9 RÉFLEXES SÉCURITÉ À ADOPTER DANS VOTRE VIE PRIVÉE

PAR CARTE

Ne communiquez votre code confidentiel à personne :
ni à votre famille, ni à votre banque, ni à la police...

Conservez votre carte en lieu sûr, à l'abri des regards et surveillez vos relevés de compte

Ne jamais donner les informations de votre carte, en toute circonstance

EN LIGNE

Vérifiez que le site internet est sécurisé
(https devant l'adresse du site, cadenas fermé, ou icône d'une clé dans le navigateur)

Sur internet et votre ordinateur, n'enregistrez jamais vos informations bancaires et évitez de vous connecter depuis un réseau Wi-Fi public

Veillez aux publications sur les réseaux sociaux pour ne pas donner trop d'informations

PAR CHÈQUE

Limitez le nombre de chéquiers en votre possession, conservez-les en lieu sûr

Complétez le début et la fin de chaque ligne d'un trait horizontal, pour que rien ne puisse être ajouté

Ne signez jamais de chèque sans y indiquer le montant et le bénéficiaire

QUE FAIRE EN CAS DE FRAUDE ?

• Si vous pensez avoir été victime de fraude, contactez votre agence au plus vite et déposez plainte auprès des forces de l'ordre.

Pour faire opposition sur votre carte bancaire, contactez votre agence Banque Palatine ou composez le numéro suivant :

01 49 37 80 34
7j/7 – 24h/24
(coût d'un appel vocal depuis la France).

• En cas de perte ou vol d'un chèque, avertissez votre agence ou contactez le Centre d'opposition national de la Banque de France au:

0 892 68 32 08
(0,34 TTC/min à partir d'un téléphone fixe).

BANQUE PALATINE
L'Art d'être Banquier

Plus d'informations sur :
www.palatine.fr/securite

Société Anonyme au capital de 688.802.680 Euros - Une Société du Groupe BPCE - Siège social : 42, rue d'Anjou - 75382 Paris Cedex 08 - Tél : 01 55 27 94 94 - Siège administratif : Le Péripôle - 10, avenue Val de Fontenay - 94131 Fontenay-sous-Bois Cedex - Tél : 01 43 94 47 47 – Immatriculation : 542 104 245 RCS Paris - CCP Paris 2071 - BIC BSPFFRPPXXX - Swift BSPF FR PP - N° TVA intracommunautaire FR77542104245 - Membre de la Fédération Bancaire Française et couverte par le fonds de garantie des dépôts et de résolution - Intermédiaire en assurance immatriculé à l'Orias sous le numéro 07 025 988 - Titulaire de la carte professionnelle « Transaction sur immeubles et fonds de commerce sans détention de fonds » n° CPI 7501 2015 000 001 258 délivrée par la Chambre de commerce et d'industrie de Paris Ile de France - garantie financière délivrée par la CEGC – 16 rue Hoche – Tour Kupka B – TSA 39999 – 92919 La Défense cedex – www.palatine.fr.

MKG 21015 - 12/2019 - Document non contractuel - iStockphoto

BANQUE DES ETI,
DE LEURS DIRIGEANTS
ET BANQUE PRIVÉE

ADOPTEZ LES BONS RÉFLEXES DE SÉCURITÉ

BANQUE PALATINE

9 RÉFLEXES SÉCURITÉ À ADOPTER DANS VOTRE ENTREPRISE

Respectez une procédure interne pour l'exécution des virements

Sensibilisez régulièrement vos collaborateurs au risque de fraude

Évitez le transport d'informations superflues

Maîtrisez la diffusion des informations concernant votre entreprise

Interrogez-vous sur les opérations inhabituelles (en particulier vers l'étranger)

Prenez le temps d'effectuer des vérifications

Veillez à la sécurité des accès aux services de banque à distance

Sécurisez les installations informatiques et les systèmes de stockage

Contactez rapidement la police et votre banquier en cas d'escroquerie (ou de doute)

DANS VOTRE **VIE PRIVÉE**

Vos moyens de paiement et leurs utilisations sont des cibles potentielles pour des tentatives de fraude. Quelques réflexes simples permettent de déjouer ou limiter leurs portées.

