Se voir dans le Cyberespace

Unvoyage autonome vers les cyber-risques

CYBEREADY

Commençons →

CYBERREADY

Avant de commencer :

L'objectif de cette expérience est de vous aider à **identifier** vos principaux cyber-risques, à les **comprendre** et à les **minimiser**

#1 Décrivez votre **journée de travail**

#2 Découvrez vos **risques**

#3 Découvrez des **histoires vécues**

#4 Apprenez **ce qu'il faut faire**

Je suis prêt →

Première étape :

Décrivez **votre journée de travail**

Suivant →

Choisissez un personnage auquel vous vous identifiez :

Je reçois des dizaines de **courriels** par jour

Je travaille surtout avec **des clients**

J'aime travailler dans des **lieux publics**

Je m'occupe des transactions **financières**

Chaque jour, recevez-vous des dizaines d'e-mails ?

Découvrez les **risques que vous courez**

Suivant →

Les risques

Votre utilisation intensive du courrier électronique vous rend particulièrement vulnérable à ces formes de fraude :

Hameçonnage

Affaires-E-mail-Compromis

Qu'est-ce que cela signifie ? →

Découvrez des histoires vécues

Des personnes sont victimes de ces escroqueries tous les jours.
Voici quelques-unes de leurs **histoires** pour vous aider à comprendre ces risques

Suivant →

«C'était un de ces jours où on n'a pas le temps de prendre un café. **J'ai reçu un email** de la part des « Ressources Humaines ». Il contenait un lien vers un formulaire me demandant des informations, notamment mon adresse électronique et mon mot de passe

Pendant le déjeuner, **j'ai découvert qu'aucun de mes collègues n'avait été invité à remplir un tel formulaire.** Ai-je été victime d'un hameçonnage ?"

Suivant →

«**J'ai reçu un courriel** d'un client me demandant de l'aider à accéder à ses données. Il a écrit qu'il était sur le point de signer un contrat et qu'il avait besoin des états financiers rapidement, **alors j'ai partagé l'information confidentielle avec lui**.

Plus tard, quand j'ai regardé l'email à nouveau, j'ai remarqué que **l'adresse e-mail était mal orthographiée. Même le nom avait une coquille**."

Suivant →

« J'ai **reçu un email** de « Danny Monel », mon patron. Dans celui-ci, il m'a demandé de **transférer des fonds à un fournisseur immédiatement,** car nous étions en violation d'un contrat.
Après avoir rapidement satisfait sa demande, je me suis sentie comme la meilleure employée.

Ce n'est que plus tard , lorsque j'ai regardé à nouveau l'e-mail, que j'ai réalisé qu'**il y avait quelque chose qui n'allait pas du tout**. »

Étape suivante →

Et maintenant, pour la dernière étape :

Apprenez ce qu'il faut faire 

4 conseils pour réduire vos risques

#1 **Examinez** l'adresse électronique de l'expéditeur et vérifiez qu'elle correspond à ce que vous attendez

#2 **Contactez la personne à l'origine de la demande** sur un autre fil ou canal (dès que vous avez des doutes)

#3 **Passez la souris sur les liens** pour vérifier que les URL pointent vers un site connu (sur les téléphones mobiles, le fait d'appuyer sur le lien et de le maintenir enfoncé permet de révéler l'adresse du site Web)

#4 **Méfiez-vous des courriels qui vous incitent à agir rapidement**. Cela devrait déclencher vous alerter.

Terminé →

Vous travaillez avec des clients ?

Découvrez les **risques que vous courez**

Suivant →

Les risques

Le fait de travailler avec de nombreuses personnes (comme les postes de service à la clientèle) vous rend particulièrement vulnérable à ces risques :

