RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

Livret pédagogique pour les médiateurs & médiatrices

Comment sensibiliser ses publics à la cybersécurité ?

agence nationale de la cohésion des territoires

Financé par
FRANCE RELANCE

Financé par l'Union européenne
NextGenerationEU

Sommaire

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

Edito

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

6 ans plus tard, avec près de 3,8 millions de visiteurs la plateforme Cybermalveillance.gouv.fr est devenue le plus important producteur de contenus de cybersécurité, avec des réalisations accessibles à tous.

Et pourtant, avec l'explosion des usages numériques, la menace, de plus en plus sophistiquée ne cesse de croître. Or, si les particuliers représentent la majorité de notre audience (92%), force est de constater que tous les publics ne sont pas égaux face à la menace.

C'est pourquoi, conjointement avec l'ANCT (Agence nationale de la cohésion des territoires), membre de Cybermalveillance.gouv.fr, nous avons décidé de mettre en place une démarche pédagogique pour accompagner les populations les plus vulnérables et les plus éloignées du numérique afin de les armer face au risque cyber.

Si le numérique peut être une source d'émancipation, la cybermalveillance est un risque auquel nos concitoyens les plus en difficulté avec le numérique sont particulièrement exposés. En partenariat avec le GIP Acyma, l'ANCT a soutenu la conception de cette mallette afin d'aider, partout en France, les professionnels de la médiation numérique à accompagner la montée en compétence des Français.

Léa **GISLAIS**,
Co-directrice du Programme Société numérique de l'ANCT

Notre ambition ? Mettre à la disposition de tous les acteurs de la médiation numérique (Conseillers numériques France Services - CNFS, France Services, Structures labellisées « Aidants Connect », Structures labellisées « Pass Numérique », etc.) des contenus de sensibilisation cyber pour leur permettre à la fois de s'acculturer au sujet mais surtout de pouvoir transmettre à leurs publics, au travers de contenus adaptés, des conseils pratiques et accessibles afin d'appréhender le sujet de la cybersécurité en toute sérénité et d'évoluer ainsi dans un numérique de confiance. C'est dans ce cadre précis que le projet de création d'une mallette de sensibilisation destinée aux acteurs de la médiation est né.

Plus qu'un outil, cette mallette constitue aujourd'hui un contenu essentiel dans la chaîne de valeur du numérique pour tous les publics éloignés de ce domaine.

Basée sur les attentes et besoins de 700 relais de la médiation, elle a été conçue en intelligence collective, dans un souci constant d'accessibilité, afin de protéger le plus grand nombre des risques cyber.

Gratuite et en source ouverte, cette première version se veut évolutive et repose essentiellement sur le savoir-faire des médiateurs.

Véritable relais de cette opération, vous jouez dans ce projet de sensibilisation à la cybersécurité un rôle fondamental et contribuez ainsi à une démarche d'intérêt public.

Nous vous encourageons à vous approprier ce contenu de façon à ce qu'il puisse répondre au mieux aux exigences de vos publics et espérons qu'il vous sera utile au quotidien.

Je remercie chacun d'entre vous pour son action. Bonne lecture et bonne mise en œuvre !

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

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

Introduction

Ce livret pédagogique s'adresse **aux professionnels de la médiation et de l'inclusion numérique**, afin de les accompagner dans la sensibilisation de leurs publics à la cybersécurité.

CONTEXTE D'UTILISATION DE LA MALLETTE CYBER

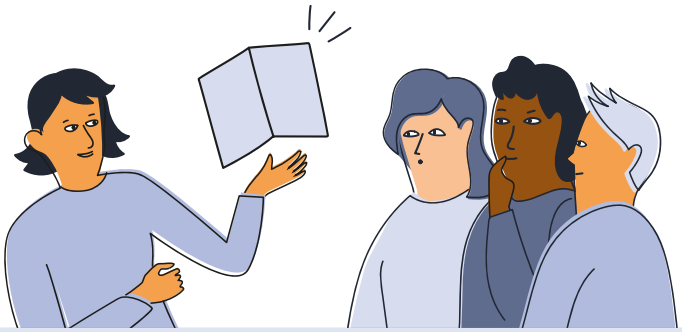
La Mallette Cyber a été conçue dans le cadre d'une démarche de **prévention** à la cybersécurité auprès d'usagers **adultes**.
Elle peut être utilisée lors d'entretiens individuels ou en ateliers **de six usagers maximum** (recommandé).

La Mallette Cyber n'a pas pour vocation d'assister les victimes de cybermalveillances. N'hésitez pas à les rediriger vers les contenus ou le parcours d'assistance victime que propose la plateforme ***Cybermalveillance.gouv.fr.***

En tête à tête ou en groupe 2 à 6 usagers

18+ ans

Prévention uniquement

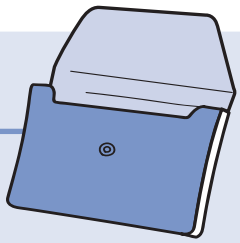


En tant que médiateur, nous vous invitons à vous approprier l'ensemble des contenus de la Mallette Cyber **avant de débuter votre entretien ou votre atelier.**

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

COMPOSANTS DE LA MALLETTE CYBER



UN LIVRET PÉDAGOGIQUE composé de :

→ **contenus de sensibilisation** à la cybersécurité avec des fiches réflexes et des fiches pratiques

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

UN SUPPORT DE MÉDIATION avec :

→ des **fiches sur les menaces** les plus courantes et **les bonnes pratiques** à adopter

UN JEU DE CARTES ET UN PLATEAU DE JEU

→ pour mettre en pratique et ancrer les notions abordées avec les usagers

UNE INFOGRAPHIE

→ à imprimer et à remettre à chaque usager pour lui laisser un résumé des bonnes pratiques essentielles

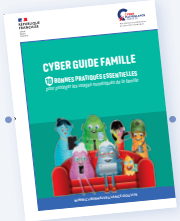
RESSOURCES COMPLÉMENTAIRES

Ce guide et les éléments qui vous ont été remis sont complétés par une page et des ressources **gratuites** dédiées aux acteurs de l'inclusion / médiation numérique en ligne sur **Cybermalveillance.gouv.fr**... Allez vite les consulter !

STICKERS

AFFICHE A2

«LES ESSENTIELS DE VOTRE SÉCURITÉ NUMÉRIQUE»



CYBER GUIDE FAMILLE

FLYER

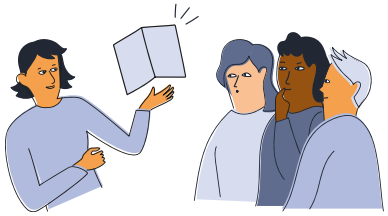
CYBERMALVEILLANCE.GOUV.FR

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 les supports de médiation pour transmettre les notions aux usagers.

3. Pratiquer et illustrer

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

4. Pérenniser

À la fin de l'atelier ou de l'entretien, pour inciter l'usager à devenir autonome, remettez lui l'infographie qui résume les principales recommandations à retenir.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

1

Contenus de sensibilisation

à l'usage du médiateur

Les menaces les plus courantes

Les mesures de sécurité à retenir

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention en sécurité numérique

COMPRENDRE LES RISQUES

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'utilisiez (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, **SIGNALEZ-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 PLAINTE** 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

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

LE PIRATAGE DE COMPTE

COMPRENDRE LES RISQUES

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 PLAINTE** 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

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

COMPRENDRE LES RISQUES

L'ARNAQUE AU FAUX SUPPORT TECHNIQUE

L'arnaque au faux support technique (***Tech support scam*** en anglais) consiste à effrayer la victime, par SMS, téléphone, chat, courriel, ou par l'apparition d'un message qui bloque son ordinateur, lui indiquant un problème technique grave et un risque de perte de ses données ou de l'usage de son équipement afin de la pousser à contacter un prétendu support technique officiel (Microsoft, Apple, Google…), pour ensuite la convaincre de payer un pseudo-dépannage informatique et/ou à acheter des logiciels inutiles, voire nuisibles. Si la victime refuse de payer, les criminels peuvent la menacer de détruire ses fichiers ou de divulguer ses informations personnelles.

BUT RECHERCHÉ

Soutirer de l'argent à la victime en la poussant à laisser prendre le contrôle de sa machine pour faire semblant de la lui dépanner et lui installer des logiciels et/ou faire souscrire des abonnements qui lui seront facturés.

