

Guide de réunion

Fraude par personnification

Présentation de l'activité



Dernière mise à jour : janvier 2026

Objectifs

Animer

une discussion au sein de l'entreprise afin de partager les bases de la sécurité sur le thème abordé.

Encourager

la prise de parole et le partage d'expériences liées à des attaques recourant aux techniques abordées durant l'atelier.

Détails de l'activité

Durée : 20 - 30 minutes

Clientèle visée : l'ensemble des employé(e)s

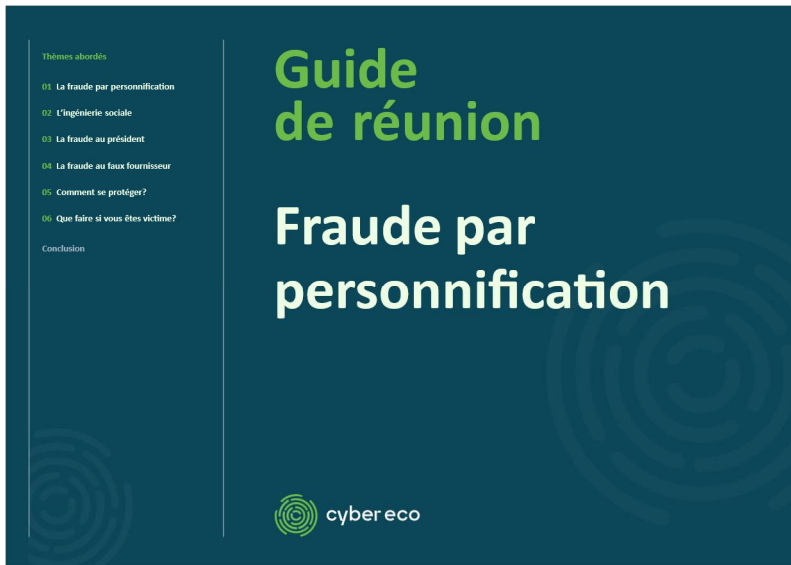
Objectifs	Responsabilité de la personne qui anime	Responsabilité des employé(e)s	Matériel recommandé
Couvrir les points essentiels du thème abordé	Présenter les questions ou sujets et commenter à l'aide des pistes fournies	Participer activement et répondre aux questions	Projecteur, tableau et marqueurs



Notes à l'intention de la personne animant l'atelier

Nous vous invitons à prendre connaissance des informations ci-dessus avant d'animer l'atelier, et d'utiliser les notes contenues dans les pages suivantes pour compléter l'information transmises à votre équipe.

Bonne présentation!



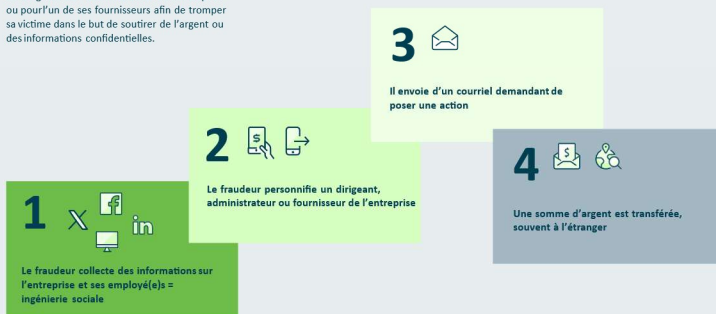
Bonjour et bienvenue à cet atelier!

La fraude a malheureusement pris de l'ampleur au cours des dernières années.

Puisque la **fraude par personification** n'y échappe pas, nous allons parler aujourd'hui. L'atelier devrait durer 20 à 30 minutes. Votre participation et vos questions sont essentielles!

La fraude par personnalisation

Stratagème qui consiste à se faire passer pour un dirigeant ou administrateur de l'entreprise ou pour l'un de ses fournisseurs afin de tromper sa victime dans le but de soutirer de l'argent ou des informations confidentielles.



Guide de réunion Définition Fraude par personnalisation

L'ingénierie sociale

Porte d'entrée menant à la fraude par personnalisation, l'ingénierie sociale est une technique de manipulation utilisée dans le but d'inciter quelqu'un à révéler de l'information plus ou moins confidentielle.

Cette information est ensuite utilisée par les cybercriminels pour personnaliser, par exemple, un membre de la direction d'une entreprise ou encore un fournisseur.

Les cybercriminels peuvent aussi collecter de l'information publique directement sur Internet.

Où

Endroits où trouver de l'information servant à rédiger le courriel destiné à une victime

Quoi

Type d'information recherchée

Page 3 [Lire le contenu de la diapo]

L'ingénierie sociale consiste à **collecter des informations sur l'entreprise et ses dirigeants** dans le but de **mener des attaques frauduleuses**.

