

Le magazine du numérique pour la profession



EDITION SPÉCIALE
CONGRÈS 2024



Cybersécurité

Ne relâchez pas votre vigilance
Le commissaire de justice et l'IA

Nos dossiers phares de l'année

Le constat par caméra aérienne
Des visites virtuelles à 360° pour vos constats



Regardons vers le futur et élargissons le champ des possibles

SOMMAIRE

ÉDITO DE MAÎTRE BARET

Plus que jamais dans l'air digital.....03

ARTICLES

La profession investit le monde virtuel04

Notre sélection d'articles à lire sur l'essor des mondes virtuels (metavers), leur évolution et leur rôle de plus en plus prépondérant dans les événements professionnels.

LA CNCJ ouvre le champ des possibles avec l'IA.....06

Évolution de l'intelligence artificielle : historique, précautions d'usage et innovations pour la profession.

D'autres avancées technologiques en perspective pour la profession.....07

Explorez trois avancées majeures pour notre profession : les visites virtuelles à 360°, les constats par drone et les passeports digitaux pour authentifier les objets d'art.

Les engagements de la profession en matière de cybersécurité08

La CNCJ renforce la sensibilisation aux risques numériques et à la cybersécurité à l'occasion de la 12^e édition du Cybermoi/s.

PRÉSENTATION

Sensibilisation aux risques numériques09

CYBERSÉCURITÉ

10 CONSEILS POUR...

Gérer vos mots de passe10

Faire vos sauvegardes12

Deepfake.....14

Mises à jour16

Objets connectés.....18

Sécuriser vos appareils mobiles20

Sécuriser vos usages pro et perso22

Rançongiciels24

Hameçonnage26

GUIDE POUR LES DIRIGEANTS

Que faire en cas de cyberattaque.....28

Consignes aux collaborateurs30

JEUX

Mots croisés.....31

Quiz32



POSTER INCLUS
LES ESSENTIELS DE
VOTRE SÉCURITÉ NUMÉRIQUE



Plus que jamais dans l'air digital ou numérique

Chères Consœurs, Chers Confrères,

Bienvenue dans cette édition spéciale du Cybermag, publiée à l'occasion de notre Congrès 2024 !

Alors que le numérique redessine chaque jour un peu plus notre profession, ce numéro se veut le reflet de notre capacité à adopter les technologies qui transforment notre quotidien. Célébrant sa première année d'existence, le Cybermag poursuit sa mission avec détermination, offrant un éclairage essentiel sur les enjeux numériques qui nous concernent tous.



Maître Olivier BARET

Secrétaire nationale de la Chambre nationale des commissaires de justice
En charge du Pôle numérique

L'ère du digital marque une avancée remarquable pour la profession de Commissaire de justice, accélérée par l'émergence de l'intelligence artificielle. Des outils comme les explorations virtuelles, les drones ou la certification numérique des objets d'art ouvrent de nouvelles perspectives tout en redéfinissant notre façon de travailler. Ces avancées technologiques, aussi prometteuses soient-elles, exigent de nous vigilance et éthique pour préserver l'intégrité de nos interventions.

Notre engagement dans le Cybermoi/s pour la seconde année consécutive illustre notre volonté de protéger les données de nos clients. La CNCJ renforce notre sécurité numérique à travers des tests d'hameçonnage, des recommandations sur la robustesse des mots de passe et des consignes pour gérer nos mises à jour.

La formation continue s'impose comme un pilier fondamental dans notre environnement professionnel en perpétuelle mutation. L'actualisation de nos programmes nous permet d'acquérir des compétences indispensables face aux défis du numérique. Notre engagement envers l'innovation se manifeste par l'intégration de l'IA à notre portail professionnel, la création de salons virtuels dédiés à notre métier, et de nouvelles formations en IA et cybersécurité.