Comment sécuriser vos paiements?

• PAR CARTE OU MOBILE

- Conservez votre carte en lieu sûr.
- Surveillez régulièrement vos relevés de compte, pour repérer les opérations dont vous ne seriez pas à l'origine.
- Avant de partir à l'étranger, contactez votre conseiller ou agence pour connaître les mécanismes de protection de cartes et soyez vigilant lors de vos paiements ne demandant pas de code.
- Privilégiez les sites de confiance et sécurisés (adresse commençant par «https»).

Attention: en aucun cas un site de paiement ne demande le code confidentiel de votre carte bancaire.

• PAR CHÈQUE

- N'adressez jamais un chèque sur une sollicitation par email.
- Méfiez-vous des chèques reçus d'un montant supérieur à celui demandé et ne reversez jamais d'argent sans être certain de la validité du chèque, il pourrait s'agir d'une fraude.

Comment veiller à votre sécurité en ligne?

• MAÎTRISEZ LA DIFFUSION DES INFORMATIONS
Il est important de veiller à vos publications sur Internet afin de ne pas donner trop d'informations qui pourraient être utiles aux cyberattaquants pour mener des actions frauduleuses.

• SOYEZ VIGILANT AVEC VOS INTERLOCUTEURS
Les organismes ne demandent pas d'informations sensibles par email ou téléphone, si vous n'en avez pas fait la demande. En cas de doute, contactez-le via le numéro de téléphone habituel (pas celui indiqué dans le mail concerné) pour vérifier la véracité de la demande. Cette fraude est communément appelée le *phishing*.

• SÉCURISEZ VOS COMPTES
Avec des mots de passe différents et difficilement identifiables.

DANS VOTRE **ENTREPRISE**

Dans votre sphère professionnelle, vous pouvez être confronté à des situations à risques. Les entreprises sont dans la ligne de mire de *hackers* avec plusieurs types d'attaques. Une vigilance constante et accrue est nécessaire face à ces pratiques qui évoluent constamment.

Comment repérer une tentative de fraude?

Une analyse, une vérification et un contrôle des motifs évoqués sont nécessaires pour déjouer une tentative de fraude. En suivant régulièrement vos mouvements bancaires, vous participez déjà au dispositif de lutte contre la fraude.

Quelques signes auxquels être vigilant

Une commande atypique; un courrier mal rédigé; une demande de données confidentielles; une sollicitation urgente pour une opération financière par mail ou téléphone; une demande de mise à jour d'information par lien cliquable; une nouvelle domiciliation d'un prestataire ou client ou bien encore un règlement supérieur à une commande.

Comment être acteur de la lutte contre la fraude ?

• SENSIBILISEZ VOS COLLABORATEURS
Un rappel régulier des procédures et l'importance de ne pas y déroger ainsi que des cas pratiques réguliers renforcent l'ensemble du dispositif de prévention.

• METTEZ EN PLACE DES SEUILS DE DÉLÉGATIONS
Le contrôle interne est un des piliers de la lutte contre la fraude en entreprise. La mise en place de procédures comme les montants autorisés, la double vérification ou encore la capacité à préparer/valider des ordres de paiement est primordial pour votre sécurité.

• SÉCURISEZ VOS INSTALLATIONS
Définition d'une politique de sécurité; contrôle des accès au réseau et aux applications; sécurisation du réseau informatique et mise en place de mots de passe robustes; mises à jour régulières des applis et antivirus ainsi que la mise en place d'authentification pour les opérations à risque. Plus d'infos sur le site de l'ANSSI: http://www.ssi.gouv.fr/entreprise

• MAÎTRISEZ LA DIFFUSION DES INFORMATIONS
Pour ne pas mettre en péril votre entreprise, adoptez une très grande vigilance sur la teneur des éléments diffusés (réseau sociaux, courriels demandant des informations sensibles, mise en ligne d'organigramme etc.). Ces éléments seront utilisés par les fraudeurs pour s'authentifier auprès de vos équipes ou intervenants de confiance et passer comme interlocuteur de bonne foi.