

ATELIER  
Milieu professionnel

# Livret pédagogique pour les animateurs d'ateliers de sensibilisation

Comment sensibiliser ses utilisateurs  
à la cybersécurité dans un milieu professionnel ?

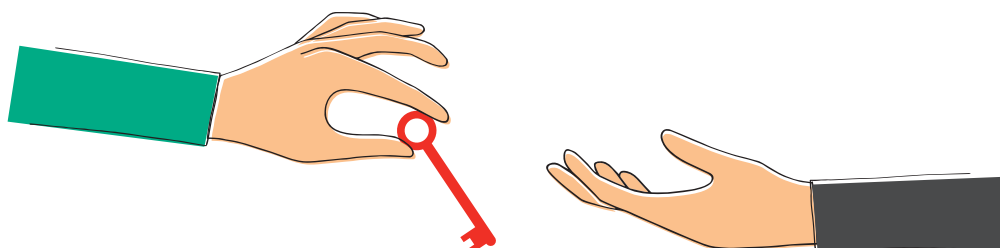


Diffusé  
par

**ORDRE DES  
EXPERTS-COMPTABLES** 

# Sommaire

<b>Édito .....</b>	<b>3</b>
<b>1. Introduction .....</b>	<b>4</b>
<i>pour s'approprier l'outil et son livret</i>	
<b>2. Contenus de sensibilisation .....</b>	<b>7</b>
<i>pour sensibiliser animateurs et utilisateurs</i>	
• Les menaces les plus courantes .....	8
• Les bonnes pratiques de sécurité à retenir.....	13
<b>3. Contenus méthodologiques.....</b>	<b>19</b>
<i>pour mieux piloter sa cybersécurité</i>	
<i>(cadres / dirigeants)</i>	
<b>4. Présentation du jeu de cartes.....</b>	<b>26</b>
<i>pour mettre en pratique les notions apprises</i>	
<b>Espace de prise de notes .....</b>	<b>38</b>



Issu de la Stratégie numérique du Gouvernement, notre groupement d'intérêt public « Action contre la Cybermalveillance\* » a été créé en 2017 pour mieux protéger les particuliers, les entreprises et les collectivités.

8 ans plus tard, avec plus de 20 millions de visiteurs ayant eu recours à ses services, la plateforme Cybermalveillance.gouv.fr est le plus important producteur de contenus de prévention, fort de plus de six cents réalisations mises à disposition gratuitement, ainsi qu'une référence en matière d'outils de sensibilisation et d'assistance aux victimes au profit des particuliers comme des professionnels. Le lancement fin 2024 du guichet unique « 17cyber.gouv.fr » en est la preuve.

En 2023, en partenariat avec l'ANCT (Agence Nationale de la Cohésion des Territoires – membre de Cybermalveillance.gouv.fr), nous avons conçu une mallette pédagogique pour outiller les professionnels de la médiation numérique : la « MalletteCyber » destinée à mieux accompagner nos nombreux concitoyens éloignés du numérique\*\*. Devant le succès rencontré, nous avons décidé de l'adapter au contexte comme aux enjeux des petites et moyennes entreprises.

Présent aux côtés des professionnels depuis son lancement, Cybermalveillance.gouv.fr entend répondre à un besoin émis par les entreprises en matière de sensibilisation au risque numérique : selon notre étude nationale menée en 2025\*\*\*, 40 % des entreprises estiment avoir un besoin prioritaire de sensibiliser leurs dirigeants ou leurs collaborateurs.

Car comme nous l'observons au fil des années, les entreprises sont des cibles de prédilection d'attaquants professionnalisés et ne cessent de venir grossir les rangs des victimes cherchant de l'assistance sur la plateforme Cybermalveillance.gouv.fr : près de 28 000 pour la seule année 2025. Cela souligne la nécessité de la prévention pour ces publics !

C'est en proposant une pédagogie reposant sur l'adhésion de l'utilisateur et des notions non techniques accessibles à tous que nous avons adapté ces contenus au contexte professionnel. Cette version destinée aux TPE-PME / associations se veut facilement et largement diffusable : ses plans sont gratuits et en licence ouverte.

En tant que porteurs de cet outil, vous jouez dans ce projet de sensibilisation de nos entreprises, premiers employeurs de France et garants de sa vitalité économique, un rôle clé et contribuez ainsi à une démarche d'intérêt général. Nous vous encourageons à vous approprier ce contenu de façon à ce qu'il puisse répondre au mieux à vos exigences et espérons qu'il vous sera utile au quotidien.

Je remercie chacun d'entre vous pour son action. Bonne lecture et bons ateliers !



**Jérôme NOTIN**  
Directeur général de  
Cybermalveillance.gouv.fr

\* GIP ACYMA : Groupement d'Intérêt Public Actions contre la cybermalveillance

\*\* La société numérique française : définir et mesurer l'éloignement numérique - ANCT 2023. Selon ce document, 16 millions de personnes restent encore « éloignées du numérique »

\*\*\* 2<sup>e</sup> édition du baromètre national de la maturité cyber des TPE-PME (enquête OpinionWay pour Cybermalveillance.gouv.fr parue en octobre 2025).

# Introduction

Dans le cadre de la prévention des risques en milieu professionnel, ce livret pédagogique s'adresse aux animateurs d'ateliers afin de les accompagner dans la sensibilisation des utilisateurs en matière de cybersécurité.

## CONTEXTE D'UTILISATION DE LA MALLETTECYBER PRO

La MalletteCyber PRO a été conçue dans le cadre d'une démarche de prévention à la cybersécurité auprès d'utilisateurs adultes. Elle peut être utilisée lors d'entretiens individuels ou en ateliers de six utilisateurs maximum (nombre recommandé afin de privilégier les échanges).



La MalletteCyber PRO n'a pas pour vocation d'assister les victimes de cybermalveillances. N'hésitez pas à les rediriger vers la plateforme nationale « 17cyber.gouv.fr » pour obtenir tous les conseils d'urgence adaptés à leur situation.

En tant qu'animateur, nous vous invitons à vous approprier l'ensemble des contenus de la MalletteCyber PRO avant de débiter votre atelier.



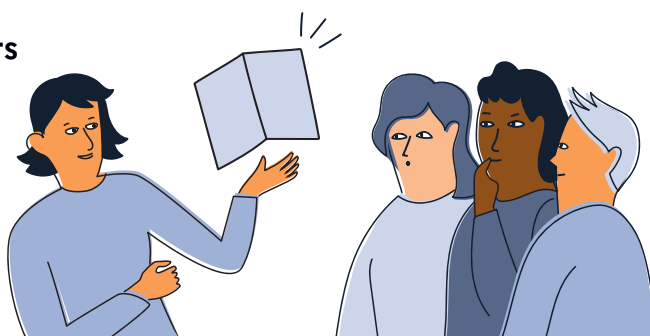
**En tête à tête  
ou en groupe  
2 à 6 utilisateurs**



**18+ ans**



**Prévention  
uniquement**

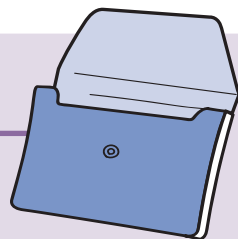


Si vous souhaitez axer votre atelier sur des cybermalveillances plus en lien avec la **sphère privée**, vous pouvez vous procurer gratuitement la « MalletteCyber » conçue au profit des aidants numériques pour tous publics :

<https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/outils-acteurs-mediation>



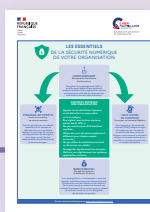
## COMPOSANTS DE LA MALLETTE CYBER PRO



**UN LIVRET PÉDAGOGIQUE** composé de :

→ **contenus de sensibilisation et de méthodologie** (dirigeants) avec des fiches réflexes et des fiches pratiques

→ une **présentation du jeu de cartes** pour vous permettre de l'animer



**UNE AFFICHE ILLUSTRÉE** avec :

→ « les essentiels de la sécurité numérique de votre organisation » présentant **les menaces et les risques les plus courants** ainsi que les bonnes pratiques élémentaires



**UN JEU DE CARTES ET UN PLATEAU DE JEU**

→ pour mettre en pratique et **ancrer les notions** abordées avec les utilisateurs



**UNE INFOGRAPHIE**

→ à imprimer et à **remettre à chaque utilisateur** pour lui laisser un résumé des bonnes pratiques essentielles au sein d'une organisation

## RESSOURCES COMPLÉMENTAIRES



**FLYER  
17CYBER**



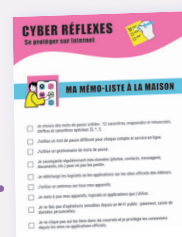
**L'ASSURANCE  
CYBER POUR  
LES TPE-PME**



**DÉPLIANT  
« SERVICES EN LIGNE  
POUR LES PROS »**



**FICHE LABEL  
EXPERTCYBER  
BÉNÉFICIAIRES**



**MÉMO-LISTE  
« CYBER RÉFLEXES »  
À LA MAISON  
ET AU TRAVAIL**

# Utilisation

Pour un meilleur apprentissage, nous vous recommandons de procéder dans cet ordre :

## 1. Apprendre ou approfondir ses connaissances

Pour s'acculturer à la cybersécurité avec des fiches réflexes et des fiches pratiques.



## 2. Transmettre

Une fois que vous êtes à l'aise avec le sujet, vous pouvez utiliser l'affiche pour décrire les attaques les plus courantes et les risques qu'elles impliquent pour l'organisation.



## 3. Pratiquer et illustrer

Pour maîtriser les notions cyber, utilisez les cartes et jouez avec les utilisateurs.