SI VOUS ÊTES VICTIME

NE RÉPONDEZ PAS AUX SOLLICITATIONS et n'appelez jamais le numéro indiqué.

CONSERVEZ TOUTES LES PREUVES. Photographiez votre écran au besoin.

S'il semble « bloqué », **REDÉMARREZ VOTRE APPAREIL**. Cela peut suffire à régler le problème.

Si votre navigateur reste incontrôlable, **PURGEZ LE CACHE, SUPPRIMEZ LES COOKIES, RÉINITIALISEZ LES PARAMÈTRES PAR DÉFAUT** et si cela ne suffit pas, supprimez et recréez votre profil.

DÉSINSTALLEZ TOUTE NOUVELLE APPLICATION SUSPECTE présente sur votre appareil.

FAITES UNE ANALYSE ANTIVIRALE COMPLÈTE de votre appareil.

Si un faux technicien a pris le contrôle de votre machine, **DÉSINSTALLEZ LE PROGRAMME DE GESTION À DISTANCE ET CHANGEZ TOUS VOS MOTS DE PASSE**. En cas de doute ou si vous n'arrivez pas à reprendre le contrôle de votre appareil, vous pouvez faire appel à un professionnel référencé sur www.cybermalveillance.gouv.fr/diagnostic/profil.

Si vous avez fourni vos coordonnées de carte bancaire, **FAITES OPPOSITION SANS DÉLAI**. Si un paiement est débité sur votre compte, **EXIGEZ LE REMBOURSEMENT** en indiquant que vous déposez plainte.

SIGNALEZ LES FAITS sur la plateforme Internet-signalement.gouv.fr du ministère de l'Intérieur.

En fonction du préjudice subi, **DÉPOSEZ PLAINTE** 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.

MESURES PRÉVENTIVES

Appliquez de manière régulière et systématique les mises à jour de sécurité du système et des logiciels installés sur votre machine, en particulier vos navigateurs.

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

Évitez les sites non sûrs ou illicites, tels ceux qui hébergent des contrefaçons (musique, films, logiciels…) ou certains sites pornographiques qui peuvent infecter votre machine ou héberger des régies publicitaires douteuses.

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

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

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.

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

Aucun support technique officiel ne vous contactera jamais pour vous réclamer de l'argent.

EN PARTENARIAT AVEC :
MINISTÈRE DE L'INTÉRIEUR
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

COMPRENDRE LES RISQUES

FUITE OU VIOLATION DE DONNÉES PERSONNELLES

Une fuite ou violation de données personnelles est l'accès ou la divulgation non autorisés d'informations personnelles détenues par un tiers (site Internet, entreprise, association, collectivité, administration...). Une donnée personnelle est une information susceptible de permettre d'identifier une personne (nom, adresse postale ou de messagerie, numéro de téléphone ou de sécurité sociale...). L'origine de la fuite peut être accidentelle ou malveillante. Selon la nature des informations concernées et si elles sont récupérées par des cybercriminels, une fuite de données personnelles peut avoir de multiples conséquences pour la personne qui en est victime : hameçonnage ciblé, escroquerie, usurpation d'identité, piratage de compte en ligne...

BUT RECHERCHÉ

Les informations personnelles divulguées (identité, mot de passe, données bancaires...) peuvent être récupérées par des cybercriminels pour en faire un usage frauduleux.

SI VOUS ÊTES VICTIME

Si vous êtes informé d'une possible violation de vos données personnelles, **CONTACTEZ AU BESOIN LE SERVICE OU ORGANISME CONCERNÉ** pour la confirmer et savoir quelles informations ont pu être compromises.

CHANGEZ AU PLUS VITE VOTRE MOT DE PASSE sur les sites ou services concernés par la fuite de données ainsi que sur tous les autres sites ou comptes sur lesquels vous pouviez l'utiliser.

Si vos coordonnées bancaires figurent dans la fuite de données, **PRÉVENEZ IMMÉDIATEMENT VOTRE BANQUE** et faites au besoin opposition aux moyens de paiement concernés. Contrôlez régulièrement vos comptes pour détecter toute opération anormale.

SIGNALEZ ET DEMANDEZ LA SUPPRESSION DES PAGES, COMPTES, MESSAGES DIVULGUANT VOS INFORMATIONS PERSONNELLES auprès des plateformes sur lesquelles elles sont diffusées.

DEMANDEZ À CE QUE VOS DONNÉES PERSONNELLES DIVULGUÉES NE SOIENT PLUS RÉFÉRENCÉES PAR LES MOTEURS DE RECHERCHE lorsqu'elles y apparaissent.

Si, un mois après votre demande de suppression, vos données personnelles sont toujours accessibles, **VOUS POUVEZ ADRESSER UNE RÉCLAMATION (PLAINTE) À LA CNIL.**

En cas d'utilisation frauduleuse de vos données personnelles, conservez toutes les preuves et **DÉPOSEZ PLAINTE** 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.

ENGAGEZ AU BESOIN UNE ACTION DE GROUPE OU UN RECOURS COLLECTIF qui permet aux victimes de demander la cessation de la violation de données personnelles et la réparation du préjudice.

MESURES PRÉVENTIVES

Ne communiquez que le minimum d'informations nécessaires sur les sites ou services en ligne.

Ne communiquez pas de documents d'identité de manière inconsidérée (pièce d'identité, fiche de paie, avis d'imposition, RIB, etc.).

N'enregistrez pas vos coordonnées de carte bancaire pour des achats ponctuels sur un site Internet. Si vous les avez enregistrées, supprimez-les.

Utilisez des mots de passe différents et complexes pour chaque site et application pour que la compromission d'un de vos mots de passe n'impacte pas vos autres comptes. Tous nos conseils pour gérer vos mots de passe.

Activez la double authentification pour augmenter le niveau de sécurité d'accès à vos comptes lorsque le site ou le service le permettent.

Désabonnez-vous ou supprimez les comptes en ligne que vous n'utilisez plus pour limiter les risques de fuite de vos données.

Faites valoir votre droit de suppression de vos données personnelles auprès des organismes et services avec lesquels vous n'avez plus de relation. La CNIL peut être saisie en cas de difficulté.

EN PARTENARIAT AVEC:
MINISTÈRE DE L'INTÉRIEUR
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

LES **10 MESURES ESSENTIELLES** POUR ASSURER VOTRE SÉCURITÉ NUMÉRIQUE

Que ce soit dans un cadre professionnel ou personnel, l'utilisation des outils numériques ne cesse de croître et de se diversifier. Ordinateurs de bureau ou portables, téléphones mobiles, tablettes, objets connectés... Ils font de plus en plus partie de notre quotidien. Cette intensification des usages représente pour les cybercriminels une opportunité de développer leurs attaques. Comment se protéger au mieux face à ces risques ? **Voici 10 bonnes pratiques essentielles à adopter pour assurer votre sécurité numérique.**

1 PROTÉGEZ VOS ACCÈS AVEC DES MOTS DE PASSE SOLIDES

Utilisez des mots de passe suffisamment longs, complexes et différents sur tous les équipements et services auxquels vous accédez, qu'ils soient personnels ou professionnels. La majorité des attaques est souvent due à des mots de passe trop simples ou réutilisés. Au moindre doute, ou même régulièrement en prévention, changez-les. Utilisez un gestionnaire de mots de passe et activez la double authentification chaque fois que c'est possible pour renforcer votre sécurité.

2 SAUVEGARDEZ VOS DONNÉES RÉGULIÈREMENT

En cas de piratage, mais également en cas de panne, de vol ou de perte de votre appareil, la sauvegarde est souvent le seul moyen de retrouver vos données (photos, fichiers, contacts, messages...). Sauvegardez régulièrement les données de vos PC, téléphones portables, tablettes et conservez toujours une copie de vos sauvegardes sur un support externe à votre équipement (clé ou disque USB) que vous débranchez une fois la sauvegarde effectuée.

3 APPLIQUEZ LES MISES À JOUR DE SÉCURITÉ SUR TOUS VOS APPAREILS (PC, TABLETTES, TÉLÉPHONES...), DÈS QU'ELLES VOUS SONT PROPOSÉES

Vous corrigez ainsi les failles de sécurité qui pourraient être utilisées par des pirates pour s'introduire dans vos appareils, pour y dérober vos informations personnelles ou vos mots de passe, voire pour détruire vos données ou encore vous espionner (mises à jour).

