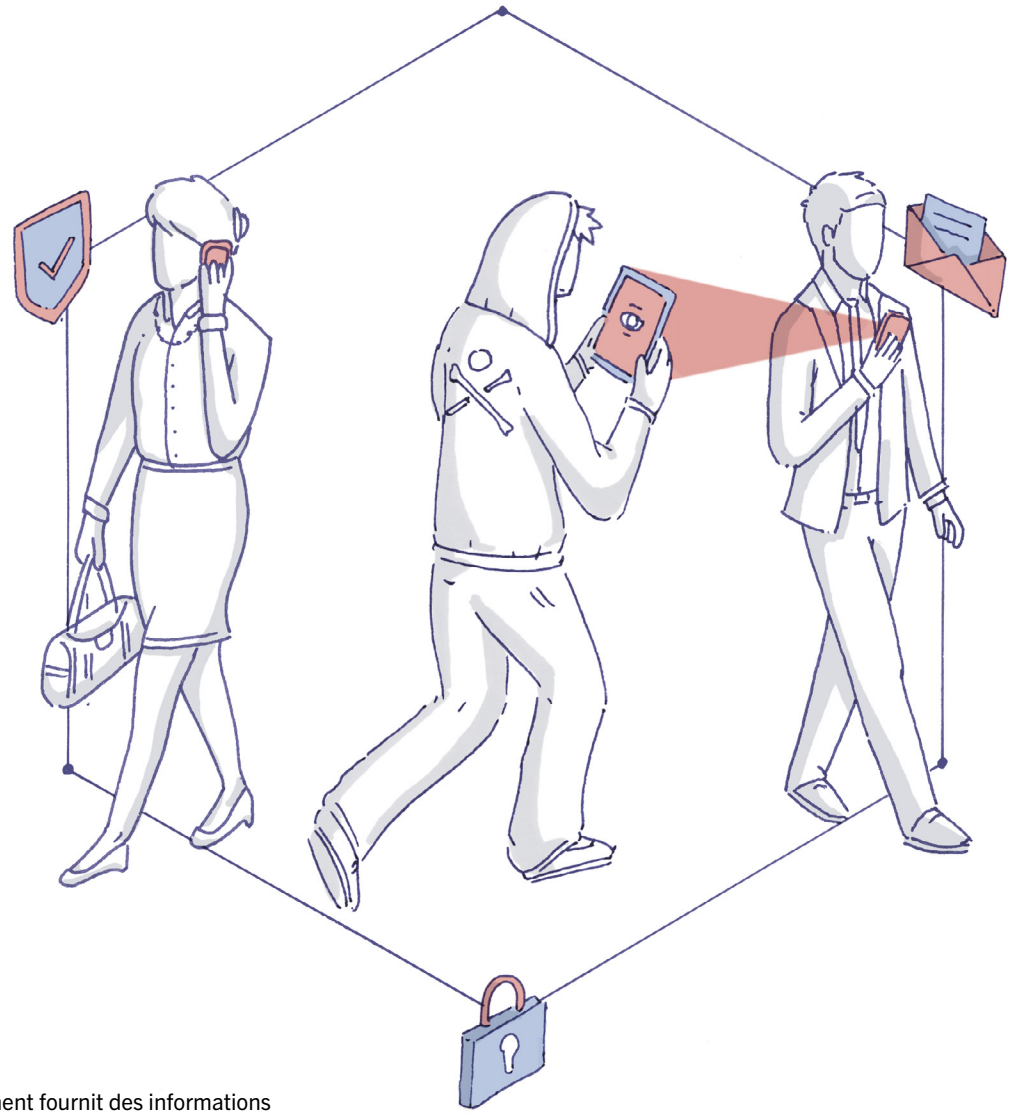
PICTET 1805

JANVIER 2020

## CYBERSÉCURITÉ

# SE PROTÉGER DES RISQUES NUMÉRIQUES



Ce document fournit des informations importantes concernant les risques liés aux communications numériques et propose des mesures facilement applicables pour les diminuer.