## 4. Pérenniser

À la fin de l'atelier remettez à l'utilisateur, l'infographie qui résume les principales recommandations à retenir dans un contexte professionnel.

# Contenus de sensibilisation à l'usage de l'animateur

## Les menaces les plus courantes

L'hameçonnage.....	08
Le piratage de compte .....	09
Fraude au virement (faux RIB) .....	10
Les virus et programmes malveillants .....	11
Les rançongiciels.....	12

## Les mémos « bonnes pratiques de sécurité »

Gérer vos mots de passe .....	13
Gérer vos mises à jour .....	14
Faire vos sauvegardes.....	15
Sécuriser vos usages pro perso .....	16
Sécuriser le télétravail .....	17
Que faire en cas de cyberattaque (collaborateurs)?.....	18





## L'HAMEÇONNAGE



L'hameçonnage (**phishing** en anglais) est une technique frauduleuse destinée à leurrer l'internaute pour l'inciter à communiquer des données personnelles (comptes d'accès, mots de passe...) et/ou bancaires en se faisant passer pour un tiers de confiance. Il peut s'agir d'un faux message, SMS ou appel téléphonique de banque, de réseau social, d'opérateur de téléphonie, de fournisseur d'énergie, de site de commerce en ligne, d'administrations, etc.

### BUT RECHERCHÉ

**Voler des informations personnelles ou professionnelles** (comptes, mots de passe, données bancaires...) pour en faire un usage frauduleux.

## SI VOUS ÊTES VICTIME

En cas de doute, **CONTACTEZ DIRECTEMENT L'ORGANISME CONCERNÉ** pour confirmer le message ou l'appel que vous avez reçu.

Si vous avez communiqué des éléments sur vos moyens de paiement ou si vous avez constaté des débits frauduleux sur votre compte bancaire, **FAITES OPPOSITION IMMÉDIATEMENT** auprès de votre organisme bancaire ou financier.

Si vous avez communiqué un mot de passe, **CHANGEZ-LE IMMÉDIATEMENT** ainsi que sur tous les autres sites ou services sur lesquels vous l'utilisez ([tous nos conseils pour gérer au mieux vos mots de passe](#)).

**CONSERVEZ LES PREUVES** et, en particulier, le message d'hameçonnage reçu.

Si vous avez reçu un message douteux sans y répondre, **SIGNELEZ-LE À SIGNAL SPAM** ([SIGNAL-SPAM.FR](#)).

Vous pouvez également **SIGNALER UNE ADRESSE DE SITE D'HAMEÇONNAGE À PHISHING INITIATIVE** ([PHISHING-INITIATIVE.FR](#)) qui en fera fermer l'accès.

En fonction du préjudice subi (débits frauduleux, usurpation d'identité...) **DÉPOSEZ PLAINTÉ** [au commissariat de police](#) ou [à la gendarmerie](#) ou écrivez [au procureur de la République](#) dont vous dépendez en fournissant toutes les preuves en votre possession.

Pour être conseillé en cas d'hameçonnage, contactez **INFO ESCROQUERIES AU 0 805 805 817** (numéro gratuit).

### MESURES PRÉVENTIVES

**Ne communiquez jamais d'informations sensibles par messagerie ou téléphone** : aucune administration ou société commerciale sérieuse ne vous demandera vos données bancaires ou vos mots de passe par message électronique ou par téléphone.

**Avant de cliquer sur un lien douteux, positionnez le curseur de votre souris sur ce lien** (sans cliquer) ce qui affichera alors l'adresse vers laquelle il pointe réellement afin d'en vérifier la vraisemblance ou allez directement sur le site de l'organisme en question par un lien favori que vous aurez vous-même créé.

**Vérifiez l'adresse du site qui s'affiche dans votre navigateur**. Si cela ne correspond pas exactement au site concerné, c'est très certainement un site frauduleux. Parfois, un seul caractère peut changer dans l'adresse du site pour vous tromper. Au moindre doute, ne fournissez aucune information et fermez immédiatement la page correspondante.

**En cas de doute, contactez si possible directement l'organisme concerné** pour confirmer le message ou l'appel que vous avez reçu.

**Utilisez des mots de passes différents et complexes pour chaque site et application** afin d'éviter que le vol d'un de vos mots de passe ne compromette tous vos comptes personnels. Vous pouvez également utiliser des coffres-forts numériques de type KeePass pour stocker de manière sécurisée vos différents mots de passe.

Si le site le permet, **vérifiez les date et heure de dernière connexion à votre compte** afin de repérer si des accès illégitimes ont été réalisés.

Si le site vous le permet, **activez la double authentification** pour sécuriser vos accès.



EN PARTENARIAT AVEC :

MINISTÈRE DE L'INTÉRIEUR  
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION



# LE PIRATAGE DE COMPTE



Le piratage de compte désigne la prise de contrôle par un individu malveillant d'un compte au détriment de son propriétaire légitime. Il peut s'agir de comptes ou d'applications de messagerie, d'un réseau social, de sites administratifs, de plateformes de commerce en ligne. En pratique, les attaquants ont pu avoir accès à votre compte de plusieurs manières: le mot de passe était peut-être trop simple, vous avez précédemment été victime d'hameçonnage (**phishing** en anglais) où vous avez communiqué votre mot de passe sans le savoir, ou bien vous avez utilisé le même sur plusieurs sites dont l'un a été piraté.

## BUT RECHERCHÉ

Dérober des informations personnelles, professionnelles et/ou bancaires pour en faire un usage frauduleux (revente des données, usurpation d'identité, transactions frauduleuses, spam, etc.).

## SI VOUS ÊTES VICTIME

Si vous ne pouvez plus vous connecter à votre compte, **CONTACTEZ LE SERVICE CONCERNÉ POUR SIGNALER VOTRE PIRATAGE ET DEMANDEZ LA RÉINITIALISATION DE VOTRE MOT DE PASSE.**

Dans vos paramètres de récupération de compte, **ASSUREZ-VOUS QUE VOTRE NUMÉRO DE TÉLÉPHONE ET VOTRE ADRESSE MAIL DE RÉCUPÉRATION SOIENT LES BONS.** Si ce n'est pas le cas, changez-les immédiatement.

**CHANGEZ AU PLUS VITE VOTRE MOT DE PASSE** et choisissez-en un solide ([voir notre fiche sur la gestion des mots de passe](#)). Et si possible, **ACTIVEZ LA DOUBLE AUTHENTIFICATION.**

**CHANGEZ SANS TARDER LE MOT DE PASSE PIRATÉ SUR TOUS LES AUTRES SITES OU COMPTES SUR LESQUELS VOUS POUVIEZ L'UTILISER.**

**PRÉVENEZ TOUS VOS CONTACTS DE CE PIRATAGE** pour qu'ils ne soient pas victimes à leur tour des cybercriminels qui les contacteraient en usurpant votre identité.

**VÉRIFIEZ QU'AUCUNE PUBLICATION OU COMMANDE N'A ÉTÉ RÉALISÉE** avec le compte piraté.

Si vos coordonnées bancaires étaient disponibles sur le compte piraté, surveillez vos comptes, **PRÉVENEZ IMMÉDIATEMENT VOTRE BANQUE** et faites au besoin opposition aux moyens de paiement concernés.

En fonction du préjudice subi, **DÉPOSEZ PLAINTÉ** au [commissariat de police](#) ou à la [gendarmerie](#) ou écrivez au [procureur de la République](#) dont vous dépendez en fournissant toutes les preuves en votre possession.

## MESURES PRÉVENTIVES

Utilisez des **mots de passes différents et complexes pour chaque site et application** utilisés pour éviter que, si un compte est piraté, les cybercriminels puissent accéder aux autres comptes utilisant ce même mot de passe.



Lorsque le site ou le service le permettent, **activez la double authentification** pour augmenter le niveau de sécurité.



**Ne communiquez jamais d'informations sensibles** (mots de passe) par messagerie, par téléphone ou sur Internet.



**Appliquez de manière régulière et systématique les mises à jour de sécurité** du système et des logiciels installés sur votre machine.



**Maintenez à jour votre antivirus et activez votre pare-feu.** Vérifiez qu'il ne laisse passer que des applications et services légitimes.



**N'ouvrez pas les courriels ou leurs pièces jointes et ne cliquez jamais sur les liens** provenant de chaînes de messages, d'expéditeurs inconnus, ou d'un expéditeur connu, mais dont le contenu du message est inhabituel ou vide.



**Évitez les sites non sûrs ou illicites**, tels ceux hébergeant des contrefaçons dont ces dernières peuvent contenir des logiciels malveillants (musique, films, logiciels, etc.) ou certains sites pornographiques.



**Vérifiez l'adresse du site qui s'affiche dans votre navigateur.** Si cela ne correspond pas exactement au site concerné, il s'agit certainement d'un site frauduleux. Il suffit parfois d'un seul caractère changeant pour vous tromper.



Si le site le permet, **vérifiez les date et heure de la dernière connexion à votre compte** afin de repérer d'éventuelles connexions anormales.



**Évitez de vous connecter à un ordinateur ou à un réseau Wi-Fi publics.** Non maîtrisés, ils peuvent être contrôlés par un pirate.



**Déconnectez-vous systématiquement de votre compte après utilisation** pour éviter que quelqu'un puisse y accéder après vous.



EN PARTENARIAT AVEC:

MINISTÈRE DE L'INTÉRIEUR

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION



## FRAUDE AU VIREMENT (FAUX RIB)



La fraude au virement ou au faux RIB vise à tromper la victime, en usurpant l'identité d'un créancier avec lequel elle est en relation (artisan, notaire, propriétaire...), afin de lui faire réaliser un virement vers un compte bancaire détenu par un escroc.