4 UTILISEZ UN ANTIVIRUS

Les antivirus permettent de se protéger d'une grande majorité d'attaques et de virus connus. Il existe de nombreuses solutions gratuites ou payantes selon vos usages et le niveau de protection ou de services recherchés. Vérifiez régulièrement que les antivirus de vos équipements sont bien à jour et faites des analyses (scans) approfondies pour vérifier que vous n'avez pas été infecté.

5 TÉLÉCHARGEZ VOS APPLICATIONS UNIQUEMENT SUR LES SITES OFFICIELS

N'installez des applications que depuis les sites ou magasins officiels des éditeurs (exemple : Apple App Store, Google Play Store) pour limiter les risques d'installation d'une application piégée pour pirater vos équipements. De même, évitez les sites Internet suspects ou frauduleux (téléchargement, vidéo, streamings illégaux) qui pourraient également installer un virus sur vos matériels.

EN PARTENARIAT AVEC :
MINISTÈRE DE L'INTÉRIEUR
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

6 MÉFIEZ-VOUS DES MESSAGES INATTENDUS

En cas de réception d'un message inattendu ou alarmiste par messagerie (*e-mail*), SMS ou chat, demandez toujours confirmation à l'émetteur par un autre moyen s'il vous semble connu et légitime. Il peut en effet s'agir d'une attaque par hameçonnage (*phishing*) visant à vous piéger pour vous dérober des informations confidentielles (mots de passe, informations d'identité ou bancaires), de l'envoi d'un virus contenu dans une pièce jointe qu'on vous incite à ouvrir, ou d'un lien qui vous attirerait sur un site malveillant.

7 VÉRIFIEZ LES SITES SUR LESQUELS VOUS FAITES DES ACHATS

Si le commerce en ligne facilite les achats et offre l'opportunité de faire de bonnes affaires, il existe malheureusement de nombreux sites de vente douteux, voire malveillants. Avant d'acheter sur Internet, vérifiez que vous n'êtes pas sur une copie frauduleuse d'un site officiel, la crédibilité de l'offre et consultez les avis. Sans cette vérification, vous prenez le risque de vous faire dérober votre numéro de carte bancaire et de ne jamais recevoir votre commande, voire de recevoir une contrefaçon ou un produit dangereux.

8 MAÎTRISEZ VOS RÉSEAUX SOCIAUX

Les réseaux sociaux sont de formidables outils de communication et d'information collaboratifs. Ils contiennent toutefois souvent de nombreuses informations personnelles qui ne doivent pas tomber dans de mauvaises mains. Sécurisez l'accès à vos réseaux sociaux avec un mot de passe solide et unique, définissez les autorisations sur vos informations et publications pour qu'elles ne soient pas inconsidérément publiques ou utilisées pour vous nuire, ne relayez pas d'informations non vérifiées (*fake news*).

9 SÉPAREZ VOS USAGES PERSONNELS ET PROFESSIONNELS

Avec l'accroissement des usages numériques, la frontière entre utilisation personnelle et professionnelle est souvent ténue. Ces utilisations peuvent même parfois s'imbriquer. Matériels, messageries, « *clouds* »… Il est important de séparer vos usages afin que le piratage d'un accès personnel ne puisse pas nuire à votre entreprise, ou inversement, que la compromission de votre entreprise ne puisse pas avoir d'impact sur la sécurité de vos données personnelles (usages personnels et professionnels).

10 ÉVITEZ LES RÉSEAUX WIFI PUBLICS OU INCONNUS

En mobilité, privilégiez la connexion de votre abonnement téléphonique (3G ou 4G) aux réseaux WiFi publics. Ces réseaux WiFi sont souvent mal sécurisés, et peuvent être contrôlés ou usurpés par des pirates qui pourraient ainsi voir passer et capturer vos informations personnelles ou confidentielles (mots de passe, numéro de carte bancaire…). Si vous n'avez d'autre choix que d'utiliser un WiFi public, veillez à ne jamais y réaliser d'opérations sensibles et utilisez si possible un réseau privé virtuel (VPN).

RETROUVEZ TOUTES NOS PUBLICATIONS SUR :
www.cybermalveillance.gouv.fr

Licence Ouverte v2.0 (ETALAB)

Version 1.0

LA SÉCURITÉ **DES APPAREILS MOBILES**

Les téléphones mobiles intelligents (smartphones) et tablettes informatiques sont devenus des instruments pratiques du quotidien, tant pour un usage personnel que professionnel. Leurs capacités ne cessent de croître et les fonctionnalités qu'ils offrent s'apparentent, voire dépassent parfois, celles des ordinateurs. Ils contiennent tout autant et plus d'informations sensibles ou permettent d'y accéder. Ils sont plus faciles à perdre ou à se faire voler. Ces appareils mobiles sont, malgré tout, généralement bien moins sécurisés que les ordinateurs par leurs propriétaires. **Voici 10 bonnes pratiques à adopter pour la sécurité de vos appareils mobiles.**

1 METTEZ EN PLACE LES CODES D'ACCÈS

Qu'il s'agisse du code de déverrouillage ou du code PIN, ces protections complémentaires (voir encadré) empêcheront une personne malintentionnée de pouvoir se servir facilement de votre appareil si vous en perdez le contrôle (perte, vol, abandon) et donc d'accéder à vos informations. Bien entendu, vos codes d'accès doivent être suffisamment difficiles à deviner (évitez 0000 ou 1234, par exemple). Activez également le verrouillage automatique de votre appareil afin que le code d'accès soit demandé au bout de quelques minutes si vous laissez votre appareil sans surveillance.

CODE D'ACCÈS ET CODE PIN, DEUX PROTECTIONS COMPLÉMENTAIRES

Mot de passe, signe, combinaison de touches ou biométrie: **le code de verrouillage empêche de pouvoir se servir de l'appareil si on ne le connaît pas.**

Composé de 4 chiffres, **le code PIN bloque quant à lui l'accès à votre carte SIM** et empêche donc de pouvoir s'en servir dans un autre appareil si on ne le connaît pas.

2 CHIFFREZ LES DONNÉES DE L'APPAREIL

En cas de perte ou de vol, seul le chiffrement des données contenues dans votre appareil vous assurera qu'une personne malintentionnée ne pourra pas contourner les codes d'accès et accéder quand même à vos informations. Tous les appareils récents proposent cette option qu'il suffit d'activer dans les paramètres et qui est quasi transparente à l'utilisation. Si vous utilisez une carte d'extension mémoire pour stocker vos informations, vérifiez qu'elle est également chiffrée.

3 APPLIQUEZ LES MISES À JOUR DE SÉCURITÉ

Qu'il s'agisse du système d'exploitation (Android, iOS) ou des applications qui sont sur votre appareil, installez sans tarder les mises à jour dès qu'elles sont proposées car elles corrigent souvent des failles de sécurité qui pourraient être exploitées par des cybercriminels pour prendre le contrôle de votre appareil et accéder à vos informations.

4 FAITES DES SAUVEGARDES

Votre appareil mobile contient généralement des informations que vous n'avez nulle part ailleurs, comme votre répertoire de contacts, vos messages, vos photos… Pensez à le sauvegarder régulièrement car vous pourriez tout perdre en cas de casse, de perte ou de vol.

5 UTILISEZ UNE SOLUTION DE SÉCURITÉ CONTRE LES VIRUS ET AUTRES ATTAQUES

De nombreuses solutions de sécurité existent pour aider à se protéger des différentes attaques que peuvent subir les appareils mobiles au même titre que les ordinateurs de bureau comme les virus, les rançongiciels (*ransomware*), l'hameçonnage (*phishing*)… Des cybercriminels se spécialisent dans les attaques d'appareils mobiles qu'ils savent souvent bien moins sécurisés que les ordinateurs de bureau. Il est donc important d'avoir un bon niveau de protection et de s'équiper d'un produit spécialisé.