Les fraudeurs exploitent également les données accessibles publiquement. Par exemple :

- Les **réseaux sociaux professionnels** (LinkedIn, Facebook, Instagram, etc.)
- Le **site web de l'entreprise** : qui est le président? Qui est le directeur des finances ou comptable?
- Les **articles, communiqués de presse ou conférences**
- Ou en appelant directement l'entreprise

Les « **approches** » peuvent se faire en personne, en ligne ou par téléphone. **L'objectif** : obtenir des informations personnelles ou financières, sensibles.

La **stratégie** : se faire passer pour des employés de confiance ou des entités proches de l'entreprise.

Ces informations leur permettent de :

- **Personnaliser une attaque** (ex. : mentionner un dirigeant ou un projet en cours)
- **Gagner en crédibilité** auprès de la cible
- **Créer un sentiment de légitimité ou d'urgence**

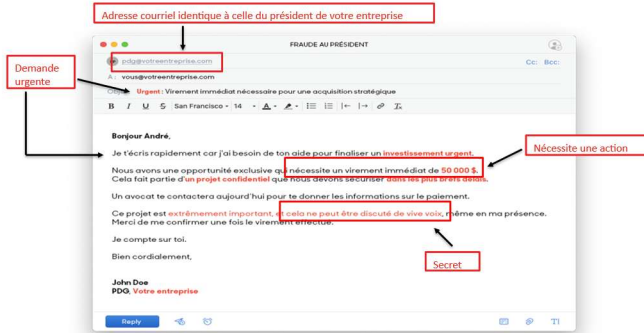
Exemple 1 : Un courriel semblant provenir d'un cadre supérieur, demandant un transfert urgent de fonds ou l'accès à un document confidentiel.

Les cybercriminels exploitent désormais l'IA pour rendre leur attaque encore plus crédible et difficile à détecter. Grâce à des outils d'IA générative, ils peuvent créer des courriels, des messages ou des appels vocaux parfaitement rédigés, imitant le ton et le style d'une organisation ou d'un individu. L'IA permet aussi de produire des hypertrucages ou deepfakes (images, vidéos, voix) pour renforcer la confiance et manipuler les victimes.

Réflexion : Comme entreprise, est-ce que l'on donne trop d'informations sur les réseaux sociaux et notre site Internet?

La fraude au président

Un fraudeur réussit à compromettre la boîte courriel du président d'une entreprise et envoie, à partir de cette adresse, un message urgent et confidentiel à la personne responsable des finances. Dans ce courriel, il demande le transfert immédiat de fonds.



7

Page 4 [Lire la mise en situation de la diapo]

Notes importantes

La fraude au président est une **tentative de manipulation** dans laquelle une personne malveillante se fait passer pour un dirigeant de l'entreprise — président, directeur général ou cadre supérieur — pour convaincre un employé, souvent dans les finances ou la comptabilité, d'effectuer un **virement urgent** vers un compte frauduleux.

Le fraudeur utilise des techniques très convaincantes : il peut envoyer un courriel qui semble authentique ou appeler directement, en créant un **sentiment d'urgence** et en demandant de garder la demande **confidentielle**. L'objectif est de pousser l'employé à agir rapidement, sans vérifier ni suivre les procédures habituelles.

Indicateurs de fraude

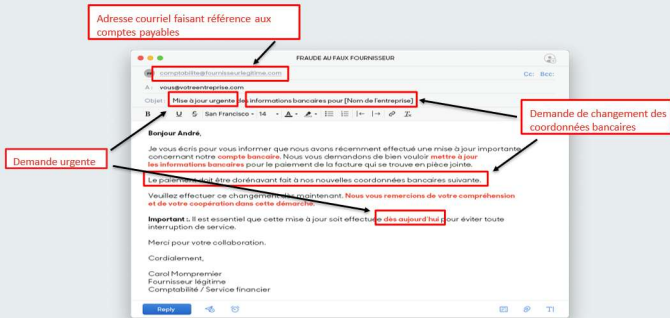
- La demande peut provenir de l'adresse courriel réelle du président (qui a été piratée) ou d'une adresse très semblable à une lettre près.
Un bon truc : ce qui vient après le @ est un nom de domaine qu'un fraudeur ne peut pas recréer. Il peut, par contre, modifier une lettre pour laisser croire qu'il s'agit du même nom de domaine.
- La transaction doit être effectuée en **mode d'urgence**
- Dans notre exemple de courriel, la demande est **confidentielle**
- On demande de **poser une action** (dans ce cas-ci une transaction de 50 000 \$)
- La notion de **secret** ressort, la demande ne peut pas être discuté de vive voix
- Dans l'exemple, le fraudeur demande une confirmation de la transaction. Le fraudeur donne souvent un numéro de téléphone ou un service de messagerie instantanée, comme WhatsApp, en misant sur le fait que c'est confidentiel et que l'employé ciblé ne doit pas passer par les canaux formels. On comprend ici que le fraudeur veut s'assurer que l'employé ne contacte pas le vrai président par courriel, Teams ou tout autre canal officiel.