Ce type d'escroquerie est souvent consécutif au piratage du compte de messagerie (mail) du créancier ou de la victime.

En pratique, l'escroc va identifier une transaction imminente ou récurrente entre le créancier et la victime. En usurpant l'identité du créancier, il va alors adresser un message à la victime lui demandant de réaliser le paiement par virement. En général, l'escroc aura joint à son message une facture avec un RIB falsifié contenant les coordonnées d'un compte bancaire qu'il détient pour dérober le montant du virement.

### BUT RECHERCHÉ

Détourner un virement de la victime en usurpant l'identité de son créancier.

## SI VOUS ÊTES VICTIME

**ALERTEZ IMMÉDIATEMENT VOTRE BANQUE** pour tenter de suspendre le virement ou demander le retour des fonds.

**ALERTEZ LE CRÉANCIER DONT L'IDENTITÉ A ÉTÉ USURPÉE** car il est possible que l'un de ses comptes de messagerie ait été piraté.

**CONSERVEZ LES PREUVES** (messages reçus, relevés de comptes, factures...) qui pourront vous servir pour signaler les faits.

**VÉRIFIEZ LES PARAMÈTRES DE VOTRE MESSAGERIE** pour vous assurer de l'absence de règles de redirection ou de filtrage, ou encore de connexions inconnues. Si vous en identifiez, faites des photos ou des captures d'écran avant de les supprimer.

**CHANGEZ IMMÉDIATEMENT VOTRE MOT DE PASSE** si l'escroquerie a pu être réalisée suite au piratage de votre messagerie.

**DÉPOSEZ PLAINTÉ** au commissariat de police ou à la brigade de gendarmerie ou encore par écrit au procureur de la République du tribunal judiciaire dont vous dépendez.

Pour plus de conseils, **CONTACTEZ INFO ESCROQUERIES** au 0 805 805 817 (appel et service gratuits).

### MESURES PRÉVENTIVES

Pour toute demande de virement sur un nouveau RIB reçu par message, **contactez directement votre créancier sur son numéro habituel pour lui faire confirmer le message et les coordonnées du RIB reçus.**

**Méfiez-vous des messages d'hameçonnage** qui vous incitent à communiquer votre **mot de passe de messagerie**. Vérifiez qu'ils ne vous amènent pas sur un site frauduleux pour vous le dérober.

**Utilisez des mots de passe différents et complexes pour chaque site et application que vous utilisez.** Activez la **double authentification** quand elle est disponible.

**Appliquez de manière régulière et systématique les mises à jour de sécurité** du système, des applications et des logiciels installés sur vos appareils.

**N'installez des applications ou logiciels que depuis les sites ou magasins officiels** au risque de télécharger une version infectée par un **virus**.

**Utilisez un antivirus** pour vous protéger des virus qui pourraient dérober vos mots de passe.



EN PARTENARIAT AVEC :

MINISTÈRE DE L'INTÉRIEUR

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION





# LES VIRUS INFORMATIQUES



Un virus est un programme informatique malveillant dont l'objectif est de perturber le fonctionnement normal d'un système informatique à l'insu de son propriétaire. Il existe différents types de virus comme le rançongiciel, le cheval de Troie, le logiciel espion... Les virus peuvent s'infiltrer dans un système informatique par l'ouverture d'un message (mail, MMS, chat), d'une pièce jointe ou d'un clic sur un lien frauduleux, par exemple. Il peut aussi s'introduire en naviguant sur un site malveillant, en s'installant dans un appareil ou un logiciel non mis à jour, par l'absence d'utilisation d'un antivirus, l'installation d'une application piratée, etc. Les symptômes d'une infection par un virus peuvent se manifester par une alerte de l'antivirus, un ralentissement ou un blocage anormal de l'appareil, des fenêtres ou des messages d'erreur qui s'affichent sans raison, la modification de logiciels ou programmes, etc.

## BUT RECHERCHÉ

Prendre le contrôle d'un système informatique pour en faire un usage frauduleux, espionner l'utilisateur, dérober des données personnelles et/ou confidentielles, attaquer d'autres appareils, chiffrer les fichiers et demander une rançon, etc.

## SI VOUS ÊTES VICTIME

**DÉCONNECTEZ L'ÉQUIPEMENT INFECTÉ D'INTERNET OU DU RÉSEAU** pour éviter que le virus ne se propage à d'autres appareils.

**IDENTIFIEZ LA SOURCE DE L'INFECTION ET SON ÉTENDUE** (faible de sécurité, message malveillant) et prenez les mesures nécessaires pour qu'elle ne puisse pas se reproduire.

**RÉCUPÉREZ OU TENTEZ DE FAIRE RÉCUPÉRER PAR UN PROFESSIONNEL LES PREUVES DISPONIBLES.** Séquestrez la ou les machines touchées ou réalisez-en une copie physique complète.

Avant de remettre en état votre système, et en fonction du préjudice subi, **DÉPOSEZ PLAINTÉ** au commissariat de police ou à la brigade de gendarmerie ou en adressant votre plainte au procureur de la République du tribunal judiciaire dont vous dépendez.

Après avoir vérifié que votre antivirus est en état de fonctionnement et à jour, **FAITES UNE ANALYSE ANTIVIRALE COMPLÈTE (SCAN) DE VOS APPAREILS** et supprimez les virus.

**CHANGEZ AU PLUS VITE VOS MOTS DE PASSE** au moindre doute sur leur piratage.

**RESTAUREZ VOTRE SYSTÈME** si les symptômes de l'infection continuent de se manifester.

**RÉINITIALISEZ OU RÉINSTALLEZ COMPLÈTEMENT VOTRE APPAREIL EN DERNIER RECOURS** si le virus persiste toujours.

## MESURES PRÉVENTIVES

**Utilisez un antivirus et mettez-le à jour régulièrement.**



**Mettez régulièrement à jour votre appareil**, votre système d'exploitation ainsi que les logiciels et applications installés.



**N'installez pas de logiciels, programmes, applications ou équipements « piratés »** ou dont l'origine ou la réputation sont douteuses.



**N'ouvrez pas les messages suspects, leurs pièces jointes et ne cliquez pas sur les liens** provenant de chaînes de messages, d'expéditeurs inconnus ou d'un expéditeur connu mais dont le contenu est inhabituel ou vide.



**Évitez les sites non sûrs ou illicites** tels ceux hébergeant des contrefaçons (musique, films, logiciels, etc.) ou certains sites pornographiques qui peuvent injecter du code en cours de navigation et infecter votre machine.



**N'utilisez pas un compte avec des droits « administrateur »** pour consulter vos messages ou naviguer sur Internet.



**Faites des sauvegardes régulières** de vos données et de votre système pour pouvoir le réinstaller dans son état d'origine au besoin.



**Utilisez des mots de passe suffisamment complexes et changez-les au moindre doute** (tous nos conseils pour gérer vos mots de passe).



**N'utilisez pas de supports amovibles dont vous ne connaissez pas la provenance** (clé USB trouvée, etc.).



EN PARTENARIAT AVEC :

MINISTÈRE DE L'INTÉRIEUR

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

# LES RANÇONGIERS



Un rançongiciel (*ransomware* en anglais) est un logiciel malveillant qui bloque l'accès à l'ordinateur ou à des fichiers en les chiffrant et qui réclame à la victime le paiement d'une rançon pour en obtenir de nouveau l'accès. La machine peut être infectée après l'ouverture d'une pièce jointe, ou après avoir cliqué sur un lien malveillant reçu dans des courriels, ou parfois simplement en naviguant sur des sites compromis, ou encore suite à une intrusion dans le système. Dans la majorité des cas, les cybercriminels exploitent des vulnérabilités connues dans les logiciels, mais dont les correctifs n'ont pas été mis à jour par les victimes.

## BUT RECHERCHÉ

Extorquer de l'argent à la victime en échange de la promesse (pas toujours tenue) de retrouver l'accès aux données corrompues. Certaines attaques visent juste à endommager le système de la victime.

## SI VOUS ÊTES VICTIME

**DÉBRANCHEZ LA MACHINE D'INTERNET** ou du réseau informatique.

**NE PAYEZ PAS LA RANÇON** réclamée car vous n'êtes pas certain de récupérer vos données et vous alimenteriez le système mafieux.

**CONSERVEZ LES PREUVES** : message piégé, fichiers de journalisation (logs) de votre pare-feu, copies physiques des postes ou serveurs touchés. À défaut, conservez les disques durs.

**DÉPOSEZ PLAINTÉ** [au commissariat de police](#) ou [à la gendarmerie](#) ou en écrivant [au procureur de la République](#) dont vous dépendez en fournissant toutes les preuves en votre possession.

**IDENTIFIEZ LA SOURCE DE L'INFECTION** et prenez les mesures nécessaires pour qu'elle ne puisse pas se reproduire.

**APPLIQUEZ UNE MÉTHODE DE DÉSINFECTION ET DE DÉCHIFFREMENT**, lorsqu'elle existe\*. En cas de doute, effectuez une restauration complète de votre ordinateur. Reformatez les postes et/ou serveurs touchés et réinstallez un système sain puis restaurez les copies de [sauvegarde](#) des fichiers perdus lorsqu'elles sont disponibles.

**FAITES-VOUS ASSISTER AU BESOIN PAR DES PROFESSIONNELS QUALIFIÉS**. Vous trouverez sur [www.cybermalveillance.gouv.fr](http://www.cybermalveillance.gouv.fr) des professionnels en sécurité informatique susceptibles de pouvoir vous apporter leur assistance.