EN PARTENARIAT AVEC:
MINISTÈRE DE L'INTÉRIEUR
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

6 N'INSTALLEZ DES APPLICATIONS QUE DEPUIS LES SITES OU MAGASINS OFFICIELS

Seuls les sites ou magasins officiels vous permettent de vous assurer au mieux que les applications que vous installez ne sont pas piégées. Méfiez-vous des sites « parallèles », qui ne contrôlent pas les applications qu'ils proposent ou qui offrent gratuitement des applications normalement payantes en téléchargement illégal : elles sont généralement piégées. Consultez le nombre de téléchargements et les avis des autres utilisateurs avant d'installer une nouvelle application. Au moindre doute, n'installez pas l'application et choisissez-en une autre.

7 CONTRÔLEZ LES AUTORISATIONS DE VOS APPLICATIONS

Vérifiez également les autorisations que vous donnez à vos applications lors de leur première installation, mais aussi après leurs mises à jour car leurs autorisations peuvent évoluer. Certaines applications demandent parfois des droits très importants sur vos informations et qui peuvent être « surprenants ». Par exemple, un simple jeu de cartes « gratuit » qui vous demanderait l'autorisation d'accéder à votre répertoire, vos mots de passe, vos messages, votre position GPS ou encore votre appareil photo est évidemment suspect. Au moindre doute, n'installez pas l'application et choisissez-en une autre.

8 NE LAISSEZ PAS VOTRE APPAREIL SANS SURVEILLANCE

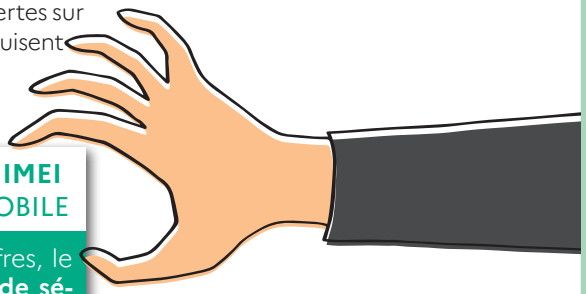
Une personne malintentionnée pourrait profiter de votre manque de vigilance pour accéder à vos informations ou piéger votre appareil. Pour ces mêmes raisons, il est fortement déconseillé de laisser un tiers se servir de votre appareil mobile (pour passer un appel par exemple) sans que vous ne puissiez contrôler physiquement l'utilisation réelle qu'il en fait.

9 ÉVITEZ LES RÉSEAUX WIFI PUBLICS OU INCONNUS

Ces réseaux peuvent être contrôlés par des cybercriminels qui peuvent intercepter vos connexions et récupérer au passage vos comptes d'accès, mots de passe, données de carte bancaire… afin d'en faire un usage délictueux. D'une manière générale, désactivez toutes les connexions sans fil quand vous ne vous en servez pas (Wi-Fi, Bluetooth, NFC…) car elles sont autant de portes d'entrée ouvertes sur votre appareil. De plus, elles épuisent votre batterie inutilement.

10 NE STOCKEZ PAS D'INFORMATIONS CONFIDENTIELLES SANS PROTECTION

Ne notez jamais d'informations secrètes comme vos mots de passe ou vos codes bancaires dans votre répertoire de contacts, votre messagerie ou un fichier non chiffré sur votre appareil mobile. Un cybercriminel qui aurait pris le contrôle de votre appareil pourrait facilement les récupérer. En outre, certaines applications que vous avez installées peuvent aussi accéder et récupérer ces informations dont vous perdriez alors le contrôle. Pour protéger vos informations secrètes, utilisez une solution de chiffrement avec un mot de passe solide.



CONSERVEZ LE CODE IMEI DE VOTRE APPAREIL MOBILE

Composé de 15 à 17 chiffres, le code IMEI est **le numéro de série de votre appareil mobile**. Il est généralement inscrit sur sa boîte d'emballage. En cas de perte ou de vol, ce code peut permettre de bloquer l'usage du téléphone sur tous les réseaux.

Notez-le soigneusement et si vous l'avez égaré **vous pouvez le récupérer en tapant *#06# sur votre clavier.**

POUR ALLER PLUS LOIN

- **Par la CNIL :** Comment sécuriser au maximum l'accès à votre smartphone ?
- **Par l'ANSSI :** Sécuriser son ordiphone

DOCUMENT RÉALISÉ AVEC NOS MEMBRES :

CHAMBRE DE COMMERCE ET D'INDUSTRIE · CLUSIF · e-Enfance 3018

RETROUVEZ TOUTES NOS PUBLICATIONS SUR :
www.cybermalveillance.gouv.fr

Licence Ouverte v2.0 (ETALAB)

Version 2.0

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

LES MOTS DE PASSE

Messageries, réseaux sociaux, banques, administrations et commerces en ligne, réseaux et applications d'entreprise… la sécurité de l'accès à tous ces services du quotidien repose aujourd'hui essentiellement sur les mots de passe. Face à la profusion des mots de passe, la tentation est forte d'en avoir une gestion trop simple. Une telle pratique serait dangereuse, car elle augmenterait considérablement les risques de compromettre la sécurité de vos accès. **Voici 10 bonnes pratiques à adopter pour gérer efficacement vos mots de passe.**

1 UTILISEZ UN MOT DE PASSE DIFFÉRENT POUR CHAQUE SERVICE

Ainsi en cas de perte ou de vol d'un de vos mots de passe, seul le service concerné sera vulnérable. Dans le cas contraire, tous les services pour lesquels vous utilisez le même mot de passe compromis seraient piratables.

2 UTILISEZ UN MOT DE PASSE SUFFISAMMENT LONG ET COMPLEXE

Une technique d'attaque répandue, dite par « force brute », consiste à essayer toutes les combinaisons possibles de caractères jusqu'à trouver le bon mot de passe. Réalisées par des ordinateurs, ces attaques peuvent tester des dizaines de milliers de combinaisons par seconde. Pour empêcher ce type d'attaque, il est admis qu'un bon mot de passe doit comporter au minimum 12 signes mélangeant des majuscules, des minuscules, des chiffres et des caractères spéciaux.

3 UTILISEZ UN MOT DE PASSE IMPOSSIBLE À DEVINER

Une autre technique d'attaque utilisée par les pirates est d'essayer de « deviner » votre mot de passe. Évitez donc d'employer dans vos mots de passe des informations personnelles qui pourraient être faciles à retrouver (sur les réseaux sociaux par exemple), comme le prénom de votre enfant, une date anniversaire ou votre groupe de musique préféré. Évitez également les suites logiques simples comme 123456, azerty, abcdef… qui font partie des listes de mots de passe les plus courants et qui sont les premières combinaisons qu'essaieront les cybercriminels pour tenter de forcer vos comptes.

4 UTILISEZ UN GESTIONNAIRE DE MOTS DE PASSE

Il est humainement impossible de retenir les dizaines de mots de passe longs et complexes que chacun est amené à utiliser quotidiennement. Ne commettez pas pour autant l'erreur de les noter sur un pense-bête que vous laisseriez à proximité de votre équipement, ni de les inscrire dans votre messagerie ou dans un fichier non protégé de votre ordinateur, ou encore dans votre téléphone mobile auquel un cybercriminel pourrait avoir accès. Apprenez à utiliser un gestionnaire de mot de passe sécurisé qui s'en chargera à votre place, pour ne plus avoir à retenir que le seul mot de passe qui permet d'en ouvrir l'accès. *Voir notre encadré sur Keepass au dos de cette fiche.*

5 CHANGEZ VOTRE MOT DE PASSE AU MOINDRE SOUPÇON

Vous avez un doute sur la sécurité d'un de vos comptes ou vous entendez qu'une organisation ou société chez qui vous avez un compte s'est faite pirater. N'attendez pas de savoir si c'est vrai ou pas. Changez immédiatement le mot de passe concerné avant qu'il ne tombe dans de mauvaises mains.

CRÉER UN MOT DE PASSE SOLIDE

LA MÉTHODE DES PREMIÈRES LETTRES
Un tiens vaut mieux que deux tu l'auras
1tvmQ2tl'A

LA MÉTHODE PHONÉTIQUE
J'ai acheté huit CD pour cent euros cet après-midi
ght8CD%E7am

Inventez votre propre méthode connue de vous seul !