# DONNÉES PERSONNELLES: DES RISQUES EN AUGMENTATION

Les données personnelles sont devenues une nouvelle forme de matière première. Elles permettent d'accéder à des services gratuits tels que réseaux sociaux, systèmes de messagerie ou réseaux Wi-Fi publics, souvent sans que l'utilisateur connaisse les normes de sécurité appliquées. Ceux qui recueillent les données peuvent les exploiter commercialement, que ce soit de manière légale ou illégale.

Il s'agit donc de se montrer particulièrement prudent lorsque l'on communique des informations personnelles. D'autant que les fuites de données sont toujours plus fréquentes, même quand le comportement de l'usager n'est pas en cause. Les géants du numérique ont montré leur fragilité, à l'image de Facebook (87 millions d'utilisateurs touchés par la fuite de données Cambridge Analytica) et Google (52 millions de personnes concernées par une faille en 2018).

Le but premier de Pictet est d'établir, dans un esprit de partenariat, des relations responsables avec ses clients. Nous sommes soucieux d'assurer leur protection et nous nous préoccupons naturellement des risques liés à leurs données personnelles. Dans cette optique, nous souhaitons partager nos recommandations en matière de cybersécurité.

Des données personnelles telles que l'identité, la localisation ou les mots de passe peuvent facilement tomber entre les mains de fraudeurs, qui s'en servent pour accéder à un compte ou effectuer un chantage. Le respect de mesures simples peut considérablement réduire certains risques. Ce document permet de renforcer sa sécurité numérique (cf. pages 4-5) et de réagir de manière adéquate en cas de vol de données (cf. page 6). Nous vous recommandons de lire attentivement cette brochure et de la conserver dans un endroit facile d'accès.

Janvier 2020

# COMMENT LES PIRATES INFORMATIQUES OPÈRENT-ILS?

En collectant des informations confidentielles, les cybercriminels peuvent accéder aux comptes de leurs victimes ou les soumettre à un chantage.

Les cybercriminels rivalisent d'ingéniosité pour s'emparer des données personnelles de leurs victimes. Il leur suffit parfois de récolter des informations qui ont été rendues publiques par négligence ou par accident. Ils peuvent aussi deviner des mots de passe, s'infiltrer dans des systèmes informatiques, ou encore usurper une identité.

Il faut savoir que les fraudeurs utilisent des messages qui jouent sur l'émotion («votre ordinateur contient un virus»), l'empathie («un ami dans une situation difficile»), l'urgence («demande de réaction immédiate») ou la promesse de gains («une opportunité à saisir»).

Voici quelques exemples de vol de données ou de fraudes:

### 1. GARE AUX DÉTAILS

Un courriel en provenance d'un expéditeur connu invite l'utilisateur à se rendre sur une copie frauduleuse du site Pictet, hébergée à une adresse proche de l'originale, par exemple picttet.com, plctet.com ou pic-tet.com. Par ce biais, il est possible que la victime livre des informations qui seront ensuite utilisées par les cybercriminels.

### 2. LES DONNÉES EN OTAGE

L'utilisateur reçoit de la part d'une personne dont l'identité a été usurpée un courriel contenant une pièce jointe. L'ouverture de cette pièce jointe va bloquer l'ordinateur de la victime. Un message l'informe alors que seul le paiement d'une rançon sur un compte en *cryptomonnaie* permettra de débloquer l'ordinateur. Cette menace est fréquemmentmentionnée dans la presse sous le terme de *ransomware*.

### 3. LA FRAUDE AU PRÉSIDENT

Le comptable d'une entreprise reçoit un appel d'un cybercriminel se faisant passer pour un supérieur hiérarchique ou un haut responsable de son entreprise. Prétextant une opération urgente (acquisition à l'étranger, contrôle fiscal), l'usurpateur exige que des informations confidentielles lui soient communiquées.