\* Le site suivant peut fournir des solutions dans certains cas : <https://www.nomoreransom.org/fr/index.4html>

## MESURES PRÉVENTIVES

Appliquez de manière régulière et systématique les **misés à jour de sécurité** du système et des logiciels installés sur votre machine.



Tenez à jour l'antivirus et configurez votre **pare-feu**. Vérifiez qu'il ne laisse passer que des applications, services et machines légitimes.



N'ouvrez pas les courriels, leurs pièces jointes et ne cliquez pas sur les liens provenant de chaînes de messages, d'expéditeurs inconnus ou d'un expéditeur connu, mais dont la structure du message est inhabituelle ou vide.



N'installez pas d'application ou de programme « piratés » ou dont l'origine ou la réputation sont douteuses.



Évitez les sites non sûrs ou illicites tels ceux hébergeant des contrefaçons (musique, films, logiciels...) ou certains sites pornographiques qui peuvent injecter du code en cours de navigation et infecter votre machine.



Faites des **sauvegardes régulières** de vos données et de votre système pour pouvoir le réinstaller dans son état d'origine au besoin.



N'utilisez pas un compte avec des droits « administrateur » pour consulter vos messages ou naviguer sur Internet.



Utilisez des mots de passe suffisamment complexes et changez-les régulièrement, mais vérifiez également que ceux créés par défaut soient effacés s'ils ne sont pas tout de suite changés ([tous nos conseils pour gérer vos mots de passe](#)).



Éteignez votre machine lorsque vous ne vous en servez pas.



EN PARTENARIAT AVEC :

MINISTÈRE DE L'INTÉRIEUR

AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION





RÉPUBLIQUE  
FRANÇAISE

Liberté  
Égalité  
Fraternité



Assistance et prévention  
en cybersécurité

mémo



## 10 CONSEILS POUR GÉRER VOS MOTS DE PASSE

1

Utilisez un mot  
de passe différent  
pour chaque service



6

Ne communiquez jamais  
votre mot de passe à un  
tiers



2

Utilisez un mot de passe  
suffisamment long et  
complexe



7

N'utilisez pas vos mots de  
passe sur un ordinateur  
partagé



3

Utilisez un mot  
de passe impossible  
à deviner



8

Activez la double  
authentification  
lorsque c'est possible



4

Utilisez un gestionnaire  
de mots de passe



9

Changez les mots  
de passe par défaut  
des différents services  
auxquels vous accédez



5

Changez votre mot  
de passe au moindre  
soupçon



10

Choisissez un mot de  
passe particulièrement  
robuste pour votre  
messagerie



Pour en savoir plus, lisez notre article complet sur  
[Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr) en flashant ce QR-code



ADOPTER LES BONNES PRATIQUES

mémo



## 10 CONSEILS POUR GÉRER VOS MISES À JOUR

1

Pensez à mettre à jour  
sans tarder l'ensemble de  
vos appareils et logiciels



6

Planifiez les mises à  
jour lors de périodes  
d'inactivité



2

Téléchargez les mises  
à jour uniquement  
depuis les sites officiels



7

Méfiez-vous des fausses  
mises à jour sur Internet



3

Identifiez l'ensemble  
des appareils et logiciels  
utilisés



8

Informez-vous sur la  
publication régulière des  
mises à jour de l'éditeur



4

Activez l'option de  
téléchargement  
et d'installation  
automatique des mises à jour



9

Testez les mises à jour  
lorsque cela est possible  
et faites des sauvegardes



5

Définissez les règles  
de réalisation des mises  
à jour



10

Protégez autrement les  
appareils qui ne peuvent  
pas être mis à jour



Pour en savoir plus, lisez notre article complet sur  
[Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr) en flashant ce QR-code



ADOPTER LES BONNES PRATIQUES



RÉPUBLIQUE  
FRANÇAISE

Liberté  
Égalité  
Fraternité



Assistance et prévention  
en cybersécurité

mémo

ADOPTER LES BONNES PRATIQUES



## 10 CONSEILS POUR FAIRE VOS SAUVEGARDES

1

Effectuez des sauvegardes régulières de vos données



6

Déconnectez votre support de sauvegarde après utilisation



2

Identifiez les appareils et supports qui contiennent des données



7

Protégez vos sauvegardes (perte, vol, casse...)



3

Déterminez quelles données doivent être sauvegardées



8

Testez vos sauvegardes



4

Choisissez une solution de sauvegarde adaptée à vos besoins



9

Vérifiez le support de sauvegarde



5

Planifiez vos sauvegardes



10  
Pro

Sauvegardez les logiciels indispensables à l'exploitation de vos données



Pour en savoir plus, lisez notre article complet sur  
[Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr) en flashant ce QR-code





RÉPUBLIQUE  
FRANÇAISE

Liberté  
Égalité  
Fraternité



Assistance et prévention  
en cybersécurité



## 10 CONSEILS POUR SÉCURISER VOS USAGES PRO ET PERSO

mémo

1

Utilisez des mots de passe différents pour tous les services professionnels et personnels auxquels vous accédez



6

Faites les mises à jour de sécurité de vos équipements



2

Ne mélangez pas votre messagerie professionnelle et personnelle



7

Utilisez une solution de sécurité contre les virus et autres attaques



3

Ayez une utilisation raisonnable d'Internet au travail



8

N'installez des applications que depuis les sites ou magasins officiels



4

Maîtrisez vos propos sur les réseaux sociaux



9

Méfiez-vous des supports USB



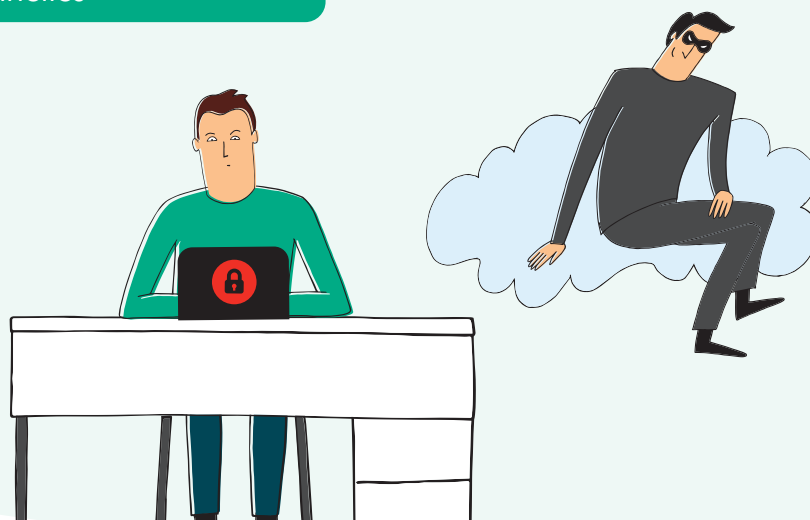
5

N'utilisez pas de service de stockage en ligne personnel à des fins professionnelles



10

Évitez les réseaux Wi-Fi publics ou inconnus



Pour en savoir plus, lisez notre article complet sur [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr) en flashant ce QR-code



ADOPTER LES BONNES PRATIQUES



RÉPUBLIQUE  
FRANÇAISE

Liberté  
Égalité  
Fraternité



Assistance et prévention  
en cybersécurité

mémo



## 10 CONSEILS POUR SÉCURISER LE TÉLÉTRAVAIL

1

Équipez les  
télétravailleurs de  
matériels maîtrisés



6

Durcissez la sauvegarde  
de vos données



2

Filtrez et limitez vos accès  
extérieurs



7

Utilisez des solutions  
antivirales professionnelles



3

Sécurisez vos accès  
extérieurs (VPN)



8

Journalisez l'activité de  
tous vos équipements  
d'infrastructure



4

Renforcez la gestion des  
mots de passe (2FA)



9

Supervisez l'activité de  
vos accès externes et  
systèmes sensibles



5

Déployez sans tarder les  
mises à jour de sécurité



10

Sensibilisez et apportez  
un soutien réactif à vos  
télétravailleurs



Pour en savoir plus, lisez notre article complet sur  
[Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr) en flashant ce QR-code



ADOPTER LES BONNES PRATIQUES

## CONSIGNES EN CAS DE CYBERATTAQUE



**DÉBRANCHEZ LA MACHINE D'INTERNET  
OU DU RÉSEAU INFORMATIQUE**

*Débranchez le câble réseau et désactivez la connexion Wi-Fi  
ou les connexions de données pour les appareils mobiles.*



**N'ÉTEIGNEZ PAS L'APPAREIL**

*Certains éléments de preuve contenus dans la mémoire de l'équipement  
et nécessaires aux investigations seront effacés s'il est éteint.*



**ALERTEZ AU PLUS VITE  
VOTRE SUPPORT INFORMATIQUE**

*Votre support pourra prendre les mesures nécessaires pour contenir,  
voire réduire, les conséquences de la cyberattaque.*



**N'UTILISEZ PLUS L'ÉQUIPEMENT  
POTENTIELLEMENT COMPROMIS**

*Ne touchez plus à l'appareil pour éviter de supprimer des traces  
de l'attaque utiles pour les investigations à venir.*



**PRÉVENEZ VOS COLLÈGUES  
DE L'ATTAQUE EN COURS**

*Une mauvaise manipulation de la part d'un autre collaborateur  
pourrait aggraver la situation.*

Pour vous informer sur les bonnes pratiques  
et les principales menaces en matière de cybersécurité  
rendez-vous sur :

[www.cybermalveillance.gouv.fr](http://www.cybermalveillance.gouv.fr)