EN PARTENARIAT AVEC :
MINISTÈRE DE L'INTÉRIEUR
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

KEEPASS

UN GESTIONNAIRE DE MOTS DE PASSE SÉCURISÉ ET GRATUIT

Ce petit logiciel libre et en français, certifié par l'ANSSI, permet de stocker en sécurité vos mots de passe pour les utiliser dans vos applications. Il dispose aussi d'une fonction permettant de générer des mots de passe complexes aléatoires. **https://keepass.info**

6 NE COMMUNIQUEZ JAMAIS VOTRE MOT DE PASSE À UN TIERS

Votre mot de passe doit rester secret. Aucune société ou organisation sérieuse ne vous demandera jamais de lui communiquer votre mot de passe par messagerie ou par téléphone. Même pour une « maintenance » ou un « dépannage informatique ». Si l'on vous demande votre mot de passe, considérez que vous êtes face à une tentative de piratage ou d'escroquerie.

7 N'UTILISEZ PAS VOS MOTS DE PASSE SUR UN ORDINATEUR PARTAGÉ

Les ordinateurs en libre accès que vous pouvez utiliser dans des hôtels, cybercafés et autres lieux publics peuvent être piégés et vos mots de passe peuvent être récupérés par un criminel. Si vous êtes obligé d'utiliser un ordinateur partagé ou qui n'est pas le vôtre, utilisez le mode de « navigation privée » du navigateur, qui permet d'éviter de laisser trop de traces informatiques, veillez à bien fermer vos sessions après utilisation et n'enregistrez jamais vos mots de passe dans le navigateur. Enfin, dès que vous avez à nouveau accès à un ordinateur de confiance, changez au plus vite tous les mots de passe que vous avez utilisés sur l'ordinateur partagé.

8 ACTIVEZ LA « DOUBLE AUTHENTIFICATION* » LORSQUE C'EST POSSIBLE

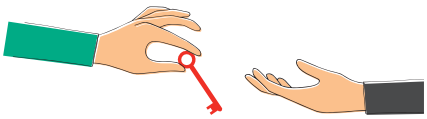
Pour renforcer la sécurité de vos accès, de plus en plus de services proposent cette option . En plus de votre nom de compte et de votre mot de passe, ces services vous demandent une confirmation que vous pouvez recevoir, par exemple, sous forme de code provisoire reçu par SMS ou par courrier électronique (e-mail), via une application ou une clé spécifique que vous contrôlez, ou encore par reconnaissance biométrique. Ainsi grâce à cette confirmation, vous seul pourrez autoriser un nouvel appareil à se connecter aux comptes protégés. *Voir encadré.*

9 CHANGEZ LES MOTS DE PASSE PAR DÉFAUT DES DIFFÉRENTS SERVICES AUXQUELS VOUS ACCÉDEZ

De nombreux services proposent des mots de passe par défaut que vous n'êtes parfois pas obligé de changer. Ces mots de passe par défaut sont souvent connus des cybercriminels. Aussi, il est important de les remplacer au plus vite par vos propres mots de passe que vous contrôlez.

QUELQUES SERVICES PROPOSANT LA DOUBLE AUTHENTIFICATION

- Outlook/Hotmail, Gmail, Yahoo Mail…
- Facebook, Instagram, LinkedIn, Snapshat, Tik Tok, Twitter…
- Skype, Teams, WhatsApp, Zoom…
- Amazon, eBay, Paypal…
- Apple iCloud, Dropbox, Google Drive, OneDrive…



10 CHOISISSEZ UN MOT DE PASSE PARTICULIÈREMENT ROBUSTE POUR VOTRE MESSAGERIE

Votre adresse de messagerie est généralement associée à beaucoup de vos comptes en ligne. Cela permet notamment de recevoir les liens de réinitialisation des mots de passe de vos autres comptes. Un cybercriminel qui réussirait à pirater votre messagerie pourrait facilement utiliser la fonction « mot de passe oublié » des différents services auxquels vous pouvez accéder, comme votre compte bancaire, pour en prendre le contrôle. **Votre mot de passe de messagerie est donc un des mots de passe les plus importants à protéger**.

POUR ALLER PLUS LOIN

- **Par la CNIL :** Les conseils de la CNIL pour un bon mot de passe
- **Par l'ANSSI :** Sécurité des mots de passe

DOCUMENT RÉALISÉ AVEC NOS MEMBRES :
FRANCE ASSUREURS · kaspersky · LA POSTE GROUPE · signal spam

* Également appelée « authentification forte », « authentification multifacteurs », « 2FA », « vérification en deux étapes », « validation en deux étapes », « authentification à deux facteurs », « identification à deux facteurs », « vérification en deux temps »…

RETROUVEZ TOUTES NOS PUBLICATIONS SUR :
www.cybermalveillance.gouv.fr

Licence Ouverte v2.0 (ETALAB)

Version 2.0

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

LES SAUVEGARDES

Dans nos usages personnels ou professionnels, nous utilisons de nombreux appareils numériques pour créer et stocker des informations. Ces appareils peuvent cependant s'endommager ou être endommagés, entraînant une perte, parfois irréversible, de vos données. Afin de prévenir un tel risque, il est fortement conseillé d'en faire des copies pour préserver vos données à long terme. **Voici 10 bonnes pratiques à adopter pour gérer efficacement vos sauvegardes.**

1 EFFECTUEZ DES SAUVEGARDES RÉGULIÈRES DE VOS DONNÉES

En cas de perte, de vol, de panne, de piratage ou de destruction de vos appareils numériques, vous perdrez les données enregistrées sur ces supports. Il peut s'agir de données auxquelles vous accordez une importance particulière ou considérées comme essentielles dans le cadre de vos activités personnelles ou professionnelles (photos, vidéos, documents personnels ou de travail, etc.). Ayez le réflexe de réaliser régulièrement une sauvegarde de vos données.

2 IDENTIFIEZ LES APPAREILS ET SUPPORTS QUI CONTIENNENT DES DONNÉES

Dans notre vie quotidienne, nous utilisons un nombre croissant d'appareils et de supports qui enregistrent et stockent nos fichiers et nos données : ordinateurs, serveurs, tablettes, téléphones mobiles (smartphone), disques durs, clés USB, etc. Prenez le temps de les identifier.

3 DÉTERMINEZ QUELLES DONNÉES DOIVENT ÊTRE SAUVEGARDÉES

Il n'est pas toujours possible ni nécessaire de sauvegarder la totalité de ses données. Sélectionnez donc les données à protéger, notamment celles qui sont stockées sur vos appareils (dans le disque dur de votre ordinateur ou dans la mémoire de votre téléphone mobile). Pour savoir si des données doivent être sauvegardées ou non, posez-vous les questions suivantes : « quelles données ne peuvent pas être récupérées par ailleurs en cas de perte ? », « quelles données je consulte régulièrement ou celles qui me sont le plus souvent demandées ? ».

4 CHOISISSEZ UNE SOLUTION DE SAUVEGARDE ADAPTÉE À VOS BESOINS

Il existe des solutions gratuites ou payantes qui répondent à différents besoins. Identifiez-les et déterminez quelles sont les fonctionnalités attendues, l'espace de stockage requis et la facilité d'utilisation de la solution. Sachez qu'il est également possible de réaliser une sauvegarde manuelle de vos fichiers en les copiant sur un disque dur externe, une clé USB, etc. Enfin, la plupart des systèmes d'exploitation proposent des fonctionnalités de sauvegarde sur le support de votre choix ou sur un service en ligne. Si vous avez des besoins particuliers, renseignez-vous auprès de professionnels ou de sites Internet spécialisés.

5 PLANIFIEZ VOS SAUVEGARDES

Lorsqu'un fichier régulièrement mis à jour est perdu ou supprimé par erreur, sa restauration dans sa version la plus récente est nécessaire. La plupart des solutions de sauvegarde intègrent une fonctionnalité permettant de planifier la sauvegarde à échéance régulière. Vérifiez qu'elle est bien activée et que la fréquence de vos sauvegardes est adaptée à vos besoins. Si vous n'utilisez pas de solution dédiée, réalisez des sauvegardes manuelles régulièrement.

DIFFÉRENTS TYPES DE SAUVEGARDES

- **La sauvegarde complète** est une copie de la totalité de vos données.
- **La sauvegarde incrémentale ou incrémentielle** ne copie que les fichiers qui ont été créés ou modifiés depuis la dernière sauvegarde.
- **La sauvegarde différentielle** est une copie complète des fichiers qui ont été créés ou modifiés depuis la dernière sauvegarde complète.