# RECOMMANDATIONS EN MATIÈRE DE SÉCURITÉ

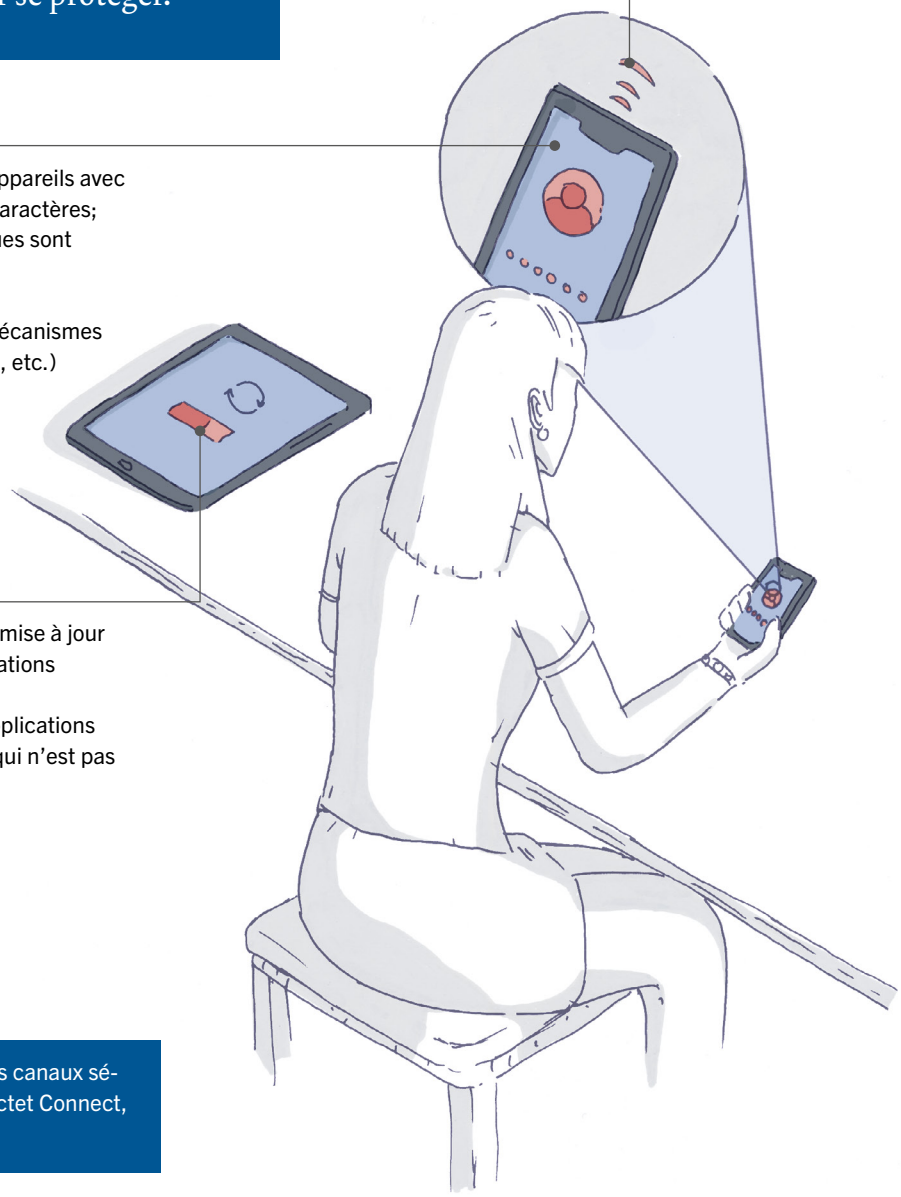
De nombreuses mesures permettent d'éviter les fuites de données et les risques de fraude. Voici quelques solutions pour se protéger.

Activer les options permettant d'effacer à distance les équipements en cas de perte ou de vol

Ne pas conserver d'informations confidentielles dans ses boîtes aux lettres (mots de passe, transactions financières, etc.)

Protéger l'accès à ses appareils avec un code de plus de six caractères; les systèmes biométriques sont également sûrs

Ne pas désactiver les mécanismes de protection (code PIN, etc.)