# Contenus méthodologiques (cadres / dirigeants)

3 piliers pour réduire les risques cyber .....	20
Comment piloter sa cybersécurité .....	21
Que faire en cas de cyberattaque (dirigeants) .....	22
Charte informatique.....	24



# 3 piliers pour prévenir les risques cyber

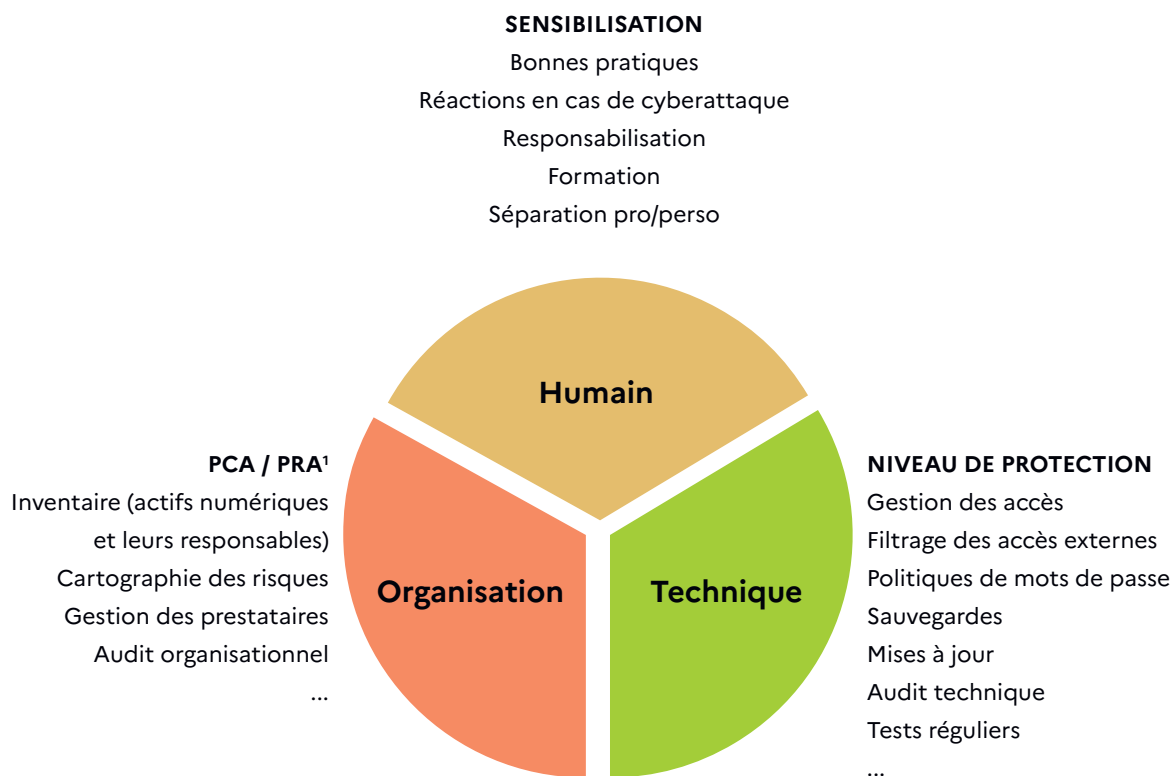
En matière de **prévention des risques**, il existe un standard largement utilisé pour construire un **plan d'action** efficient. Il s'agit du principe « H.O.T. » qui désigne trois domaines : « **H**umain, **O**rganisationnel, **T**echnique ».

Ce principe peut être adapté à la cybersécurité en définissant ces domaines de la manière suivante :

- **Humain** : formation, sensibilisation, communication ;
- **Organisationnel** : méthodes, processus, audits, contrôles ;
- **Technique** : matériels, outils, équipements.

L'idée derrière cette classification est de **vérifier** que toutes **les actions** mises en place (ou devant l'être) au sein de votre organisation soient harmonieusement réparties sur ces **trois composantes essentielles** pour prévenir le maximum de risques informatiques. Par exemple, la cybersécurité ne peut pas reposer uniquement sur des équipements ou des logiciels (domaine Technique) sans prendre en compte des mesures organisationnelles ou humaines.

En détaillant le contenu des domaines H.O.T on peut définir des actions utiles et concrètes pour sécuriser votre système d'information.



Les actions mentionnées ci-dessus sont non exhaustives car elles dépendent de la taille de votre entreprise, de son organisation et de son domaine d'activité.

<sup>1</sup> PCA / PRA : Plan de Continuité d'Activité / Plan de Reprise d'Activité





## COMMENT PILOTER SA CYBERSÉCURITÉ ? (DIRIGEANTS)



Pour en savoir plus, lisez notre article complet sur  
[Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr) en flashant ce QR-code





## QUE FAIRE EN CAS DE CYBERATTAQUE ? (dirigeants)

Méthodologie synthétique de gestion des cyberattaques pour les dirigeants des entreprises, associations, collectivités, administrations.

### 1 PREMIERS RÉFLEXES



**Alertez immédiatement votre support informatique si vous en disposez** afin qu'il prenne en compte l'incident (service informatique, prestataire, personne en charge).



**Isolez les systèmes attaqués** afin d'éviter que l'attaque ne puisse se propager à d'autres équipements en coupant toutes les connexions à Internet et au réseau local.



**Constituez une équipe de gestion de crise** afin de piloter les actions des différentes composantes concernées (technique, RH, financière, communication, juridique...).



**Tenez un registre des événements et actions réalisées** pour pouvoir en conserver la trace à disposition des enquêteurs et tirer les enseignements de l'incident a posteriori.



**Préservez les preuves de l'attaque** : messages reçus, machines touchées, journaux de connexions...

#### NE PAYEZ PAS DE RANÇON !

Car vous encourageriez les cybercriminels à chercher à vous attaquer à nouveau et financeriez leur activité criminelle tout en n'ayant aucune garantie qu'ils tiendront leur parole.

### 2 PILOTER LA CRISE



**Mettez en place des solutions de secours** pour pouvoir continuer d'assurer les services indispensables. Activez vos plans de continuité et de reprise d'activité (PCA-PRA) si vous en disposez.



**Déclarez le sinistre auprès de votre assureur** qui peut vous dédommager voire vous apporter une assistance en fonction de votre niveau de couverture assurantielle.



**Alertez votre banque** au cas où des informations permettant de réaliser des transferts de fonds auraient pu être dérobées.



**Déposez plainte** avant toute action de remédiation en fournissant toutes les preuves en votre possession.



**Identifiez l'origine de l'attaque et son étendue** afin de pouvoir corriger ce qui doit l'être et éviter un nouvel incident.



**Notifiez l'incident à la CNIL** dans les 72h si des données personnelles ont pu être consultées, modifiées ou détruites par les cybercriminels.



**Gérez votre communication** afin d'informer avec le juste niveau de transparence vos administrés, clients, collaborateurs, partenaires, fournisseurs, médias...

#### FAITES-VOUS ACCOMPAGNER

Par des prestataires spécialisés en cybersécurité que vous pourrez trouver sur [www.cybermalveillance.gouv.fr](http://www.cybermalveillance.gouv.fr).



### 3 SORTIR DE LA CRISE



**Faites une remise en service progressive et contrôlée** après vous être assuré que le système attaqué a été corrigé de ses vulnérabilités et en surveillant son fonctionnement pour pouvoir détecter toute nouvelle attaque.



**Tirez les enseignements de l'attaque** et définissez les plans d'action et d'investissements techniques, organisationnels, contractuels, financiers, humains à réaliser pour pouvoir éviter ou a minima pouvoir mieux gérer la prochaine crise.

#### PRENEZ EN COMPTE LES RISQUES PSYCHOLOGIQUES

Une cyberattaque peut engendrer une surcharge exceptionnelle d'activité et un sentiment de sidération, d'humiliation, d'incompétence voire de culpabilité susceptible d'entacher l'efficacité de vos équipes durant la crise et même au-delà.



#### CONTACTS UTILES



##### Conseils et assistance

Dispositif national de prévention et d'assistance  
aux victimes de cybermalveillance  
[www.cybermalveillance.gouv.fr](http://www.cybermalveillance.gouv.fr)

##### Notification de violation de données personnelles

Commission nationale informatique et liberté (CNIL)  
[www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles](http://www.cnil.fr/fr/notifier-une-violation-de-donnees-personnelles)

##### Police – gendarmerie : 17

[17cyber.gouv.fr](http://17cyber.gouv.fr)

La législation française impose à **toute entreprise employant plus de 50 salariés d'avoir un règlement intérieur, qui doit inclure des règles de discipline et de sécurité** applicables aux salariés... dont la cybersécurité. Elle doit aussi être communiquée aux **prestataires externes** dans le cadre de leur intervention en sous-traitance.

La **Commission Nationale de l'Informatique et des Libertés (CNIL)** fournit des conseils utiles en la matière. La charte doit regrouper les règles de **fonctionnement** du système d'information, de **protection** des données et aussi les **sanctions** encourues en cas de non-respect de celles-ci<sup>1</sup>.