Malgré nos moyens et ressources limités, nous redoublons d'efforts pour vous proposer des solutions digitales de pointe. Ces outils, conçus pour optimiser votre efficacité et votre réactivité, sont le fruit de notre engagement constant. Nous vous invitons vivement à tirer parti de ces progrès techniques afin de maintenir notre profession à l'avant-garde technologique.

Ce numéro spécial offre un mélange équilibré entre rétrospective et innovation. Vous y retrouverez des liens vers les articles clés de l'année, mais aussi des nouveautés exclusives : une bande dessinée ludique sur la cybersécurité, un guide pratique pour les études, et des jeux interactifs pour tester vos connaissances de manière engageante.

En intégrant ces nouvelles technologies, rappelons que notre véritable valeur réside dans notre expertise juridique, notre éthique, et notre dimension humaine. Comme l'a si bien dit Édouard Glissant, écrivain et penseur martiniquais : « Agis en ton lieu, pense avec le monde ». Je vous invite à explorer ce numéro avec curiosité et à partager vos réflexions. Ensemble, façonnons l'avenir numérique de notre profession.

Bonne lecture !

La profession investit le monde virtuel

Dans un monde en perpétuelle évolution, le web 3D immersif, alimenté par la réalité virtuelle (VR) et l'intelligence artificielle (IA), reconfigure notre interaction avec le numérique. Voici une sélection d'articles à lire sur l'essor des mondes virtuels (metavers), leur évolution et leur rôle de plus en plus prépondérant dans les événements professionnels, en témoigne l'organisation du premier salon virtuel dédié à la profession de commissaire de justice.

L'émergence du web 3D immersif propulsé par la VR et à l'IA

La réalité virtuelle (VR) et l'intelligence artificielle (IA) ont transformé le Web en une expérience immersive en 3D. Ces deux technologies, soutenues par le Cloud Computing, la 5G et le traitement du langage naturel, permettent de créer des mondes virtuels dynamiques et interactifs. Cette évolution offre des opportunités incroyables dans divers domaines, notamment la formation, la médiation et le recrutement.

Le métavers et les mondes virtuels, souvent confondus, désignent des environnements 3D où les utilisateurs interagissent en temps réel.

Cette convergence technologique transforme non seulement notre utilisation du Web, mais aussi la manière dont nous percevons la réalité.



LIRE PLUS

Article complet rédigé par Laurent Chrétien, fondateur et président-directeur général de la société KOMODAL, créateur de l'espace virtuel de la CNCJ : Espace virtuel – *Cybermag*

Aujourd'hui, la réalité virtuelle (VR) enrichit ces expériences via des plateformes comme VRChat. Ces environnements sont utilisés dans divers secteurs, y compris l'éducation, comme le montre le salon professionnel virtuel organisé par la Chambre nationale des commissaires de justice sur Teemew, qui a permis à des étudiants en droit de découvrir la profession à distance



LIRE PLUS

Naissance et histoire des mondes virtuels
Point d'histoire

Naissance et histoire des mondes virtuels

Les mondes virtuels, ou « métavers », sont des environnements numériques immersifs favorisant l'interaction sociale. Leur évolution a débuté dans les années 1970 avec des jeux textuels (jeux basés uniquement sur du texte), suivis des MUDs (Multi-User Dungeons) dans les années 1980, et des mondes en 3D dans les années 1990, comme Habitat et Ultima Online. Les années 2000 ont vu l'apogée des mondes virtuels avec Second Life et World of Warcraft, attirant des millions de joueurs.

en partenariat avec



BANQUE des
TERRITOIRES



Lancement du premier salon virtuel consacré à la profession de commissaire de justice

Le 6 mai 2024, la CNCJ a organisé un salon virtuel, permettant à plus de 65 étudiants en droit de l'Université de Laval de découvrir la profession de commissaire de justice. Les participants ont pu explorer les divers aspects des activités de la profession, échanger avec des commissaires de justice afin de mieux connaître leur motivation dans l'exercice de leur fonction.