EN PARTENARIAT AVEC :
MINISTÈRE DE L'INTÉRIEUR
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

ET LE CLOUD, DANS TOUT CELA ?

Des services en ligne, souvent appelés « Cloud », offrent des fonctionnalités de sauvegarde de données. Il existe des solutions gratuites ou payantes en fonction de la capacité de stockage souhaitée. Les fournisseurs d'accès Internet (FAI) et des entreprises spécialisées proposent ce type de service.

6 DÉCONNECTEZ VOTRE SUPPORT DE SAUVEGARDE APRÈS UTILISATION

Si vous êtes victime d'un virus comme un rançongiciel et que votre sauvegarde est connectée à votre ordinateur ou au réseau de votre entreprise, elle peut également être affectée par le programme malveillant qui pourrait la détruire. Déconnectez votre support de sauvegarde de votre ordinateur ou de votre réseau informatique ou mettez-le hors ligne lorsque vous ne l'utilisez plus.

7 PROTÉGEZ VOS SAUVEGARDES

Les risques de perte, de vol, de panne, de piratage ou de destruction peuvent également affecter vos sauvegardes. Protégez-les au même titre que vos données originales en effectuant, par exemple, plusieurs sauvegardes de vos données sur différents supports. Conservez également une sauvegarde dans un lieu différent de celui où sont stockées les données originales pour vous prémunir en cas de sinistre. Si vous estimez que vos données sont suffisamment sensibles pour les chiffrer ou en limiter l'accès, ou si un règlement vous y oblige, faites-en de même avec vos sauvegardes.

8 TESTEZ VOS SAUVEGARDES

Parfois, le processus de sauvegarde ne s'effectue pas correctement. Aussi, assurez-vous régulièrement que votre sauvegarde fonctionne, par exemple, en la copiant dans le système original.

9 VÉRIFIEZ LE SUPPORT DE SAUVEGARDE

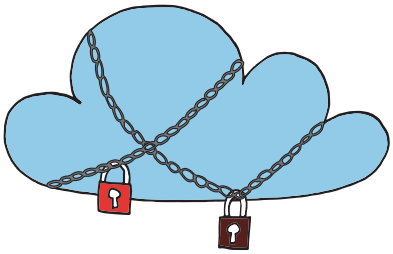
Tout comme les supports qui permettent de stocker les données originales, les supports sur lesquels sont réalisées les sauvegardes peuvent être endommagés. Vérifiez leur état, de manière à prévenir toute défaillance ou panne. Soyez également vigilant sur la durée de vie de votre support car certains conservent les données sur une durée plus ou moins longue. Par exemple, la durée de vie moyenne d'un DVD gravé est de 10 à 15 ans.

10 SAUVEGARDEZ LES LOGICIELS INDISPENSABLES À L'EXPLOITATION DE VOS DONNÉES

Pro

La défaillance d'un appareil entraîne non seulement la perte des données produites par son utilisateur mais également du système d'exploitation de l'appareil comme MS Windows, iOS, Android, et des logiciels qui y sont installés. Si les données sauvegardées sont dépendantes d'un système d'exploitation, d'un logiciel ou d'une configuration particulière, sauvegardez vos données ainsi que celles nécessaires à leur exploitation.

Les systèmes d'exploitation récents proposent des fonctionnalités de sauvegarde du système qui permettent de le restaurer. Reportez-vous à sa documentation pour plus d'information.



LÉGISLATION

Professionnels, associations, collectivités : tenez compte du cadre juridique applicable.

Quelle que que soit leur nature, vos sauvegardes sont soumises à de nombreux régimes juridiques au même titre que vos données originales. S'agissant de données personnelles, votre responsabilité civile ou pénale peut être engagée en cas de manquement avéré. De même, le Règlement Général sur la Protection des Données (**RGPD**) et la Loi Informatique et Libertés sont applicables.

Quelques textes :

- **Loi n° 78-17 du 6 janvier 1978** relative à l'informatique, aux fichiers et aux libertés - Article 34
- **Article 226-17 du Code Pénal** (relatif au traitement et à la protection des données personnelles)
- **Article 1242 du Code Civil** (relatif à la responsabilité civile liée à un dommage causé à autrui)

DOCUMENT RÉALISÉ AVEC NOS MEMBRES :
ATEMPO WOOXO GROUP — CDSE CLUB DES DIRECTEURS DE SÉCURITÉ DES ENTREPRISES — LE GROUPE LA POSTE

Pro = destiné principalement aux professionnels

Licence Ouverte v2.0 (ETALAB)

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

LES MISES À JOUR

Les appareils numériques et les logiciels que nous utilisons au quotidien sont exposés à des failles de sécurité. Ces failles peuvent être utilisées par des cybercriminels pour prendre le contrôle d'un ordinateur, d'un équipement mobile ou encore d'une montre connectée. Face à ces risques, les éditeurs et les fabricants proposent des mises à jour (*patch* en anglais) visant à corriger ces failles. Si l'opération de mise à jour est souvent ressentie comme une contrainte, il s'agit pourtant d'un acte essentiel pour se protéger. **Voici 10 bonnes pratiques à adopter pour vos mises à jour.**

1 PENSEZ À METTRE À JOUR SANS TARDER L'ENSEMBLE DE VOS APPAREILS ET LOGICIELS

Ordinateurs, téléphones, systèmes d'exploitation, logiciels de traitement de texte, objets connectés… nous utilisons un grand nombre d'appareils et de logiciels. Il suffit qu'un seul ne soit pas à jour et soit exposé à une faille de sécurité pour ouvrir une brèche dans votre environnement numérique. Afin d'empêcher les cybercriminels d'utiliser ces failles de sécurité pour vous pirater et vous dérober des informations personnelles sensibles, il est primordial de réaliser les mises à jour de vos équipements dès qu'elles sont disponibles.

2 TÉLÉCHARGEZ LES MISES À JOUR UNIQUEMENT DEPUIS LES SITES OFFICIELS

Seuls les sites ou dispositifs officiels des éditeurs et fabricants vous garantissent au mieux que les mises à jour que vous allez installer ne sont pas infectées par un virus. À l'installation de vos mises à jour, soyez attentif aux éventuelles conditions d'utilisation ou cases pré-cochées qui pourraient valoir acceptation de l'installation d'un autre logiciel non désiré (logiciels publicitaires, par exemple).

3 IDENTIFIEZ L'ENSEMBLE DES APPAREILS ET LOGICIELS UTILISÉS

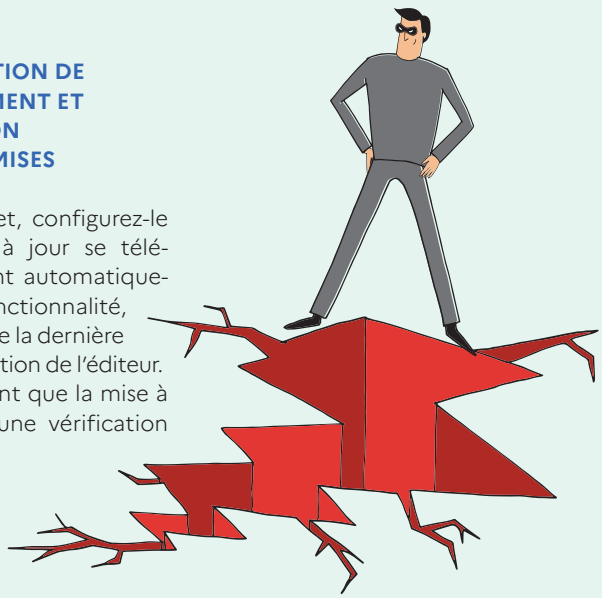
Il est conseillé d'identifier vos appareils, matériels et logiciels afin de les mettre à jour. Certains fournisseurs d'accès Internet (FAI) proposent une application d'inventaire qui permet de lister les appareils connectés à votre réseau informatique professionnel ou domestique. Si vous faites l'acquisition d'un nouvel appareil, remettez ses paramètres par défaut avant de l'utiliser en le réinitialisant et installez ensuite les différentes mises à jour proposées sur les sites du fabriquant ou des éditeurs des applications installées.