Ainsi, on devrait trouver dans cette charte (*a minima*):

1) les **moyens d'authentification** utilisés par l'organisme et sa politique de mots de passe

2) les **règles de sécurité** auxquelles les utilisateurs doivent se conformer, ce qui doit inclure notamment:

- **signaler** au service ou responsable informatique toute violation (ou tentative) suspectée de son compte informatique, toute perte ou vol de matériel et, de manière générale, tout dysfonctionnement;
- **ne jamais confier** son mot de passe (ou équivalent) à un tiers qu'il soit interne ou externe;
- **ne pas installer, copier, modifier, supprimer** des logiciels ou leur paramétrage sans autorisation;
- **verrouiller** son ordinateur dès que l'on quitte son poste de travail;
- **ne pas accéder**, tenter d'accéder à des informations ou les supprimer si cela ne relève pas des tâches incombant à l'utilisateur;
- **respecter** les procédures préalablement définies par l'organisme afin d'encadrer les opérations d'échanges ou de copie de données sur des supports externes, notamment en obtenant l'accord préalable du supérieur hiérarchique et en respectant les règles de sécurité.

<sup>1</sup> Définir un cadre pour les utilisateurs (document CNIL):  
<https://www.cnil.fr/fr/securite-definir-un-cadre-pour-les-utilisateurs>

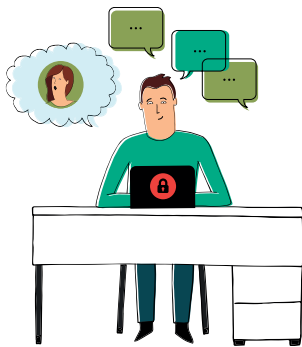
3) Les **modalités d'utilisation des moyens informatiques et de télécommunication** mises à disposition comme :

- le poste de travail et les équipements nomades (notamment dans le cadre du télétravail);
- les espaces de stockage individuel et les réseaux locaux;
- les conditions d'utilisation des dispositifs personnels;
- l'accès à Internet et à la messagerie électronique;
- la téléphonie.

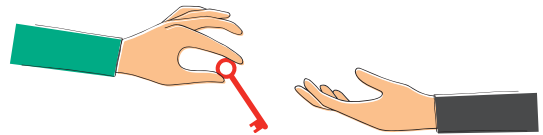
4) Les **conditions d'administration du système d'information**, et l'existence, le cas échéant, de :

- systèmes automatiques de filtrage;
- systèmes automatiques dédiés à la traçabilité des actions;
- systèmes de gestion du poste de travail.

5) Les **responsabilités et sanctions encourues** en cas de non-respect de la charte.



**Veiller à tenir compte  
des besoins réels  
des utilisateurs**



**Accompagner  
les utilisateurs**



**Rendre cette charte  
opposable en l'annexant  
au règlement intérieur**

# Avant de commencer à jouer

Lors des échanges sur les notions théoriques ou lors de la mise en pratique par le jeu de cartes, il est important de pouvoir **clarifier** et rendre **accessible** un certain nombre d'éléments auprès des utilisateurs :

- **Démystifier** les véritables capacités des attaquants (qui sont trop souvent perçus comme des pirates informatiques « omnipotents »);
- Privilégier **les principes généraux** sur lesquels reposent les cyberattaques en les décorrélant des aspects purement techniques (éviter acronymes et anglicismes);
- Ne pas hésiter à **rassurer** les utilisateurs qui ont parfois tendance à associer systématiquement le numérique à la cybermalveillance, au danger et à l'insécurité pour leur organisation.

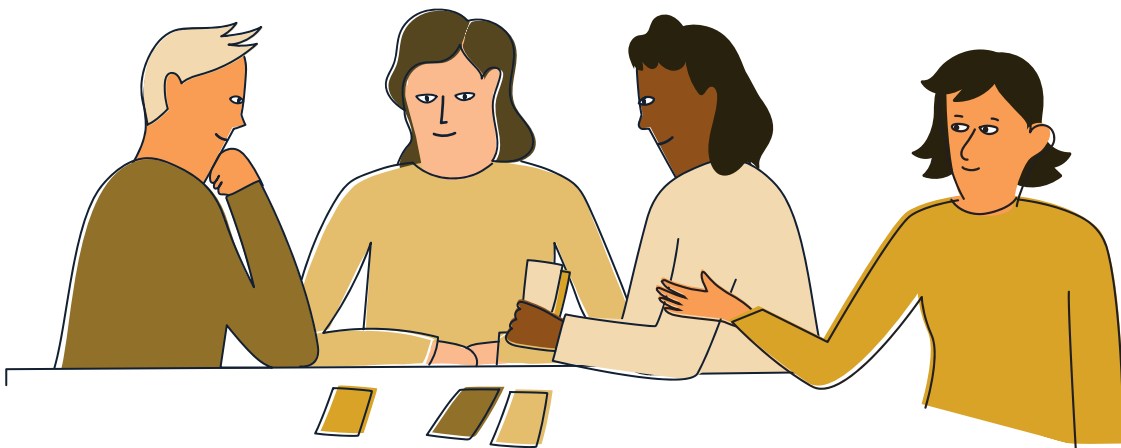
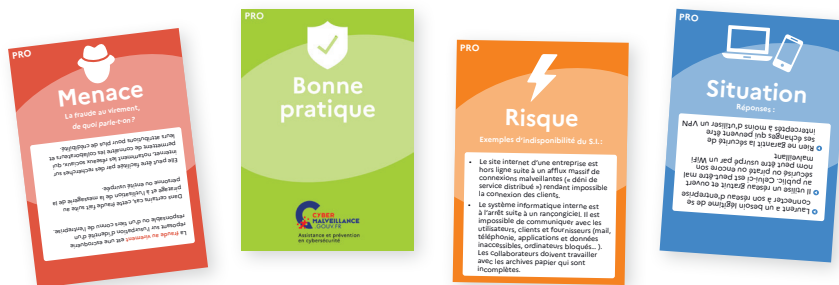
**Pour éviter ces réactions, voici quelques conseils à garder en tête :**

- Utilisez un vocabulaire **simple** et des notions **illustrées** afin d'éviter l'incompréhension ou le rejet;
- Soulignez les **avantages** qu'apporte le numérique (accès à l'information, communication, nouveaux modèles économiques et nouvelles opportunités...);
- N'hésitez pas à insister sur **les bonnes pratiques** plutôt que sur les risques,
- Donnez des exemples et astuces **concrètes**, accessibles pour se protéger en ligne;
- Rappelez, quand c'est le cas, que leur entité a déjà mis en place un certain nombre de **protections** (techniques, organisationnelles, humaines en matière de sensibilisation...) qui les prémunissent des attaques les plus triviales;
- Rassurez-les en leur expliquant que les autorités travaillent à la lutte contre les menaces et que des dispositifs sont en place pour les protéger ou les assister ([17Cyber.gouv.fr](https://17Cyber.gouv.fr)...).



# Présentation du jeu de cartes

Règles du jeu .....	28
Solutions .....	32
Conseils d'animation de groupe .....	36



# Les règles du jeu

Après avoir partagé les contenus de sensibilisation avec les utilisateurs, utilisez le jeu de cartes pour les mettre en action et ainsi faciliter l'apprentissage des conseils et des réflexes cyber.

## PRINCIPE DU JEU DE CARTES

Le jeu de cartes est composé de quatre types de cartes :

- les cartes **Situation**
- les cartes **Menace**
- les cartes **Risque**
- les cartes **Bonne Pratique**

L'objectif pédagogique est de parvenir à associer la menace correspondant à chaque situation, puis d'identifier les risques liés à cette menace, et enfin les bonnes pratiques pour mieux s'en prémunir.



### L'essentiel n'est pas de gagner !

Ce jeu constitue avant tout un support pédagogique pour vous permettre d'initier un dialogue avec les utilisateurs, d'approfondir et enfin d'ancrer leurs connaissances.

La partie sera gagnée si vous parvenez à engager un échange et à répondre aux questions soulevées.

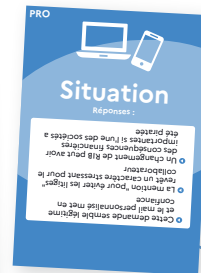
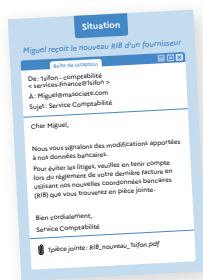




# Structure des cartes

## Carte Situation

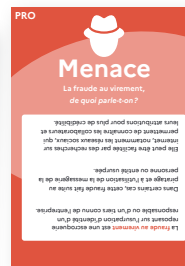
Présente une **situation** dans laquelle un utilisateur est confronté à une cybermenace



Présente les **indices** qui permettent d'identifier une cybermalveillance

## Carte Menace

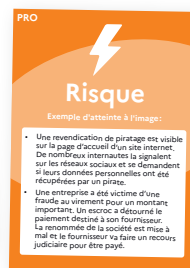
Présente les **principales cybermenaces** auxquelles un utilisateur peut être confronté



Présente les **impacts** que des cybermenaces vis-à-vis de l'entreprise ou de l'organisation

## Carte Risque

Présente les **principaux risques** encourus lorsque l'on fait face à une cybermenace



Présente des **exemples concrets** illustrant chaque risque et indiquant aux utilisateurs ce qu'ils impliquent



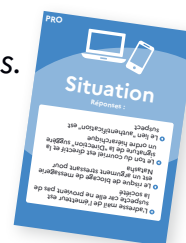
## Carte Bonne Pratique

Présente les **bonnes pratiques** à retenir pour prévenir des cybermenaces

# Déroulé du jeu

## SITUATION

- 1 **Prenez une carte Situation** : vous pouvez choisir la carte en fonction des connaissances et difficultés des participants, ou bien en piocher une au hasard.
- 2 **Donnez la carte** aux participants et demandez à une personne de la décrire et de la **lire à voix haute**.
- 3 Puis aidez-les à **analyser la situation** présentée sur la carte : quelque chose leur semble-t-il anormal ? Et si oui, quoi en particulier ? *Veillez à ce qu'ils ne retournent pas la carte pour ne pas voir les réponses.*
- 4 Laissez-leur le temps de **partager leur raisonnement et de donner leurs réponses**, puis invitez-les à **retourner la carte** pour découvrir les bonnes réponses et répondez à leurs éventuelles questions. Enfin, laissez-les placer la carte sur le **plateau de jeu** à l'emplacement indiqué.