L'événement a été bien accueilli pour son interactivité et son aspect ludique. Il a permis à la profession de valoriser un nouveau concept adapté aux attentes de la nouvelle génération, laquelle a particulièrement apprécié le parcours libre, l'accès facilité à l'information, la qualité des échanges et la disponibilité des intervenants, ainsi que l'exhaustivité des contenus présentés. En effet, avant de proposer cet événement, Maître Baret a rencontré les étudiants concernés, environ 1% d'entre eux ont répondu connaître la profession et s'y intéresser.

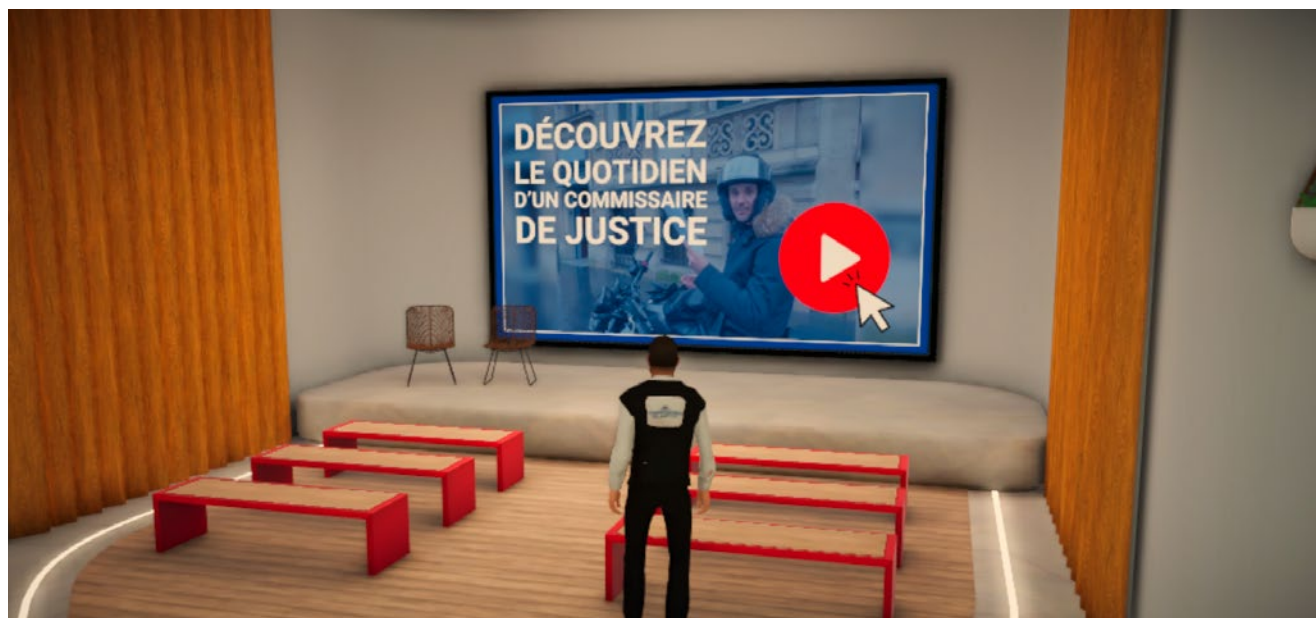
Après l'événement, ces mêmes étudiants ont été à nouveau interrogés, 96% d'entre eux déclaraient avoir été parfaitement informés, dont 30% affirmaient être intéressés pour rejoindre la profession comme commissaire de justice ou collaborateur.

Les perspectives d'utilisation pour 2025 visent le renouvellement de la profession en permettant à tous les étudiants des facultés de droit d'accéder à cet espace virtuel, afin qu'ils puissent appréhender les métiers proposés par la profession.



LIRE PLUS

Lancement du premier salon virtuel consacré à la profession de commissaire de justice – Cybermag



La profession ouvre le champ des possibles avec l'IA

Bien que l'intelligence artificielle (IA) monopolise l'attention de tous depuis trois ans, en réalité, les premières pierres ont été posées au milieu du XXe siècle.

