AFOC AUBE

Présenter informer conseiller

COMPTES

Reconnaître et déjouer les fraudes à l'ingénierie sociale

Pour mieux déjouer les fraudes à l'ingénierie sociale, il faut pouvoir les identifier à temps. Les fraudeurs utilisent la manipulation et l'usurpation d'identité pour obtenir la réalisation d'une opération bancaire à leur profit. Découvrez ces fraudes et les moyens pour vous protéger.

Reconnaître une fraude au président ou au dirigeant

L'escroc usurpe l'identité d'un **dirigeant** ou prétend agir sur son ordre. Il demande à un collaborateur d'**effectuer en urgence un virement**, sous prétexte d'un rachat d'entreprise, d'une OPA (Offre Publique d'Achat), d'une dette à régler, de l'exécution d'un contrat ou toute autre situation d'urgence.

Certains points doivent vous alerter :

- la demande est présentée comme urgente et confidentielle (il pourra être demandé de passer sur un numéro de téléphone privé le cas échéant pour plus de confidentialité);
- usage de la flatterie, de l'autorité ou de l'intimidation;
- recours à une tierce personne (faux notaire ou faux avocat) qui indiquera l'opération à réaliser;
- caractère inhabituel du montant, du bénéficiaire et du pays destinataire des fonds;
- utilisation abondante de détails sur l'entreprise pour rassurer;
- proposition de passer sur un numéro de téléphone privé;
- exigence de confidentialité concernant la demande afin d'éviter toute fuite.

En savoir plus sur la fraude au dirigeant

Reconnaître une fraude aux modifications des coordonnées bancaires

L'escroc usurpe l'identité d'un **fournisseur** ou **bailleur de l'entreprise**. Il indique **avoir changé ses coordonnées bancaires** et souhaite donc que l'entreprise les mette à jour. Il pourra ainsi détourner à son profit le paiement des prochaines factures ou loyers de la personne usurpée.

Certains points doivent vous alerter :

- transmission, pour rassurer, d'informations précises, comme une vraie facture en cours dont l'IBAN aura été modifié;
- changement soudain des coordonnées bancaires;
- pays inhabituel de l'IBAN qui peut être incohérent par rapport à la localisation de la société usurpée.

Vérifier un IBAN avec Diamond

Reconnaître une fraude au faux technicien

L'escroc peut aussi usurper l'identité **d'un technicien d'un service informatique**. Cette fraude peut intervenir lorsque le client a téléchargé un virus qui bloque son écran. En allumant son ordinateur, son écran affiche un numéro de téléphone à appeler.

Dans ce scénario, l'escroc usurpe l'identité d'un **technicien de la banque** (technicien du service informatique par exemple). Il indique devoir faire des vérifications et demande à prendre le contrôle du poste informatique à distance. Il pourra demander l'exécution d'un **virement « test »** par exemple.

Certains de ces points doivent vous alerter :

- réception d'un appel de techniciens non sollicités;

- demande de prise de poste à distance et celle de cliquer sur un lien hypertexte.

Appelez immédiatement votre conseiller.

En cas de suspicion de fraude ou de fraude avérée : réagissez !

En cas d'attaque informatique, déposez également une plainte auprès des forces de l'ordre en apportant tous les éléments à votre disposition.

Les bonnes pratiques pour vous protéger

Ces scénarios reposent sur une connaissance précise de l'entreprise et de son organisation.

- **Sensibilisez les collaborateurs sur les informations** qu'ils divulguent sur l'entreprise, notamment sur les réseaux sociaux.
- **Protégez votre système d'information** pour empêcher les piratages informatiques.
- **Sensibilisez les services** comptables et financiers, mais aussi le secrétariat et le standard, pour repérer les appels suspects.
- **Vérifiez l'adresse mail du dirigeant** dont la terminaison est souvent différente de celle qu'il utilise habituellement.
- Organisez des **procédures de validation** engageant plusieurs personnes (saisie et validation) par exemple.
- Utilisez vos **moyens d'authentification ou de signature**. Ils sont personnels : ne les confiez jamais à personne. Refusez de saisir ou de valider une opération avec une authentification qui ne vous appartient pas.
- Recontactez votre interlocuteur par les moyens habituels et **demandez confirmation** de la demande : rappelez ou écrivez directement en utilisant le carnet d'adresse de l'entreprise.
- Ne cédez pas à l'impératif d'urgence, prenez le temps de faire les **vérifications d'usage**.
- **Refusez une demande de prise de contrôle** à distance de votre poste informatique.
- En **période de vacances**, redoublez de vigilance et répétez les consignes.

Guide des ordres de virement des entreprises

La Fédération Bancaire Française a édité un guide complet sur les fraudes à l'ingénierie sociale.

Consultez-le et diffusez le auprès de vos collègues

En cas de suspicion de fraude ou de fraude avérée : réagissez !

Appelez immédiatement votre conseiller.

En cas d'attaque informatique, déposez également une plainte auprès des forces de l'ordre en apportant tous les éléments à votre disposition.

ATTENTION
Votre banque ne vous demande jamais vos codes confidentiels, ni de transférer votre argent pour « sécuriser » vos fonds.

Si vous êtes démarché par une personne qui prétend être votre conseiller ou votre banquier et qu'il vous demande :

- Vos identifiants et mot de passe de votre Espace Client
- Votre code de carte de paiement
- De transférer votre argent vers un autre compte pour déjouer une arnaque

vous avez forcément affaire à un escroc.

Vous pouvez le signaler à la police ou à votre banque par un contre-appel, **mais en aucun cas vous ne devez donner vos codes à qui que ce soit.**