

Le paysage de la fraude évolue rapidement, avec de nouvelles tactiques plus sophistiquées qui émergent rapidement. Il est essentiel de rester vigilant et de prendre des mesures proactives pour vous protéger, vous et votre entreprise, contre la fraude.

L'intégration en cours d'UBS et de Credit Suisse offre aux fraudeurs une occasion unique de contacter nos clients en prétendant appartenir à notre organisation ou en vendant de faux plans d'investissement utilisant le nom d'entités UBS. Il peut s'agir d'un moyen d'obtenir des informations de votre part ou de vous inciter à envoyer de l'argent à des comptes non liés. Soyez vigilant si vous êtes contacté par une personne inconnue. Dans le cadre de ses mesures de sécurité, UBS peut vous demander de fournir des informations d'identification lors de rappel de vérification. Toutefois, nous ne demanderons en aucun cas d'informations sensibles, en particulier des identifiants de connexion, par exemple un nom d'utilisateur et un mot de passe, que ce soit par téléphone, par e-mail ou par SMS.

Cette note a pour but de vous sensibiliser et de vous offrir des conseils pratiques pour vous protéger contre les fraudeurs.

Ingénierie sociale - fraude alimentée par l'IA

Les fraudeurs ont souvent recours à des tactiques d'ingénierie sociale pour créer un sentiment d'urgence et de pression émotionnelle afin de manipuler les individus à divulguer des informations sensibles ou à autoriser des transactions frauduleuses. En utilisant l'intelligence artificielle (IA), les fraudeurs peuvent désormais générer des courriels de phishing réalistes, des imitations vocales ou des interactions de chatbot qui imitent des sources de confiance.

- Faites attention aux demandes inhabituelles ou urgentes (par exemple, pour vérifier les détails du compte) reçues par e-mail, téléphone ou SMS.
- Soyez attentif aux e-mails ou messages mal rédigés contenant des liens ou des fautes d'orthographe.
- Vérifiez l'authenticité d'une demande avant de partager toute information avec des personnes que vous ne connaissez pas. Si vous avez des doutes, ne cliquez pas sur les liens ou ne téléchargez pas les pièces jointes avant de les avoir vérifiés.
- Vérifiez toujours les nouvelles demandes de paiement, ainsi que toute demande que vous recevez vous demandant de mettre à jour vos coordonnées existantes et/ou les détails bancaires.
- Restez vigilant face aux appels frauduleux ou non autorisés. Ne partagez jamais d'informations personnelles telles que des mots de passe, des détails financiers ou des codes d'authentification sans avoir vérifié que la demande est légitime.

Réseaux sociaux et identité synthétique

Les plateformes de réseaux sociaux deviennent de plus en plus une ressource précieuse pour les cybercriminels afin de recueillir des informations personnelles et de créer des identités synthétiques. En combinant des données réelles avec des informations fabriquées, les criminels peuvent établir de fausses identités difficiles à détecter.

- Limitez les informations personnelles que vous partagez publiquement sur les réseaux sociaux, telles que les dates de naissance, l'adresse de votre domicile et vos projets de voyage.
- Soyez sélectif avec vos connexions et n'acceptez que les demandes de personnes que vous connaissez et en qui vous avez confiance.
- Vérifiez régulièrement vos paramètres de confidentialité pour vous assurer que vous partagez des informations uniquement avec des personnes de confiance.
- Surveillez votre présence en ligne et effectuez des recherches régulières pour vous assurer qu'aucun faux profil n'est créé utilisant vos informations.

Banque numérique et fraude aux paiements

L'essor de la banque numérique et du commerce électronique a rendu la fraude aux paiements en ligne plus courante. Les cybercriminels exploitent les vulnérabilités des processus d'authentification des titulaires de carte, utilisant souvent des informations de carte volées ou frauduleuses.

- Assurez-vous que les sites Web sont sécurisés avant d'effectuer des transactions et que l'URL est correctement saisie. Un site Web sécurisé commencera par: <https://>
- Utilisez l'authentification multifactorielle dans la mesure du possible. Si ce n'est pas disponible, utilisez des mots de passe forts et uniques et gérez-les dans un gestionnaire de mots de passe.
- Surveillez régulièrement vos comptes et mettez en place des alertes pour toute transaction inhabituelle ou non autorisée.
- Méfiez-vous des points d'accès Wi-Fi publics. Évitez de les utiliser pour les services bancaires en ligne, l'envoi d'e-mails ou la mise à jour des réseaux sociaux, car les pirates peuvent accéder à vos informations.
- Téléchargez uniquement des logiciels à partir de magasins d'applications de confiance et maintenez-les à jour.
- Assurez-vous que votre logiciel antivirus et votre pare-feu sont à jour et régulièrement mis à jour par des fournisseurs de confiance.

Fraude à l'investissement

Les fraudeurs ciblent de plus en plus les particuliers et les entreprises par le biais d'escroqueries à l'investissement, en particulier sur les marchés à haut risque comme les cryptomonnaies. Ils utilisent des promesses de rendements élevés ou des informations privilégiées pour attirer les victimes dans des investissements frauduleux.

- Soyez prudent face aux opportunités d'investissement non sollicitées ou aux offres « trop belles pour être vraies ». Méfiez-vous des ventes sous pression. Traitez toute opportunité d'investissement annoncée en ligne avec scepticisme. Ne confiez pas d'argent à quelqu'un qui n'agit pas manifestement au nom d'une institution fiable et réglementée.
- Consultez un conseiller financier expert et de confiance avant de prendre des décisions financières importantes.
- Prenez le temps de rechercher et de vérifier tout investissement, ne vous laissez jamais presser lorsque vous investissez.

En restant vigilant et en suivant les meilleures pratiques, vous pouvez réduire votre exposition à la fraude et protéger vos finances. Si vous pensez être victime d'une fraude ou si vous remarquez une activité/transaction inhabituelle sur votre compte UBS, veuillez contacter votre conseiller à la clientèle UBS.