Fraude par usurpation d'identité

Partage d'informations confidentielles

Qu'est-ce que cela signifie ? →

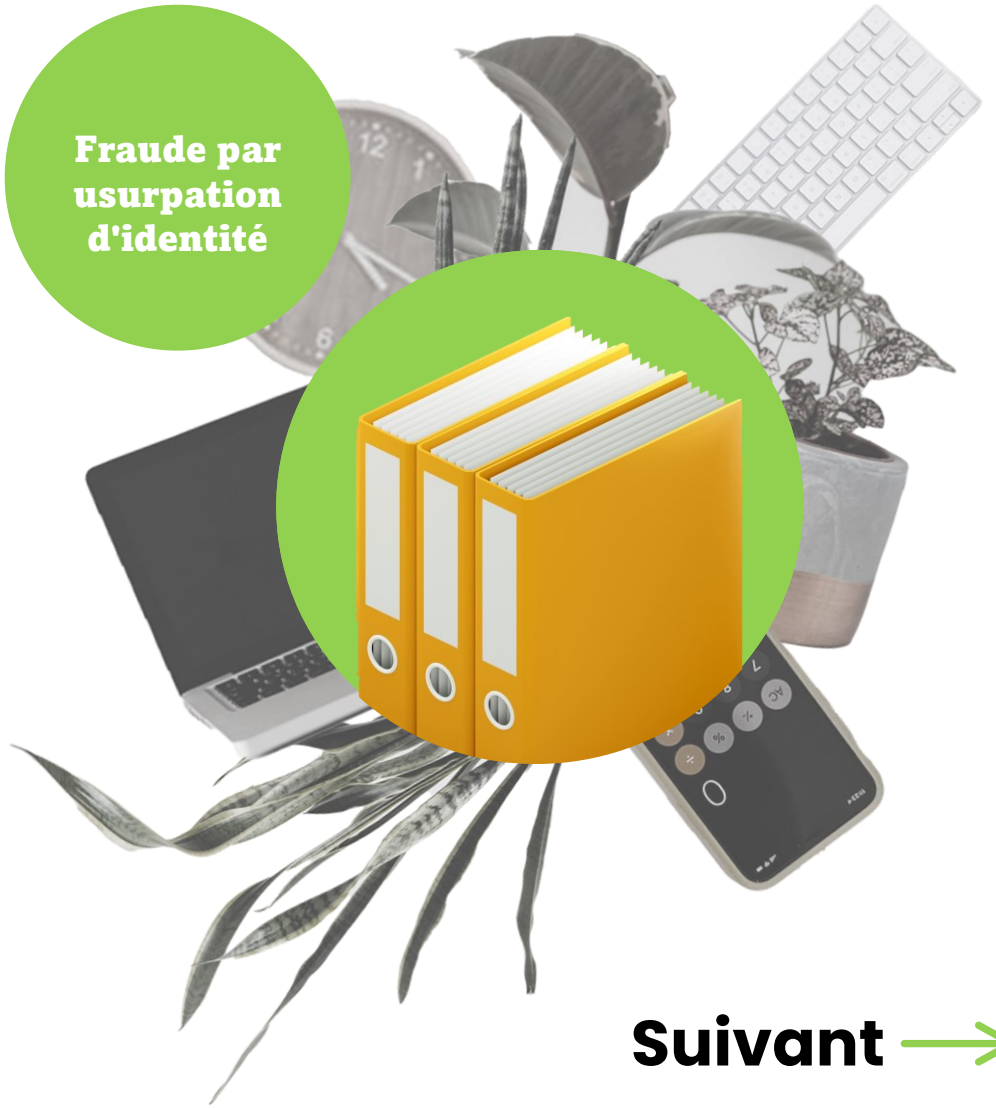
Découvrez des histoires vécues

Des personnes sont victimes de ces escroqueries tous les jours.
Voici quelques-unes de leurs **histoires** pour vous aider à comprendre ces risques

Suivant →

«**J'ai reçu un courriel** de "Ben", de la comptabilité client, demandant des documents pour le projet sur lequel je travaillais. **Alors je le lui ai envoyé par e-mail**.

Ce n'est que lorsque mon entreprise a été poursuivie que **J'ai découvert qu'il n'y avait pas de Ben sur la liste de paie du client**. »



Suivant →

« **Mon patron m'a demandé de partager la feuille de calcul des revenus annuels** avec Michael des finances, **ce que j'ai fait**. Une semaine plus tard, c'était dans les nouvelles.

Il s'avère que je l'ai accidentellement envoyé à un Michael d'une autre entreprise dans notre lieu de travail. »

Suivant →

«**Une femme m'a appelé** en pleurant, demandant le journal d'appels de son fils de treize ans, qui a disparu. **J'ai ressenti un besoin immédiat de l'aider** sans l'accabler de trop de questions.

