Fiche technique

# Internet et e-banking : comment se protéger de la fraude

## De quoi s'agit-il ?

Le nombre de fraudes augmente d'année en année, un constat inquiétant. Les cybercriminels utilisent des techniques de plus en plus élaborées. Il est donc toujours plus difficile de détecter à temps une escroquerie ou une attaque ciblant un compte bancaire ou une carte de crédit. De nombreux escrocs ont recours à des astuces psychologiques pour mettre la pression sur leurs victimes. Dans le pire des cas, ils arrivent à obtenir l'accès aux mots de passe, données bancaires et autres données personnelles sensibles. Cette fiche technique vous indique quelles sont les méthodes les plus répandues et comment vous protéger des fraudes.

## E-banking – attention aux attaques de phishing

Bon nombre de Suisses effectuent leurs opérations bancaires en ligne sur PC, tablette ou smartphone. Les banques font leur possible pour mettre à disposition de leur clientèle des systèmes d'e-banking qui soient sûrs. La plupart des attaques ne ciblent pas les banques elles-mêmes, mais les appareils des clients. Les méthodes suivantes sont particulièrement répandues.

**Phishing / hameçonnage :** le terme « phishing » signifie « pêche aux mots de passe ». Les criminels tentent par ce moyen d'obtenir les données confidentielles de clients bancaires pour avoir accès à leurs économies. Des analyses de la Prévention Suisse de la Criminalité (PSC) montrent que les attaques de phishing peuvent se dérouler de différentes manières. Néanmoins, on retrouve certaines caractéristiques typiques :

- Les escrocs envoient des e-mails frauduleux dans lesquels ils se font passer par exemple pour des employés de banque. Ils essaient de convaincre les clients que les informations relatives à leur compte ou leurs données d'accès ne sont plus sûres ou plus actuelles, et donc qu'elles doivent être actualisées à l'aide du lien indiqué dans l'e-mail.
- Le lien ne renvoie pas vers le site Internet de la banque du client, mais vers un site web frauduleux qui ressemble à s'y méprendre à celui de la banque. Toutes les données personnelles qui sont saisies sur ce site se retrouvent alors entre les mains des escrocs.
- À l'aide des données d'accès volées, ils transfèrent de l'argent très rapidement, souvent des dizaines de milliers de francs qu'ils débitent du compte de leurs victimes. Dans bien des cas, cet argent est perdu.

### Conseils : prenez garde aux points suivants quand vous utilisez votre e-banking

Pour utiliser votre e-banking de manière sûre, suivez les conseils usuels à ce sujet. Vous trouverez ici le résumé des principales règles à appliquer.

- Saisissez toujours manuellement l'adresse de la page de connexion à votre e-banking dans la barre d'adresse de votre navigateur. Ne recherchez pas cette page sur les moteurs de recherche (Google, Bing, etc.).
- Si vous n'êtes pas sûr(e) d'être sur la bonne page, vérifiez qu'il s'agit bien d'une connexion SSL sécurisée (https://, icône cadenas).
- L'adresse Internet correcte est affichée à côté du cadenas ou apparaît après un clic sur ce dernier.
- Vérifiez que l'adresse Internet de la page de la connexion est écrite correctement. Les fraudeurs ne modifient souvent que quelques lettres dans l'adresse.
- Mettez immédiatement fin au processus de connexion si une interruption du système se produit (p. ex. l'apparition subite d'un écran blanc) ou si des messages d'erreur inhabituels apparaissent à l'écran (p. ex. « Le système est actuellement surchargé. Nous vous prions de bien vouloir patienter et de réessayer de vous connecter plus tard »).
- Lorsque vous êtes en déplacement, cachez bien votre identifiant et votre mot de passe, et vérifiez que personne ne regarde par-dessus votre épaule.
- Utilisez votre e-banking uniquement depuis des appareils connus et sécurisés. La connexion depuis un appareil mis à disposition de tout le monde, par exemple dans un hôtel, est à proscrire.
- Contactez immédiatement votre banque s'il se passe quelque chose d'étrange.