L'intelligence artificielle, née en 1956 lors d'une conférence au Dartmouth College, a cheminé depuis les mythes antiques jusqu'aux concepts modernes. Des automates de la Grèce antique aux idées révolutionnaires de René Descartes et aux inventions de Charles Babbage et Ada Lovelace, l'IA a évolué à travers les âges. L'introduction du terme « robot » par Karel Čapek en 1920 dans sa pièce R.U.R. et les réflexions sociales et éthiques dans le roman Metropolis illustrent cette évolution.

Aujourd'hui, boostée par les avancées en informatique et l'accès massif aux données, l'IA transforme notre quotidien dans divers domaines tels que la santé,

les finances et les transports. La CNCJ intègre désormais cette technologie dans son portail professionnel, permettant une recherche efficace des publications et ouvrant la voie à un apprentissage continu et collaboratif de cette entité artificielle.

L'IA a depuis parcouru un long chemin, évoluant vers des technologies qui aujourd'hui transforment nos vies. La profession ne pouvait pas rester en marge de ces avancées majeures qui changent profondément la société. Elle travaille donc sur différentes voies d'utilisation de l'IA. L'une d'entre elles, a été durant l'année 2024, de proposer un moteur de recherche intelligent intégré au portail professionnel. Cette expérience démontre

que l'investissement nécessaire est bien plus important, que la simple intégration de l'IA. En effet, posséder de l'information en grande quantité, s'est avéré insuffisant pour proposer un outil de qualité. Il est essentiel d'éduquer cette nouvelle technologie afin qu'elle puisse répondre aux objectifs fixés, c'est un travail de longue haleine.

D'après les dernières statistiques d'utilisation, les recherches se concentrent principalement sur des sujets juridiques, professionnels et les outils numériques. Ces données d'utilisation sont analysées régulièrement pour mieux répondre à vos besoins et ainsi optimiser votre expérience sur le portail.

ARTICLES PUBLIÉS DANS LE CYBERMAG TOUT AU LONG DE CETTE ANNÉE



L'intelligence artificielle :
de la science-fiction
à la réalité
- Cybermag



L'intelligence artificielle
intégrée à votre portail
professionnel
- Cybermag



Intelligence artificielle
- Cybermag

Précautions à prendre dans l'utilisation de l'IA relativement à la protection des données personnelles et au secret des affaires

L'intelligence artificielle (IA) est essentielle dans de nombreux secteurs, apportant des avantages en productivité et innovation, mais elle présente également des risques pour la protection des données personnelles et le secret des affaires. Il est crucial de prendre des précautions pour sécuriser les informations sensibles. Avant de soumettre des données à une IA, il est recommandé d'anonymiser ou pseudonymiser les informations, de connaître la réglementation (comme

le RGPD), et de minimiser les données transmises. De plus, il est important de ne pas compromettre le secret des affaires. L'IA offre d'énormes opportunités, mais son utilisation doit être responsable et éthique.



LIRE PLUS

Précautions à prendre
dans l'utilisation de l'IA



D'autres avancées technologiques pour la profession

Dans un monde en constante évolution, les innovations technologiques jouent un rôle crucial pour améliorer l'efficacité et la précision des constats pour les commissaires de justice. Nous vous proposons d'explorer trois avancées majeures révolutionnaires pour notre profession : l'utilisation des visites virtuelles à 360°, des drones pour les constats aériens et des passeports digitaux pour authentifier les objets d'art.

Des visites virtuelles à 360° pour enrichir et simplifier vos constats

Les nouvelles technologies, telles que les visites virtuelles à 360°, révolutionnent les pratiques de constat des commissaires de justice, offrant une précision accrue, un gain de temps et une communication fluide. Ces outils permettent de documenter de manière immersive et détaillée l'état d'un lieu, capturant l'intégralité de l'environnement en qualité 4K, ce qui est particulièrement utile pour les constats d'état des lieux, de sinistres, de voirie, de violations de propriété et de non-respect des normes de sécurité.

