synchronisation entre vos comptes et Isabel 6 vous garantit que toutes les informations sont transmises avec précision, tant en interne qu'à vos banques. Ceci réduit le risque de manipulation des données.

Les caractéristiques intelligentes d'Isabel 6 vous permettent par ailleurs d'optimiser vos procédures internes :

- Partagez les bénéficiaires validés et regroupez-les sur une liste unique.
- Utilisez un récapitulatif de paiement détaillé pour effectuer des vérifications ciblées.
- Recevez un appel téléphonique en cas de transaction douteuse.
- Consultez votre (vos) banque(s) pour préciser l'autorisation de chaque employé disposant de mandats.
  - Qui peut consulter quelles informations ?
  - Qui peut créer des paiements ?
  - Qui peut signer les paiements ?
  - Quelle est la limite de paiement ?

PRÉVENTION : AMÉLIOREZ VOTRE SÉCURITÉ AVEC ISABEL 6.

Isabel 6 MultiSign : pour encore plus de sécurité

Quatre yeux voient plus que deux. Multisign vous permet d'inviter un collègue ou un partenaire à vérifier et à signer des transactions importantes encore plus facilement. Pour réduire encore davantage les risques d'erreur et de fraude, l'idéal consiste à demander une carte personnelle Isabel 6 pour chacun des signataires.

Saviez-vous que vous pouvez assigner plus de deux signataires aux paiements de montants importants ? Prenez contact avec votre banque pour connaître les options.

Nous aspirons à vous simplifier la vie. Avec 20 ans d'expérience et d'expertise approfondie dans la sécurité multibancaire, nous vous fournissons des conseils sur mesure.

Votre besoin	Notre solution
Protéger votre ordinateur des logiciels malveillants	Installez Isabel 6
Optimiser la sécurité de vos transactions financières	Inscrivez-vous à notre bulletin d'information
Suivre les évolutions et mises à jour les plus récentes	

SAFE INTERNETBANKING .BE

CONTACTEZ-NOUS.
Parlez sans engagement de toutes les possibilités avec nos spécialistes au **02 290 55 90**.

Vous êtes un professionnel. Nous aussi.

SÉCURISEZ VOS TRANSACTIONS BANCAIRES EN LIGNE AVEC ISABEL 6

Découvrez tous les avantages et toutes
les fonctionnalités sur **isabel.multibanking.eu**

isabel group