Je n'ai découvert que **j'avais envoyé les détails à un détective privé** qui enquêtait sur un conjoint infidèle que lorsque nous ayons été poursuivis. »

Étape suivante →

Et maintenant, pour la dernière étape :

Apprenez ce qu'il faut faire 

4 conseils pour réduire vos risques

#1 **Vérifiez toujours** l'identité de la personne avec laquelle vous conversez

#2 Avant de partager des informations relatives aux clients, **vérifiez** que ces informations peuvent être explicitement partagées

#3 Partagez les informations sensibles **uniquement par le biais de canaux désignés**

#4 Soyez attentif au **ton du demandeur**. Si quelqu'un essaie de faire pression sur vous, c'est généralement un signe de fraude

Terminé →

Vous travaillez dans des lieux publics ?

Découvrez les **risques que vous courez**

Suivant →

Les risques

Le fait de travailler dans des lieux publics vous rend particulièrement vulnérable à ces risques :

Vol d'ordinateur portable

Piquage de mot de passe

Attaque Wi-Fi

Qu'est-ce que cela signifie ? →

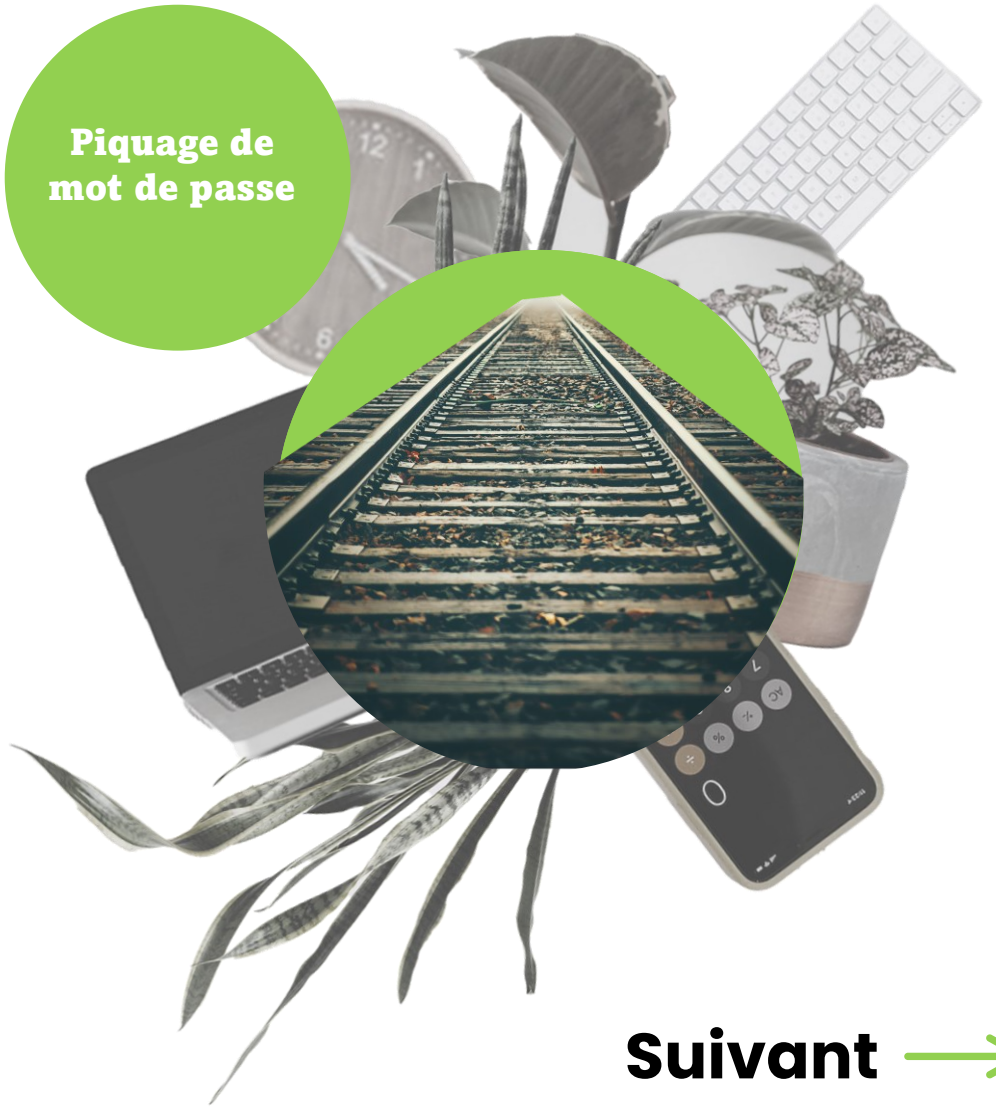
Découvrez des histoires vécues

Des personnes sont victimes de ces escroqueries tous les jours.
Voici quelques-unes de leurs **histoires** pour vous aider à comprendre ces risques

Suivant →

« C'était un jour de grande affluence dans le **train**. Puisque j'avais un rapport important à compléter, **j'ai travaillé sur mon ordinateur portable**. Le jour suivant, je suis tombé sur un post Reddit contenant **des informations internes sur notre entreprise qui étaient mentionnées dans mon document**.