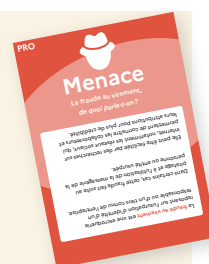
Si les utilisateurs sont en difficulté, essayez de leur poser quelques questions pour les orienter vers les bonnes réponses. Par exemple : « Avez-vous vu l'adresse mail de l'émetteur ? »

## MENACE

- 5 Donnez aux participants **le paquet de cartes Menace** et guidez-les pour **identifier à quelle menace** correspond la situation qu'ils viennent d'analyser. Laissez-leur le temps de sélectionner la carte de leur choix.



Certains utilisateurs peuvent avoir du mal à appréhender ce que représentent les cybermenaces et les effets qu'elles peuvent avoir. Si c'est le cas durant la partie, invitez-les à **retourner les cartes** pour qu'ils puissent découvrir les impacts de ces menaces sur leur milieu professionnel.



- 6 Une fois que les utilisateurs ont choisi une carte, **signalez-leur toute confusion éventuelle**. S'ils ont sélectionné la **bonne carte**, invitez-les à la **placer sur le plateau** à côté de la carte Situation. S'ils ont sélectionné la **mauvaise carte**, donnez-leur la **bonne** en **prenant le temps de leur expliquer**.

→ Les réponses sont présentées page 32

## RISQUE



7 Donnez aux participants le **paquet de cartes Risque** et guidez-les pour **les aider à identifier les risques prioritaires encourus** pour chaque cybermenace précédemment identifiée. Laissez-leur le temps de sélectionner les cartes de leur choix.

8 Une fois que les utilisateurs ont choisi les cartes, vérifiez leur sélection et **signalez leurs éventuelles erreurs**. S'il y en a, indiquez-leur lesquelles et prenez le temps de leur expliquer.

→ Les réponses sont présentées page 32

9 Si besoin, invitez-les à **retourner les cartes** pour découvrir des **exemples concrets** qui illustrent chaque risque, et répondez à leurs éventuelles questions. Enfin, demandez-leur de **placer les cartes Risque sur le plateau** à côté de la carte Menace.

## BONNE PRATIQUE

10 Enfin, donnez aux participants le **paquet de cartes Bonne Pratique**. Ces cartes mentionnent en haut à gauche l'un de ces trois critères : **Humain, Organisation** ou **Technique**. Cette classification (cf. page 20) peut permettre à l'animateur de scinder le paquet « bonnes pratiques » **en trois**.

Laissez-leur le temps de sélectionner les cartes de leur choix pour se prémunir de la menace identifiée.

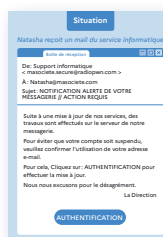
11 Une fois que les utilisateurs ont choisi les cartes, **signalez leurs éventuelles erreurs**. S'il y en a, indiquez-leur lesquelles et explicitiez un choix de cartes plus adapté. Puis demandez-leur de **placer les cartes sur le plateau** à côté des cartes Risque.

Pour conclure la partie, faites le point avec eux et répondez à leurs éventuelles questions.



Vous pouvez ensuite relancer une partie en choisissant une nouvelle carte Situation, ou bien vous arrêter là !

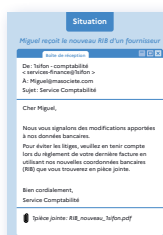
# Solutions



Natasha reçoit un mail du service informatique



Eric reçoit un mail de notification d'un réseau social



Miguel reçoit le nouveau RIB d'un fournisseur



Laurent est en déplacement professionnel et doit se connecter à son réseau d'entreprise



Asma envoie des fichiers volumineux au moyen d'un service grand public



Hameçonnage (Phishing)



Violation de données



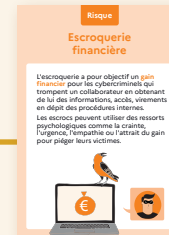
Usurpation d'identité



Fraude au virement (FOVI)



Usurpation d'identité



Escroquerie financière



Récupération de données



Violation de données



Usurpation d'identité

**Risque**

**Escroquerie financière**

L'escroquerie a pour objectif un gain **financier** pour les cybercriminels qui trompent un collaborateur en obtenant de lui des informations, accès, virements en dépit des procédures internes. Les escrocs peuvent utiliser des ressorts psychologiques comme la crainte, l'urgence, l'émotion ou l'attrait du gain pour piéger leurs victimes.



## Escroquerie financière

**HUMAIN** Bonne pratique

**1**

**Limitez la publication d'informations** concernant votre société/organisation et ne publiez pas d'informations internes sensibles sur internet et les réseaux sociaux (déformation de poste, projets, structure de la société, fournisseurs...)

1

**HUMAIN** Bonne pratique

**3**

**Ne pas divulguer, à l'extérieur ou à un contact inconnu, par mail ou téléphone, des informations sur le fonctionnement de la société, ses fournisseurs et clients** (logigrammes, contacts, documents comportant la signature d'acteurs clés, procédures internes...).

3

**ORGA** Bonne pratique

**6**

**Signalez toute sollicitation suspecte** à vos collègues, responsables ou support technique qu'il s'agisse :

- d'un appel ou mail suspect,
- d'un changement de coordonnées bancaires (RIB),
- d'une demande de virement non planifiée.

Cela peut permettre de mettre au grand jour une attaque ciblée contre votre organisation.

6

**HUMAIN** Bonne pratique

**7**

**Soyez vigilant avec les liens ou les pièces jointes** contenus dans les mails, SMS ou QRcode qui peuvent vous mener vers une page d'hameçonnage (phishing) ou infecter votre appareil. Vérifiez bien l'adresse du site avant de renseigner des données. En cas de doute, saisissez directement dans votre navigateur l'adresse du site concerné.

7

**ORGA** Bonne pratique

**12**

**Connaitre et respecter la charte informatique interne.** Ce document établit les droits et obligations des collaborateurs dans les usages numériques au sein de son organisation. En cas de manquement, votre responsabilité personnelle pourrait être engagée.

12

**Risque**

**Atteinte à l'image**

La **réputation** de l'entreprise peut être dégradée suite à des cybermauvaises rendues publiques mettant en avant un défaut de sécurité ou de professionnalisme (négligence de données, fraude au virement, rançongiciel...). Cette mauvaise publicité peut entacher la confiance des clients, fournisseurs ou partenaires.



## Atteinte à l'image

**HUMAIN** Bonne pratique

**1**

**Limitez la publication d'informations** concernant votre société/organisation et ne publiez pas d'informations internes sensibles sur internet et les réseaux sociaux (déformation de poste, projets, structure de la société, fournisseurs...)

1

**HUMAIN** Bonne pratique

**3**

**Ne pas divulguer, à l'extérieur ou à un contact inconnu, par mail ou téléphone, des informations sur le fonctionnement de la société, ses fournisseurs et clients** (logigrammes, contacts, documents comportant la signature d'acteurs clés, procédures internes...).

3

**ORGA** Bonne pratique

**4**

**En cas de demande de virement ou de changement de coordonnées bancaires** (fournisseur, employé, client...) recue par message ou appel, **vérifiez systématiquement** l'identité de votre correspondant en l'appelant directement à un numéro de téléphone en votre possession.

4

**ORGA** Bonne pratique

**6**

**Signalez toute sollicitation suspecte** à vos collègues, responsables ou support technique qu'il s'agisse :

- d'un appel ou mail suspect,
- d'un changement de coordonnées bancaires (RIB),
- d'une demande de virement non planifiée.

Cela peut permettre de mettre au grand jour une attaque ciblée contre votre organisation.

6

**ORGA** Bonne pratique

**12**

**Connaitre et respecter la charte informatique interne.** Ce document établit les droits et obligations des collaborateurs dans les usages numériques au sein de son organisation. En cas de manquement, votre responsabilité personnelle pourrait être engagée.

12

**Risque**

**Atteinte à l'image**

La **réputation** de l'entreprise peut être dégradée suite à des cybermauvaises rendues publiques mettant en avant un défaut de sécurité ou de professionnalisme (négligence de données, fraude au virement, rançongiciel...). Cette mauvaise publicité peut entacher la confiance des clients, fournisseurs ou partenaires.



## Atteinte à l'image

**ORGA** Bonne pratique

**2**

**N'utilisez pas de services externes non validés** par l'entreprise pour manipuler des données internes (traduction ou conversion de documents en ligne, transfert de fichiers, outils d'intelligence artificielle...).

Ces données pourraient être utilisées de manière frauduleuse par un tiers.

2

**TECH** Bonne pratique

**9**

**En mobilité ou télétravail, utilisez le VPN (réseau privé virtuel)** de l'entreprise pour vous connecter à son système informatique.

**Privilégiez la connexion au réseau téléphonique (4G/5G) plutôt qu'à un WiFi Public** (hôtel, gare...). Ces réseaux WiFi, souvent mal sécurisés, peuvent être contrôlés ou usurpés par des pirates qui pourraient capter vos données.

9

**ORGA** Bonne pratique

**12**

**Connaitre et respecter la charte informatique interne.** Ce document établit les droits et obligations des collaborateurs dans les usages numériques au sein de son organisation. En cas de manquement, votre responsabilité personnelle pourrait être engagée.