(Suite)

**Phishing via les moteurs de recherche :** bon nombre de personnes accèdent à leur e-banking en cherchant la page de connexion de leur banque sur Internet (sur Google, Bing, Yahoo, etc.). Elles ne savent pas que cela peut être dangereux. En effet, les escrocs font aussi la publicité de leurs sites d'e-banking frauduleux sur les moteurs de recherche les plus utilisés :

- Lorsqu'une recherche est effectuée, le faux site de la banque s'affiche de manière bien visible – souvent tout en haut de la liste des résultats avec la mention « Sponsorisé », « Publicité » ou « Annonce ».
- En cliquant sur un tel lien, on se retrouve sur une fausse page d'e-banking qui ressemble énormément au vrai site de la banque.
- Si l'on saisit ses données d'accès d'e-banking, ces dernières se retrouvent entre les mains des escrocs sans qu'on le sache.
- Avec les données de connexion, les escrocs peuvent se connecter sur la vrai page d'e-banking et voler de l'argent au détenteur des comptes.

**Phishing par SMS (smishing) :** les SMS et autres services de messagerie comme WhatsApp sont aussi fréquemment utilisés pour mener des attaques. Celles-ci sont particulièrement dangereuses, car bon nombre de moyens qui permettent de reconnaître les e-mails de phishing sont inefficaces :

- Les escrocs envoient des messages frauduleux et se font passer pour des employés de banque ou pour les collaborateurs d'un service technique.
- Ils font croire par exemple au destinataire du message que ses données d'accès ou que les informations relatives à son compte ne sont plus sûres.
- C'est sous ce prétexte que le client est incité à actualiser son identifiant et son mot de passe en cliquant sur un lien contenu dans le message.
- Mais le lien renvoie vers un site web frauduleux qui ressemble en tout point à la page de connexion habituelle de la banque.
- Les malfaiteurs n'ont plus qu'à récupérer les données de connexion qui ont été saisies sur cette fausse page web.

**Voice phishing (vishing) :** les fraudeurs n'ont pas peur de contacter les clients bancaires par téléphone. Ces attaques, appelées tentatives de « vishing », augmentent toujours plus :

- Les fraudeurs appellent les clients et se présentent sous une fausse identité. Ils se font passer par exemple pour des fonctionnaires de police, des employés de banque ou encore pour des collaborateurs travaillant dans de grandes entreprises telles que Microsoft ou Swisscom.
- Durant la conversation, les escrocs mettent la pression sur leurs victimes, utilisent diverses techniques de manipulation et font planer la menace de graves conséquences – tout cela dans le but d'amener les clients bancaires à effectuer des actions irréfléchies.
- Ils peuvent par exemple exiger de la personne qu'elle installe un nouveau programme de sécurité sous prétexte que son PC est infecté par un virus informatique.
- Dans la majorité des cas, il s'agit de logiciels malveillants. Si une victime installe ce programme, les escrocs peuvent accéder à ses identifiants et mots de passe, et donc à ses comptes et à ses économies.

### Conseils : comment vous protéger des attaques de phishing

Les escrocs développent sans cesse leurs techniques et tentent d'exploiter au maximum le potentiel de la technologie. Pour ce faire, ils associent souvent le phishing, le vishing et le smishing. Faites attention aux points suivants :

- Aucune banque ou organisation sérieuse ne vous demandera votre identifiant et votre mot de passe par e-mail, SMS, WhatsApp ou téléphone.
- Ne donnez donc jamais de données ou d'informations confidentielles par téléphone, par e-mail ou sur des sites web que vous ne connaissez pas.
- Effacez les messages suspects et videz immédiatement la corbeille. Faites-le également si vous n'êtes pas sûr(e) à 100 % de l'authenticité d'un message.
- Soyez très méfiant(e) lorsque vous recevez un e-mail que vous n'attendiez pas.
- Ne vous laissez pas intimider si quelqu'un vous demande des données personnelles en faisant planer la menace d'une perte d'argent, d'un dépôt de plainte ou du blocage de votre carte.
- Utilisez des mots de passe sûrs et mettez toujours à jour votre système d'exploitation, votre navigateur Internet et votre logiciel de messagerie. Actualisez régulièrement votre logiciel antivirus.
- L'utilisation d'un filtre anti-spams ou d'un logiciel anti-hameçonnage peut aussi aider à repérer les sites et e-mails d'hameçonnage. Ne téléchargez les logiciels que sur les boutiques d'applications officielles.
- Examinez régulièrement vos relevés bancaires et relevés de carte de crédit, et informez immédiatement votre banque en cas d'irrégularité.