Est-il possible que je sois la source de la **fuite** ? »



Suivant →

« Un jour, alors que je **travaillais dans un café** où je m'assieds souvent, **je me suis levé** pour choisir une pâtisserie **et j'ai laissé mon ordinateur portable sans surveillance pendant un moment**.

Quand je suis revenu, **il n'était plus là**. »

Suivant →

"En me rendant chez un client, j'ai dû vérifier certains détails. **Alors je me suis connecté au Wi-Fi gratuit du café voisin,** j'ai vérifié et je l'ai fermé.

Le mois suivant, **il y a eu un piratage de notre système** en utilisant mon utilisateur. Je n'arrive pas à me débarrasser de l'idée que cela pourrait avoir été causé par mon utilisation d'un Wi-Fi rogue. »

Étape suivante →

Et maintenant, pour la dernière étape :

Apprenez ce qu'il faut faire 

3 conseils pour réduire vos risques

#1 **Gardez** toujours **votre ordinateur portable à côté de vous**. Vous seriez étonné de savoir combien sont volés chaque année.

#2 **N'utilisez qu'une connexion internet privée**, jamais publique

#3 Assurez-vous que **vous êtes le seul à pouvoir voir l'écran** de votre ordinateur portable et vos notes

Terminé →

Traitement des transactions financières ?

Découvrez les **risques que vous courez**

Suivant →

Les risques

Le fait d'avoir l'autorisation de transférer des fonds vous rend vulnérable à ces formes de fraude :

Affaires-E-mail-Compromis

Fraude par usurpation d'identité du fournisseur

Qu'est-ce que cela signifie ? →

Découvrez des histoires vécues

Des personnes sont victimes de ces escroqueries tous les jours.
Voici quelques-unes de leurs **histoires** pour vous aider à comprendre ces risques

Suivant →

«**J'ai reçu un email** de mon patron me demandant de **transférer 17 000 dollars à un nouveau fournisseur**. Il a écrit : Je suis en réunion. Je ne peux pas parler. **Veuillez transférer l'argent dès que possible**et je l'ai fait.

Seulement un jour plus tard, dans le bureau, j'ai réalisé qu' **il n'avait aucune idée de ce dont je parlais**. »

Suivant →

«**J'ai reçu un mail** du **directeur financier nouvellement nommé** du fournisseur qui demandait que les **futurs paiements** soient envoyés sur un compte bancaire différent. **Alors je l'ai fait**.

C'était une **fraude**, mais comment aurais-je pu le savoir ? »

Suivant →

«**J'ai reçu un courriel** des RH avec un long fil de discussion. Ils m'ont demandé d' **acheter des cartes-cadeaux** pour la fête du nouvel an. Ils n'avaient besoin que de leurs numéros. Alors j' **ai acheté les cartes et leur ai envoyé les numéros**.

Il s'est avéré qu'il s'agissait d'une fraude, et que tout **l'argent avait disparu**. »

Étape suivante →

Et maintenant, pour la dernière étape :

Apprenez ce qu'il faut faire 

3 conseils pour réduire vos risques

#1 **Vérifiez** l'adresse électronique de l'expéditeur. Si elle est différente de la normale, fermez le courriel et contactez l'expéditeur présumé d'une autre manière

#2 **Vérifiez toute demande de changement** de mode de paiement auprès de votre interlocuteur habituel, en face à face ou par téléphone

#3 **Ralentissez**. Les pirates informatiques tentent d'inciter les gens à agir rapidement afin qu'ils ne remarquent pas les signes alarmants ou ne consultent pas les autres

Terminé →

Super ! Vous avez terminé le voyage

Que voulez-vous faire maintenant ?

Explorez un autre voyage

Fin

Nous vous remercions
d'avoir participé

Nous espérons que vous avez apprécié cette expérience et
que vous en avez tiré des enseignements précieux