4 ACTIVEZ L'OPTION DE TÉLÉCHARGEMENT ET D'INSTALLATION AUTOMATIQUE DES MISES À JOUR

Si le logiciel le permet, configurez-le pour que les mises à jour se téléchargent et s'installent automatiquement. Avec cette fonctionnalité, vous disposerez ainsi de la dernière version à jour de la solution de l'éditeur. Assurez-vous également que la mise à jour fonctionne par une vérification manuelle, au besoin.

DIFFÉRENTS TYPES DE MISES À JOUR

- **Les mises à jour importantes ou critiques** corrigent des failles de sécurité qui peuvent être utilisées pour pirater votre équipement.
- **Les mises à jour de version** apportent en général de nouvelles fonctionnalités et corrigent également des failles de sécurité. Ce type de mise à jour peut être payant.



EN PARTENARIAT AVEC :
MINISTÈRE DE L'INTÉRIEUR
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

QUELQUES EXEMPLES DE FAILLES DE SÉCURITÉ

• **Aux États-Unis,** des cybercriminels ont réussi à dérober des données confidentielles **d'un casino grâce au thermomètre connecté présent dans un aquarium** de l'établissement.
• **En France,** la **trottinette** électrique connaît un succès grandissant. **Une faille de sécurité sur certains modèles** a été découverte. Elle permettait d'exécuter certaines commandes sans avoir besoin du mot de passe comme **les déverrouiller, contrôler l'accélération ou le freinage.** Une mise à jour a été publiée pour corriger cette faille.

5 DÉFINISSEZ LES RÈGLES DE RÉALISATION DES MISES À JOUR Pro

Pour assurer votre sécurité numérique, la définition de certaines règles peut faciliter l'opération de mise à jour, notamment en entreprise. Il s'agit par exemple de spécifier la façon de réaliser l'inventaire des appareils et logiciels utilisés, de savoir où et comment rechercher les mises à jour, comment et qui procède à la mise à jour ou encore à quel moment réaliser cette opération.

6 PLANIFIEZ LES MISES À JOUR LORS DE PÉRIODES D'INACTIVITÉ

Lorsqu'ils interrompent une activité personnelle ou professionnelle (visionnage d'une vidéo, rédaction d'un courriel...), les messages indiquant la disponibilité d'une mise à jour sont souvent ignorés car le processus de mise à jour peut être ressenti comme une contrainte. En effet, la mise à jour peut prendre du temps, allant de quelques secondes à plusieurs minutes ou heures, selon les cas. Aussi, profitez de périodes d'inactivité pour effectuer vos mises (déjeuner, réunion, de nuit...).

7 MÉFIEZ-VOUS DES FAUSSES MISES À JOUR SUR INTERNET

En naviguant sur Internet, il arrive que des messages prenant l'apparence d'alertes de mises à jour apparaissent à l'écran: fausses publicités sur des sites Internet ou fenêtres (*pop-up* en anglais) malveillantes. Restez extrêmement vigilant car il peut s'agir d'une technique pour vous inciter à installer une prétendue mise à jour qui serait en réalité un virus.

8 INFORMEZ-VOUS SUR LA PUBLICATION RÉGULIÈRE DES MISES À JOUR DE L'ÉDITEUR Pro

L'utilisation d'un appareil ou d'un logiciel pas à jour augmente les risques d'attaques informatiques. Si les mises à jour ne sont plus proposées, ils sont plus vulnérables. Aussi, avant l'acquisition d'un nouveau matériel ou logiciel, vérifiez la publication régulière des mises à jour de l'éditeur ou du fabricant, ainsi que la date de fin de leur mise à disposition. Lorsqu'une solution arrive en fin de vie et que des mises à jour ne sont plus proposées, identifiez les délais et les ressources nécessaires pour migrer vers de nouveaux outils afin de rester protégé.

9 TESTEZ LES MISES À JOUR LORSQUE CELA EST POSSIBLE ET FAITES DES SAUVEGARDES Pro

Il arrive que la mise à jour d'un équipement ou d'un logiciel entraîne des conséquences inattendues, comme de rendre incompatible la solution qui vient d'être mise à jour avec un autre équipement ou logiciel. Il convient donc de tester les mises à jour lorsque cela est possible. Par ailleurs, n'hésitez pas à réaliser une sauvegarde de vos données et de vos logiciels avant une opération de mise à jour pour pouvoir revenir en arrière si nécessaire.

10 PROTÉGEZ AUTREMENT LES APPAREILS QUI NE PEUVENT PAS ÊTRE MIS À JOUR Pro

Dans certains cas, des appareils peuvent ne pas être mis à jour pour diverses raisons, comme leur ancienneté, la perte d'une garantie ou d'un agrément. Il est, par conséquent, nécessaire de protéger ce dispositif autrement, par exemple en ne le connectant pas à Internet, en le séparant du reste du réseau informatique ou encore, en désactivant les services vulnérables.

BON À SAVOIR

En entreprise, s'il existe un service informatique, il est généralement chargé de la mise à jour des appareils et des logiciels. **Dans le cas contraire, ce sont les collaborateurs qui effectuent cette opération, sous l'autorité du chef d'entreprise.**

DOCUMENT RÉALISÉ AVEC NOS MEMBRES:

CESIN · CLUSIF · Fédération Française de l'Assurance · paloalto NETWORKS · STORMSHIELD

Pro = destiné principalement aux professionnels

RETROUVEZ TOUTES NOS PUBLICATIONS SUR :
www.cybermalveillance.gouv.fr

Licence Ouverte v2.0 (ETALAB)

Version 2.0

Avant de commencer à jouer

Lors de la transmission des notions théoriques, ou lors de la mise en pratique par le jeu de cartes, il est important de pouvoir rassurer les usagers :

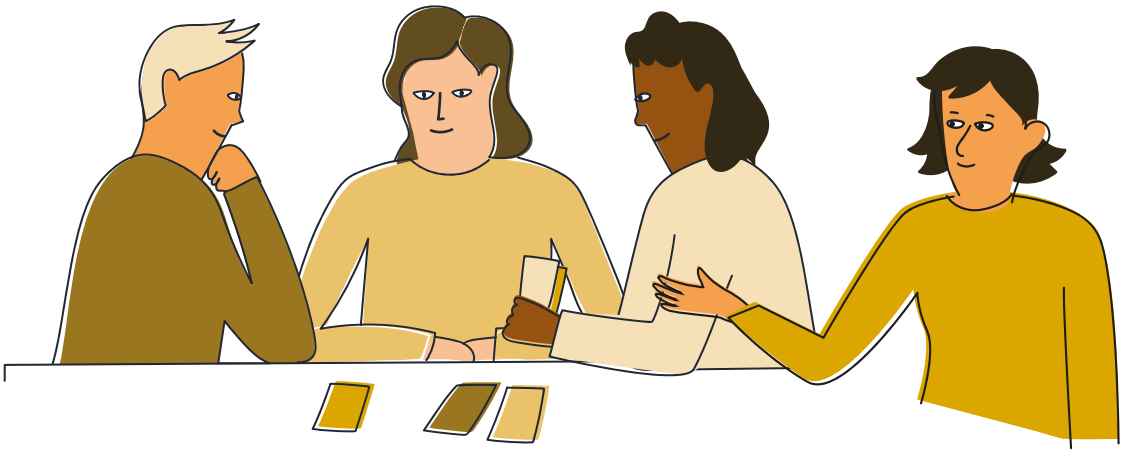
Certaines personnes, notamment les plus éloignées du numérique, ont tendance à systématiquement associer le numérique à la cybermalveillance, au danger et à l'insécurité. Le sujet devient alors anxiogène et empêche les usagers de bénéficier des avantages que peut apporter le numérique.

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

- Rappelez les avantages qu'apporte le numérique (accès à l'information, communication, autonomie…)
- 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 que la plupart des sites Web sont sûrs
- Rassurez-les en leur expliquant que les autorités travaillent à la lutte contre les menaces et que des mesures sont en place pour les protéger

2

Présentation du jeu de cartes



Les règles du jeu

Après avoir partagé les contenus de sensibilisation avec les usagers, 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 usagers, 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.