Sources : Prévention Suisse de la Criminalité, Stiftung für Konsumentenschutz, www.ebas.ch/phishing, www.cybercrimepolice.ch

## Placements financiers et immobilier – attention aux escroqueries

Les cybercriminels utilisent tous les moyens possibles et les technologies les plus modernes pour tromper les clients bancaires, les consommateurs et les internautes. L'Ombudsman des banques suisses appelle à la plus grande prudence, notamment parce que les personnes qui effectuent par exemple des paiements de leur propre chef sans savoir qu'elles sont victimes d'une fraude doivent bien souvent en supporter les conséquences. En effet, dans de tels cas, les banques n'assument généralement aucune responsabilité. Les escroqueries listées ci-après surviennent particulièrement souvent :

**Fraude à l'investissement en ligne :** à l'aide d'annonces accrocheuses envoyées par e-mail ou postées sur les réseaux sociaux, les escrocs promeuvent de prétendues plateformes d'investissement qui promettent de l'argent rapide ou de grosses sommes. Pour gagner la confiance des victimes, ils copient les sites web de médias sérieux comme la RTS ou *Blick*. Sur les sites frauduleux créés, ils publient des articles mettant en scène des personnalités – qui ne savent rien de tout cela. Selon la police cantonale de Zurich, lorsqu'une victime s'inscrit sur l'une de ces plateformes frauduleuses, elle ne tarde pas à être contactée par e-mail ou par téléphone. L'objectif des escrocs est que les victimes versent rapidement de l'argent. Cet argent est ensuite, selon eux, investi dans des produits de placement ou des cryptomonnaies. Mais ce n'est pas le cas. À la place, l'argent se retrouve directement entre les mains des fraudeurs. Derrière ces escroqueries se cachent des criminels agissant au niveau international, qui utilisent des technologies de pointe et opèrent même avec leurs propres centres d'appel. Ne vous laissez pas leurrer par des promesses irréalistes. Aucun prestataire financier sérieux ne vous fera miroiter des gains supérieurs à la moyenne en peu de temps. Suivez les recommandations des autorités et de la police. L'Autorité fédérale de surveillance des marchés financiers (FINMA) gère par exemple une liste d'alerte, que vous retrouverez sur cette page : www.finma.ch/fr/finma-public/liste-d'alerte. Signalez les offres suspectes à la FINMA.

**Fraude des agents financiers :** les escrocs recherchent régulièrement des « agents financiers ». Ils ciblent les personnes en recherche d'emploi et les personnes en difficulté financière en publiant des offres d'emploi alléchantes sur des plateformes en ligne, sur les réseaux sociaux et dans la presse. Les fraudeurs disposent souvent d'un site web qui a l'air sérieux ou usurpent le nom d'une entreprise. Attention : ces méthodes cachent souvent des intentions criminelles. Les escrocs utilisent notamment les comptes bancaires des personnes recrutées pour transférer de l'argent sale. De plus en plus, ils exigent la conversion des actifs en cryptomonnaie, par exemple en bitcoins. En contrepartie, une compensation financière sous la forme d'une provision doit être versée. Méfiez-vous lorsque l'on vous promet de l'argent rapide contre peu d'efforts. En effectuant de telles opérations, on peut se rendre coupable de blanchiment d'argent.

**Fraude à l'acompte :** prudence également lors de la recherche d'un bien immobilier ou d'un objet à acheter. Les autorités signalent une hausse des fraudes liées à de fausses annonces. Les malfaiteurs copient par exemple des annonces de logements à louer et promeuvent ces logements à la vente, à des prix alléchants, sur des portails immobiliers bien connus, sur les réseaux sociaux ou sur de faux sites web qui paraissent sérieux. Les annonces servent d'appât. Les personnes qui y répondent sont contactées par des escrocs professionnels. Ceux-ci exigent par exemple une copie du passeport ou de la carte d'identité. Pour paraître fiables, ils se présentent aussi avec une pièce d'identité – mais celle-ci est souvent fausse ou appartient à une précédente victime. Les malfaiteurs prétendent réserver le bien immobilier pour la personne intéressée. Avant qu'une visite puisse être organisée, ils demandent un acompte. Généralement, cet argent disparaît et les malfaiteurs restent introuvables. Conseil : ne croyez pas à des annonces qui sont trop belles pour être vraies. Ne versez jamais d'argent via un service de transfert si vous n'avez pas de contrat valable et que vous n'avez jamais visité le bien. Jouez la sécurité et montrez toujours une annonce douteuse à un expert chevronné.