Activer les fonctions de mise à jour automatique des applications

Ne pas télécharger d'applications depuis une plateforme qui n'est pas celle du constructeur

Dans tous les cas, privilégier les canaux sécurisés proposés par Pictet (Pictet Connect, applications mobiles)

Vérifier les adresses des sites

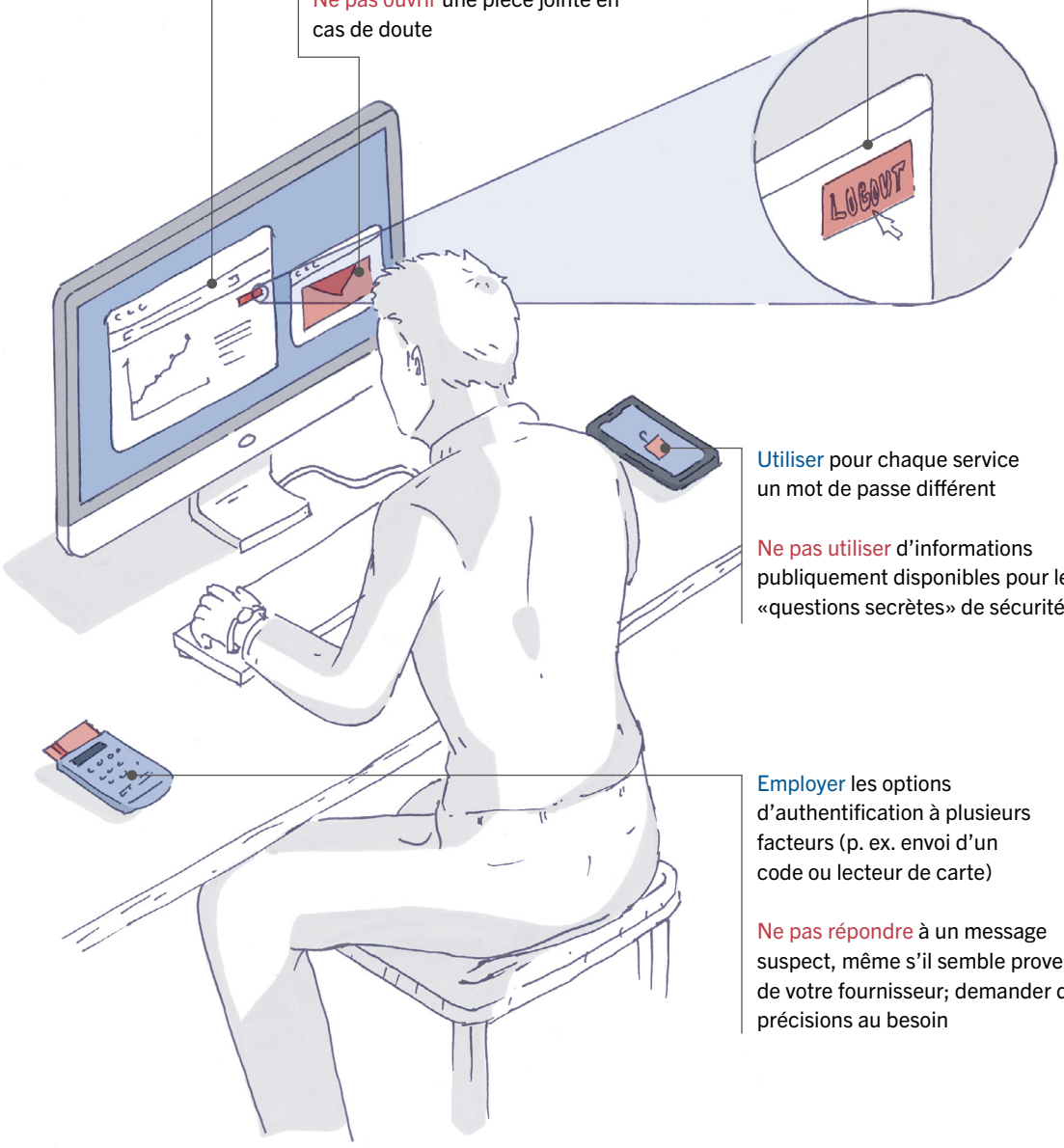
Ne pas divulguer d'informations sur un site non sécurisé, tout spécialement lors de l'emploi d'un réseau public

Adopter une attitude sainement méfiante vis-à-vis des courriels non sollicités

Ne pas ouvrir une pièce jointe en cas de doute

Fermer correctement les sessions à l'aide des fonctions fournies

Ne pas laisser une session ouverte sans surveillance




Utiliser pour chaque service un mot de passe différent

Ne pas utiliser d'informations publiquement disponibles pour les «questions secrètes» de sécurité

Employer les options d'authentification à plusieurs facteurs (p. ex. envoi d'un code ou lecteur de carte)

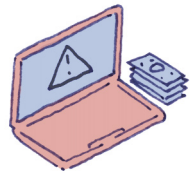
Ne pas répondre à un message suspect, même s'il semble provenir de votre fournisseur; demander des précisions au besoin

# QUE FAIRE EN CAS DE VOL DE DONNÉES?

En cas d'incident, les mesures suivantes doivent être prises immédiatement.