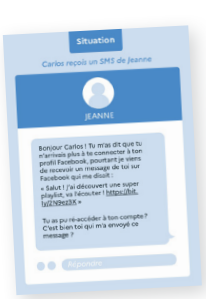
RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

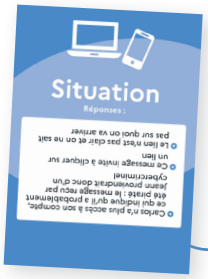
CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

Structure des cartes

Carte Situation

Présente une **situation** dans laquelle une personne est confrontée à une cybermenace





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

Carte Menace

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

Présente chaque menace sous la forme d'une **situation de la vie réelle** et permet aux usagers moins à l'aise avec le numérique de se projeter plus concrètement pour mieux comprendre la menace

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 usagers 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 usagers, ou bien en piocher une au hasard.

2. **Donnez la carte** aux usagers 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 usagers 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 usagers **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 usagers peuvent être **perturbés par l'aspect «virtuel»** des cybermenaces et avoir des difficultés à appréhender ce qu'elles représentent concrètement.

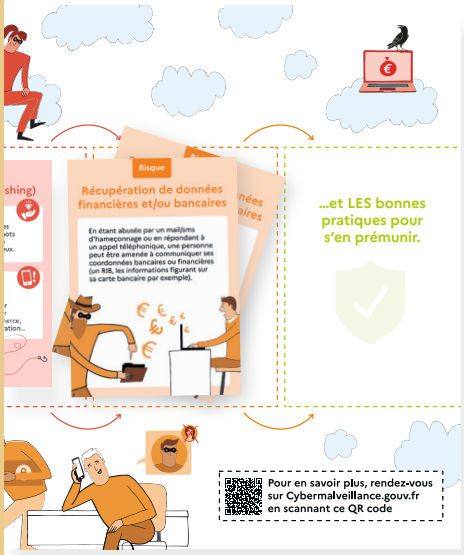
Si c'est le cas durant la partie, invitez-les à **retourner les cartes** pour qu'ils puissent découvrir une situation de la vie réelle qui illustre la cybermenace.

6. Une fois que les usagers ont choisi une carte, **signalez-leur toute confusion éventuelle**. S'ils ont sélectionné **la bonne carte**, invitez-les à la **placer sur la 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 28*

RISQUE

7 Donnez aux usagers 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 usagers ont choisi les cartes, vérifiez leur sélection et **signalez leurs éventuelles erreurs.** Si il y en a, indiquez-leur lesquelles et prenez le temps de leur expliquer.

⟶ *Les réponses sont présentées page 28*

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 usagers le **paquet de cartes Bonne Pratique** et demandez-leur quelles sont celles à retenir pour se prémunir de la menace identifiée.

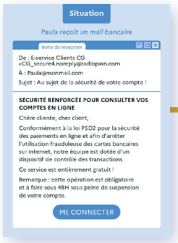
Laissez-leur le temps de sélectionner les cartes de leur choix.

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

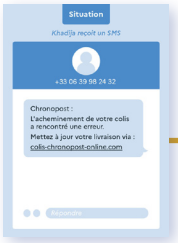
Pour conclure la partie, faites le point avec eux et répondez à leurs éventuelles questions.

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

Solutions



Paula reçoit un mail bancaire

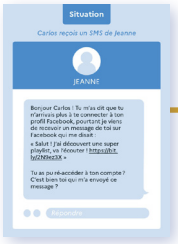


Khadija reçoit un SMS

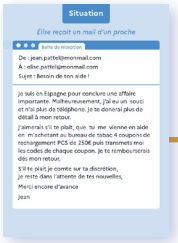
Hameçonnage (Phishing)

Vol de données bancaires

Vol de données d'identité



Carlos reçoit un SMS de Jeanne

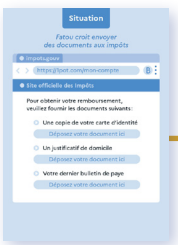


Elise reçoit un mail d'un proche

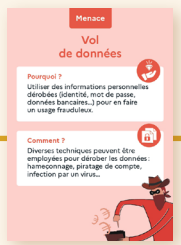
Piratage de compte

Vol de données bancaires

Vol de données d'identité



Fatou croit envoyer des documents aux impôts



Vol de données

Vol de données d'identité

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

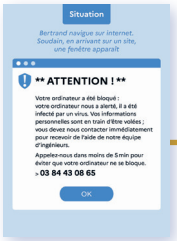
CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

Usurpation d'identité | Escroquerie financière | 1 | 2 | 4 | 5

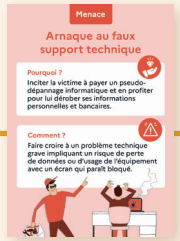
Usurpation d'identité | Perte de données | Escroquerie financière | 2 | 5 | 6 | 11

Usurpation d'identité | Escroquerie financière | 4 | 7 | 8 | 9

Solutions

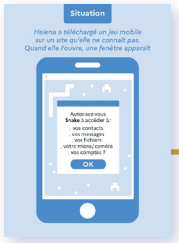


Bertrand navigue sur internet. Soudain, une fenêtre apparaît



Arnaque au faux support technique

Escroquerie financière



Helena a téléchargé un jeu mobile sur un site qu'elle ne connaît pas. Quand elle l'ouvre, une fenêtre apparaît.

Virus informatique

Vol de données bancaires

Vol de données d'identité


Bonne pratique
2
Soyez vigilant avec les liens ou les pièces jointes contenus dans les mails ou SMS qui peuvent infecter votre appareil ou vous mener vers une page de phishing. 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.
Bonne pratique
11
Utilisez un antivirus sur vos appareils (ordinateur, téléphone mobile, tablette). Vérifiez régulièrement qu'il est bien à jour et faites des analyses pour vous assurer que vos appareils ne sont pas infectés.
Bonne pratique
12
Évitez les sites internet non sûrs ou illicites, tels ceux qui hébergent des contrefaçons (musique, films, logiciels...) ou certains sites pornographiques qui peuvent infecter votre appareil avec un virus.
2
11
12


Risque
Perte de données
Suite au piratage d'un compte ou à l'infection d'un appareil par un virus, un cybercriminel peut modifier, supprimer ou rendre illisibles les données de la victime.
Perte de données
Bonne pratique
3
Sauvegardez régulièrement vos données pour pouvoir les retrouver en cas de panne, perte, vol, destruction ou piratage de vos appareils.
Bonne pratique
11
Utilisez un antivirus sur vos appareils (ordinateur, téléphone mobile, tablette). Vérifiez régulièrement qu'il est bien à jour et faites des analyses pour vous assurer que vos appareils ne sont pas infectés.
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.
Bonne pratique
12
Évitez les sites internet non sûrs ou illicites, tels ceux qui hébergent des contrefaçons (musique, films, logiciels...) ou certains sites pornographiques qui peuvent infecter votre appareil avec un virus.
Bonne pratique
13
N'installez pas d'application ou de programme « pirates », ou dont l'origine ou la réputation sont douteuses. Ils pourraient contenir des virus.
3
10
11
12
13

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

PREMIÈRE MINISTRE

MINISTÈRE DE L'ÉCONOMIE, DES FINANCES
ET DE LA SOUVERAINETÉ INDUSTRIELLE ET NUMÉRIQUE

MINISTÈRE DE L'INTÉRIEUR ET DES OUTRE-MER

MINISTÈRE DE LA JUSTICE

MINISTÈRE DES ARMÉES

MINISTÈRE DE L'ÉDUCATION NATIONALE
ET DE LA JEUNESSE

Remerciements

Cette mallette est le fruit de la collaboration entre Cybermalveillance.gouv.fr et l'A.N.C.T.

Nous adressons nos sincères remerciements à l'Association Delta7, à la Médiathèque de Stains et de Saint-Denis, au Cube Garges, au Réseau PIMMS, aux Conseillers numériques France Services, aux Conseiller.ère.s numériques des Villes de Troyes et de Montigny-lès-Cormeilles ainsi qu'au G.I.P. «Vendée Numérique» pour le temps accordé et leurs contributions.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE .GOUV.FR
Assistance et prévention en sécurité numérique

Pour aller plus loin : Cybermalveillance.gouv.fr

Retrouvez la version numérique de la mallette sur notre site

agence nationale de la cohésion des territoires

Financé par
FRANCE RELANCE

Financé par l'Union européenne
NextGenerationEU