## Autres formes de fraude répandues

Il existe en outre d'autres formes de fraude. Ces abus touchent particulièrement les personnes de 55 ans et plus, comme le montre une étude publiée par Pro Senectute. L'organisation estime le montant des dommages à environ 675 millions de francs par année. Mais les fondateurs de start-up peuvent aussi être les victimes d'escroqueries. Lisez ci-après les types de fraude qu'il est important de connaître pour pouvoir s'en protéger :

**Fraude du petit-fils ou du neveu :** le malfaiteur se fait passer pour un proche qui se trouve en difficulté financière et a urgemment besoin de l'aide de sa famille. Il appelle la victime, lui fait deviner de qui il s'agit, cherche à obtenir des informations et les utilise ensuite dans la conversation. Il fait semblant d'être la personne en question et de ne pas pouvoir venir chercher l'argent lui-même, pour diverses raisons. À la place, il envoie une amie ou une connaissance.

**Conseil :** méfiez-vous si vous ne reconnaissez pas immédiatement un prétendu membre de votre famille au téléphone. En cas de doute, raccrochez. Et ne remettez jamais d'argent ou d'objets de valeur à des inconnus, même s'ils se présentent comme étant des tenants de l'autorité tels que des policiers, des avocats ou des collaborateurs judiciaires.

**Appel choc :** cette forme particulièrement agressive d'arnaque téléphonique consiste à se faire passer pour une personne d'autorité comme un médecin-chef, un avocat ou un policier. Cette personne transmet un message, faux mais crédible, qui vise à créer le choc chez la victime. Le message concerne souvent un membre de la famille, soi-disant en détresse ou en grand danger. Les malfaiteurs demandent à leurs victimes de remettre de l'argent ou des objets de valeur à un coursier pour aider leur proche. Ces dernières, en état de choc, n'arrivent souvent pas à penser rationnellement et tombent dans le piège.
**Conseil :** les appels choc se reconnaissent uniquement par le contenu du message, toujours associé à une demande d'argent. Méfiez-vous si vous recevez un message choquant, que l'on vous met la pression et que vous devez donner de l'argent. Même chose ici : raccrochez simplement le combiné.

**Inscriptions aux registres :** après avoir enregistré leur nouvelle entreprise au registre du commerce, les entrepreneurs reçoivent souvent du courrier les invitant à inscrire leur entreprise dans divers registres. À première vue, les formulaires reçus ont tout l'air de documents officiels émanant des autorités. Mais il s'agit d'engagements payants pour s'inscrire dans des registres d'entreprises, de professionnels, de marques, des annuaires téléphoniques, des plans de localité et autres registres similaires, qui n'ont aucune utilité. Ne souscrivez en aucun cas ces contrats.
**Conseil :** ne tombez pas dans le piège d'une telle « arnaque aux registres ». Réglez uniquement les factures officielles du registre du commerce du canton compétent et d'éventuels partenaires tels que les notaires et les administrateurs fiduciaires.

## Liens importants

Il existe divers sites et pages Internet qui permettent de s'informer sur les formes d'escroquerie actuelles et d'obtenir des conseils utiles pour se protéger contre ces tentatives de fraude.

- Prévention Suisse de la Criminalité : **www.skppsc.ch/fr**
- « eBanking – en toute sécurité ! » : **www.ebas.ch/fr**
- Police cantonale vaudoise : **www.votrepolice.ch/cybercriminalite-cat**
- Office fédéral de la cybersécurité : **www.ofcs.admin.ch**

## Pour être bien conseillé

VZ VermögensZentrum est en Suisse le principal prestataire indépendant de services financiers. De nombreux clients profitent de notre expertise : ils préparent leur retraite, investissent de manière intelligente, financent leurs biens immobiliers de façon avantageuse, règlent leur succession et cessent de payer plus d'impôts que nécessaire.

Les entreprises et caisses de pension sont aussi à la bonne adresse chez VZ : elles améliorent les prestations d'assurance et de prévoyance, obtiennent de meilleurs rendements de leurs placements et économisent en même temps des primes, taxes et impôts.

Pour toute question financière, VZ est de bon conseil.

**VZ VermögensZentrum SA (siège principal)**
Avenue de la Gare 50, 1003 Lausanne
Tél. 021 341 30 30
vzlausanne@vzch.com
www.vzch.com

Aarau I Affoltern am Albis I Baden I Bâle I Bellinzone I Berne I Berthoud
Brigue I Coire I Fribourg I Genève I Horgen I Kreuzlingen I Lausanne
Lenzbourg I Liestal I Lucerne I Lugano I Meilen I Neuchâtel I Nyon I Olten
Rapperswil I Rheinfelden I Schaffhouse I Sion I Soleure I St-Gall I Sursee
Thoune I Uster I Vevey I Wil SG I Winterthour I Zoug I Zurich