Autres indicateurs possibles dans ce type d'arnaque

- Le président/dirigeant est à l'extérieur lorsqu'on reçoit la demande
- C'est une demande INHABITUELLE

La fraude au faux fournisseur

Un fraudeur se fait passer pour le fournisseur d'une entreprise. Il envoie à l'un des employés un courriel dans lequel est annoncé un changement dans les modalités de paiement. Le message contient les « nouvelles » coordonnées bancaires et demande que les prochains paiements soient envoyés à ce « nouveau » compte.



Page 5 [Lire la mise en situation de la diapo]

L'arnaque au faux fournisseur est une **tentative de manipulation** où une personne malveillante se fait passer pour un fournisseur de l'entreprise afin de convaincre un employé, souvent dans les finances ou la comptabilité, d'effectuer un **changement de coordonnées bancaires** vers un compte frauduleux.

Dans notre exemple, nous voyons une demande écrite provenant d'un faux fournisseur

- On y demande de **mettre à jour** les **informations bancaires** dans le système de l'entreprise
- Si la demande est **acceptée sans vérification**, **l'argent est envoyé au fraudeur** et NON au fournisseur officiel

IMPORTANT

- L'adresse courriel **pourrait** être celle du fournisseur officiel. On doit néanmoins vérifier en utilisant une autre source. En téléphonant au fournisseur, par exemple.
- L'adresse courriel **pourrait ressembler** à celle du fournisseur. Encore là, on doit vérifier en utilisant une autre source. Le téléphone, par exemple.
- Les mentions d'urgence et de CHANGEMENT DE COORDONNÉES BANCAIRES devraient nous mettre la puce à l'oreille.

Comment se protéger?

Personne n'est à l'abri d'une fraude! Faire preuve de vigilance et rester au fait des stratagèmes de fraude sont deux grands alliés, en plus des conseils ci-dessous!

Ne répondez **jamais** à une demande de transaction sans vérifier auprès d'une **seconde source**

- Toujours valider une demande urgente auprès d'une seconde source**
 - Au sujet d'une transaction ou de coordonnées bancaires
- Limiter les informations partagées sur les réseaux sociaux**
 - On ne partage aucun renseignement personnel ni aucune information confidentielle
 - On garde en tête que toute information publiée n'est jamais entièrement privée
- Respecter les procédures de l'entreprise**
 - Pour la validation d'opérations financières et le changement de comptes bancaires

9

Page 6 [Lire le contenu de la diapo]

Voici comment nous pouvons nous protéger **ensemble!**

Avant de faire un virement (courriel d'un président) ou un changement de coordonnées bancaires, **validez avec une autre personne.**

Toujours utiliser les **coordonnées officielles** (et non celles dans le message reçu) pour appeler ou écrire à notre contact chez le fournisseur.

Soyons vigilants

Si vous recevez un courriel ou un appel inhabituel, **posez des questions.** Ne vous fiez **PAS** à l'apparence du message (logo, signature, ton). Respectez nos procédures.

Réseaux sociaux

Faisons attention à ce que nous publions sur les réseaux sociaux de l'entreprise.

Ex. Publier que le président participera au congrès XYZ en Floride indique au fraudeur que c'est le bon temps pour faire une fraude si président.

Procédures

Assurons-nous de respecter les procédures en place ou de toujours vérifier auprès d'une deuxième source les demandes de virements et de changement de coordonnées bancaires.

Réflexions

- Connaissez-vous nos procédures?
- Sauriez-vous à qui vous adresser pour vérifier s'il s'agit bien d'une demande légitime?



Que faire si vous êtes victime?

Recommandation aux victimes d'une fraude par personnalisation

- Aviser la direction de notre entreprise immédiatement
- Contacter notre institution financière le plus rapidement possible pour tenter de récupérer les sommes détournées
- Déposer une plainte auprès de la police et rapporter la fraude au Centre antifraude du Canada



Page 7 [Lire le contenu de la diapo]

Malgré notre vigilance et bonne volonté, on peut quand même tomber dans le piège des fraudeurs. Savoir comment réagir et quels gestes poser sans attendre est crucial.

En conclusion



Faites des vérifications !

Ces fraudes reposent sur la manipulation et l'urgence. Les fraudeurs exploitent la confiance et la pression pour pousser à agir rapidement. Avant d'autoriser un paiement ou de partager des informations sensibles :

- **Prenez le temps de valider** la demande par un canal officiel
- **Ne vous fiez pas uniquement au courriel ou au ton urgent**
- Appliquez la règle du **double contrôle** : une vérification supplémentaire peut éviter des pertes majeures

La vigilance et la communication interne sont notre meilleure défense.

Références

- [Les principales tactiques de fraude en entreprise | Desjardins](#)
- [Qu'est-ce qu'une fraude par personnalisation? | Banque Nationale](#)

Page 8 [Lire le contenu de la diapo]

En conclusion

Pour en apprendre davantage, les références ci-dessus vous seront très utiles.

J'espère que l'atelier vous en a appris davantage sur les mots de passe et l'importance de bien se protéger, autant dans notre entreprise que dans notre vie privée.

Merci d'avoir participé à l'atelier!