12

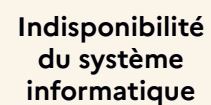
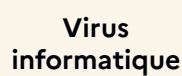
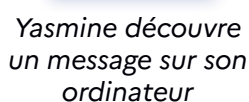
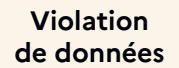
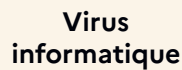
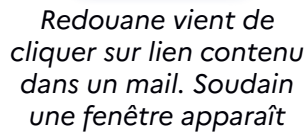
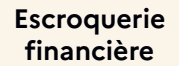
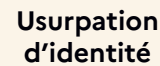
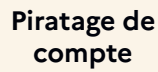
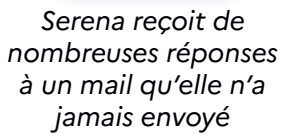
**HUMAIN** Bonne pratique

**13**

**N'utilisez pas des services grand public à des fins professionnelles** pour le stockage de données et les courriels (cloud, transfert de fichiers, transfert de mail vers une adresse personnelle...). Les outils professionnels disposent souvent de protections supplémentaires permettant de limiter les fuites de données.

13

## Solutions



**Risque**

**Violation de données**

La violation de données est la **collecte, la modification, la destruction ou la divulgation non autorisée** d'informations. Son origine peut être accidentelle ou malveillante, interne ou externe à l'organisation qui détient ces données. Elle est souvent la conséquence d'un hameçonnage, d'un piratage, d'une récupération de données ou d'un virus.



## Violation de données

**ORGA** **Bonne pratique**

**6**



**Signalez toute sollicitation suspecte** à vos collègues, responsables ou support technique qu'il s'agisse :

- d'un appel ou mail suspect,
- d'un changement de coordonnées bancaires (RIB),
- d'une demande de virement non planifiée.

Cela peut permettre de mettre au grand jour une attaque ciblée contre votre organisation.

6

**TECH** **Bonne pratique**

**8**




**Utilisez des mots de passe différents et complexes** pour chaque site et application. Vous pouvez utiliser un **gestionnaire de mots de passe** pour les stocker.

**Activez la double authentification** lorsque les sites ou les services le permettent, pour augmenter le niveau de sécurité de vos comptes.

8

**ORGA** **Bonne pratique**

**12**



**Connaitre et respecter la charte informatique interne.** Ce document établit les droits et obligations des collaborateurs dans les usages numériques au sein de son organisation. En cas de manquement, votre responsabilité personnelle pourrait être engagée.

12

**HUMAIN** **Bonne pratique**

**5**



**Ne désactivez jamais l'antivirus** installé par votre organisation sur vos appareils (ordinateur, téléphone, mobile, tablette).

**N'installez pas d'applications** ou de programmes autres que ceux validés par l'entreprise. Des logiciels dont l'origine ou la réputation sont douteuses peuvent contenir des virus.

5

**HUMAIN** **Bonne pratique**

**7**




**Soyez vigilant avec les liens** ou les **pièces jointes** contenus dans les mails, SMS ou Ouboute qui peuvent vous mener vers une page d'hameçonnage (phishing) ou infecter votre appareil.

Vérifiez bien l'adresse du site avant de renseigner des données. En cas de doute, contactez directement dans votre navigateur l'adresse du site concerné.

7

**TECH** **Bonne pratique**

**10**



**Faites les mises à jour de vos appareils, applications et logiciels** dès qu'elles sont proposées pour corriger leurs failles de sécurité qui peuvent être utilisées par des cybercriminels.

10

**ORGA** **Bonne pratique**

**12**



**Connaitre et respecter la charte informatique interne.** Ce document établit les droits et obligations des collaborateurs dans les usages numériques au sein de son organisation. En cas de manquement, votre responsabilité personnelle pourrait être engagée.

12

**TECH** **Bonne pratique**

**15**



**Sauvegardez régulièrement vos données** (sur un disque dur externe, clé USB, serveur, cloud...) et **testez leur restauration** pour pouvoir les retrouver en cas de panne, perte, vol, destruction ou piratage de vos appareils. Débranchez systématiquement le support de sauvegarde après utilisation.

15

**HUMAIN** **Bonne pratique**

**5**



**Ne désactivez jamais l'antivirus** installé par votre organisation sur vos appareils (ordinateur, téléphone, mobile, tablette).

**N'installez pas d'applications** ou de programmes autres que ceux validés par l'entreprise. Des logiciels dont l'origine ou la réputation sont douteuses peuvent contenir des virus.

5

**ORGA** **Bonne pratique**

**6**



**Signalez toute sollicitation suspecte** à vos collègues, responsables ou support technique qu'il s'agisse :

- d'un appel ou mail suspect,
- d'un changement de coordonnées bancaires (RIB),
- d'une demande de virement non planifiée.

Cela peut permettre de mettre au grand jour une attaque ciblée contre votre organisation.

6

**TECH** **Bonne pratique**

**10**



**Faites les mises à jour de vos appareils, applications et logiciels** dès qu'elles sont proposées pour corriger leurs failles de sécurité qui peuvent être utilisées par des cybercriminels.

10

**ORGA** **Bonne pratique**

**11**



**En cas d'infection réelle ou supposée d'un équipement, il faut le déconnecter d'internet et du réseau d'entreprise** pour éviter la contamination d'autres équipements (déconnecter le Wi-Fi, débrancher le câble réseau).

**Ne pas éteindre l'appareil et contacter immédiatement votre support**, prestataire ou référent informatique car des éléments techniques peuvent parfois être récupérés.

11

**ORGA** **Bonne pratique**

**12**




**Connaitre et respecter la charte informatique interne.** Ce document établit les droits et obligations des collaborateurs dans les usages numériques au sein de son organisation. En cas de manquement, votre responsabilité personnelle pourrait être engagée.

12

**ORGA** **Bonne pratique**

**14**



**Ne connectez pas de matériels personnels** ou particuliers sur des ordinateurs professionnels.

**Les supports de stockage externes** (clés USB, disques durs...) peuvent contenir des virus (cléufish, disque dur...). **Connecter un téléphone mobile** à un ordinateur pour le recharger via USB peut compromettre la sécurité en diffusant un virus préalablement présent sur le mobile. Cela revient à brancher une clé USB.

14

**TECH** **Bonne pratique**

**15**



**Sauvegardez régulièrement vos données** (sur un disque dur externe, clé USB, serveur, cloud...) et **testez leur restauration** pour pouvoir les retrouver en cas de panne, perte, vol, destruction ou piratage de vos appareils. Débranchez systématiquement le support de sauvegarde après utilisation.

15



# Conseils d'animation d'un groupe

## EN AMONT

Pour bien vous préparer en tant qu'animateur, **prenez le temps de parcourir ce guide en amont de la session.**

N'hésitez pas à vous familiariser avec les différents supports contenus dans cette mallette. Cela vous permettra de pouvoir répondre plus aisément aux éventuelles questions des participants. Il est essentiel de bien savoir manipuler et connaître l'outil.

## PENDANT

**L'animateur que vous incarnez a pour rôle de faire émerger et de catalyser au mieux l'intelligence collective.** Il génère un climat propice aux échanges, accompagne les participants sans imposer ses points de vue, s'assure que chacun s'exprime et contribue à la production du groupe. Il crée de l'émulation et de l'adhésion.

### —> Posture d'écoute

Vous avez la chance d'endosser le rôle d'animateur ! N'oubliez pas que, durant cette session, vous êtes là pour apporter toute votre expertise sur le sujet, ainsi qu'un regard extérieur. Pour autant, vous privilégiez l'écoute active et les questions ouvertes. Vous guidez les participants dans leur réflexion et encouragez leur réflexivité au travers de questionnements. Pour cela, ne leur donnez pas les réponses trop rapidement, évitez les questions fermées et surtout, reformulez leurs propos et creusez leurs questionnements !

### —> Environnement de partage

Vous communiquez un état d'esprit propice aux échanges, au partage et au droit à l'erreur. Aussi, vous favorisez cette ambiance en créant un espace convivial et de confiance. Soyez attentif à l'agencement de la salle. Si cela vous est possible, n'hésitez pas à utiliser les ressources que vous avez à disposition : mobiliers, plantes, posters, musique, etc.

### —> Introduire

Présentez-le ou les objectifs et le travail que vous allez accomplir ensemble durant cette session. N'hésitez pas à donner quelques règles pour une session réussie (on coupe les portables et les ordinateurs, on instaure la bienveillance...).



## → Établir une connexion

Créez du lien avec les participants, soyez sûr de savoir qui est qui. Montrez-vous attentif et à l'écoute des personnes présentes tout le long de la session. Si les participants ne se connaissent pas, n'hésitez pas à prévoir des fiches adhésives sur lesquelles chacun pourra écrire son prénom et venir le coller sur son vêtement.

### En cas de baisse d'énergie, tout réside dans la posture !

#### ✓ Le discours

Adoptez un discours de motivation afin de faire remonter l'énergie et la motivation de vos participants.

#### ✓ Favoriser les pauses

Il vaut mieux perdre quelques minutes en pause plutôt que d'épuiser vos participants en insistant sur un point.

#### ✓ Profils bloquants

Lorsque vous sentez que le groupe perd sa motivation car une personne est trop bavarde, ou s'il n'y a plus d'alchimie, réamorcez la discussion pour donner une nouvelle impulsion à l'équipe.

Allez chercher ceux qui ne parlent pas en leur donnant la parole.



## Espace prise de notes

Handwriting practice area with 20 horizontal dashed lines.