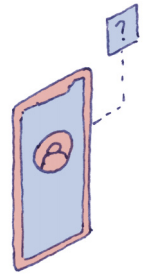
### MA MESSAGERIE A ÉTÉ PIRATÉE

- Récupérer l'accès en utilisant les consignes du fournisseur puis modifier immédiatement le mot de passe (y compris pour tout autre compte qui utilisait un mot de passe identique)
- Informer proches et contacts que cette adresse électronique n'est temporairement plus digne de confiance
- Déterminer les malversations qui auraient pu être menées sur la base du contenu de la boîte aux lettres (transactions, informations confidentielles) et contacter les parties concernées
- Vérifier ou faire vérifier la configuration de la boîte aux lettres, notamment en ce qui concerne d'éventuels renvois automatiques de messages mis en place par les pirates informatiques



### JE FAIS L'OBJET D'UNE DEMANDE DE RANÇON PAR VOIE ÉLECTRONIQUE

- Ne pas payer cette rançon
- Contacter immédiatement un expert informatique



### J'AI LIVRÉ DES INFORMATIONS SENSIBLES PAR TÉLÉPHONE À UNE PERSONNE MALVEILLANTE

- Modifier les mots de passe qui pourraient être concernés
- Informer les partenaires et proches qui pourraient être touchés
- Bloquer le numéro de téléphone de la personne malveillante et ne plus répondre à des sollicitations ultérieures

# COMMENT RECONNAÎTRE UN MESSAGE PROVENANT D'UN FRAUDEUR?

Il n'existe pas de méthode sûre à 100%, mais quelques signaux d'alerte devraient éveiller l'attention des utilisateurs.

Il est important de se méfier notamment des messages qui:

- proviennent d'une adresse inconnue ou inhabituelle; il est important de prêter une attention particulière au fait qu'une adresse malveillante peut chercher à imiter l'adresse d'un contact connu;
- incluent des éléments suspects, semblent menaçants ou convoient un sentiment d'urgence;
- contiennent des promesses vagues ou inespérées;
- incitent à ouvrir une pièce jointe ou à cliquer sur un lien pour découvrir le contenu complet du message;
- ne mentionnent pas clairement le destinataire du message et n'utilisent pas l'adresse habituellement employée par l'expéditeur.

Si un message présente un ou plusieurs des signaux mentionnés, il ne s'agit pas forcément d'un message malveillant. Il convient cependant de prendre des précautions avant de le traiter.

**Pictet**
Le groupe Pictet est dirigé par sept associés, à la fois propriétaires et gérants. Les principes de succession au sein du collège des associés et de transmission du capital sont inchangés depuis sa fondation en 1805. Le Groupe se consacre exclusivement à la gestion de fortune, à la gestion d'actifs et à l'asset servicing. Il ne propose ni crédits commerciaux ni prestations de banque d'affaires. Avec des actifs sous gestion ou en dépôt se montant à CHF 544 milliards au 30 juin 2019, Pictet compte aujourd'hui parmi les principaux acteurs indépendants de la gestion de fortune et de la gestion d'actifs en Europe.

Le Groupe a son siège à Genève, où ses activités ont débuté, et emploie plus de 4300 collaborateurs. Possédant 27 bureaux, il est également présent à Amsterdam, Bâle, Barcelone, Bruxelles, Dubaï, Francfort, Hong Kong, Lausanne, Londres, Luxembourg, Madrid, Milan, Montréal, Munich, Nassau, Osaka, Paris, Rome, Singapour, Stuttgart, Taipei, Tel-Aviv, Tokyo, Turin, Vérone et Zurich.

**Réalisation**
Large Network

FSC
MIX
Paper
FSC® C002504

www.groupe.pictet