Grâce à un équipement accessible et facile à utiliser, les commissaires de justice peuvent réaliser des images sphériques en quelques secondes et partager les visites virtuelles protégées par mot de passe. Cette technologie rend les constats plus efficaces et les preuves plus irréfutables, enrichissant ainsi les rapports avec des détails visuels et informatifs supplémentaires.



LIRE PLUS

Des visites virtuelles à 360° pour enrichir et simplifier vos constats
– Cybermag

Le constat par caméra aérienne (ou « drone »)

L'utilisation des drones par les commissaires de justice représente une avancée significative dans la modernisation des pratiques juridiques, bien que leur emploi soulève des défis juridiques complexes. Le cadre législatif actuel pour les drones nécessite une compréhension approfondie des règles aéronautiques et une formation rigoureuse, notamment en raison de l'évolution rapide des réglementations. Les drones doivent être utilisés avec précaution pour respecter les lois sur la vie privée et obtenir les autorisations nécessaires, surtout dans les zones sensibles telles que les aéroports et les rassemblements de personnes.



Le constat par drone permet aux commissaires de justice d'améliorer la qualité et la précision de leurs constats grâce à la technologie de pointe. Cependant, il est crucial pour eux de bien maîtriser les aspects techniques et juridiques liés à l'utilisation de ces appareils. Des formations spécialisées et

le respect des réglementations sont essentiels pour garantir la légalité et l'efficacité des constats réalisés par drone. En somme, bien que prometteurs, les drones exigent une gestion rigoureuse et une expertise spécifique pour être pleinement intégrés dans le domaine juridique.

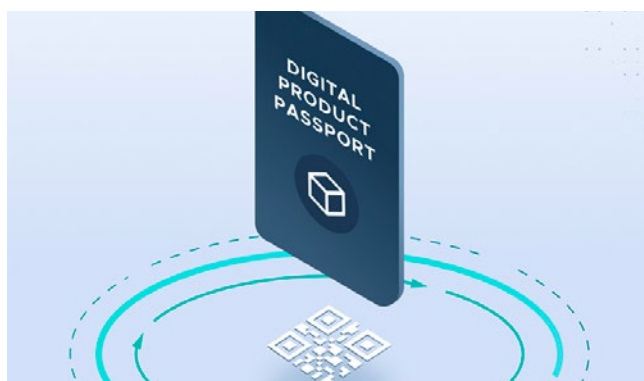


LIRE PLUS

Le constat par caméra aérienne (ou « drone »)
– Cybermag

Passeport digital et objets d'art

Le 6 mai 2024, la CNCJ a organisé un salon virtuel, permettant à plus de 65 étudiants en droit de l'Université de Laval de découvrir la profession de commissaire de justice. Les participants ont pu explorer les divers aspects des activités de la profession, échanger avec des commissaires de justice afin de mieux connaître leur motivation dans l'exercice de leur fonction.



L'événement a été bien accueilli pour son interactivité et son aspect ludique. Il a permis à la profession de valoriser un nouveau concept adapté aux attentes de la nouvelle génération, laquelle a particulièrement apprécié le parcours libre, l'accès facilité à l'information, la qualité des échanges et la disponibilité des intervenants, ainsi que l'exhaustivité des contenus présentés. En effet, avant de proposer cet événement, Maître Baret a rencontré les étudiants concernés, environ 1% d'entre eux ont répondu connaître la profession et s'y intéresser.

Après l'événement, ces mêmes étudiants ont été à nouveau interrogés, 96% d'entre eux déclaraient avoir été parfaitement informés, dont 30% affirmaient être intéressés pour rejoindre la profession comme commissaire de justice ou collaborateur.

Les perspectives d'utilisation pour 2025 visent le renouvellement de la profession en permettant à tous les étudiants des facultés de droit d'accéder à cet espace virtuel, afin qu'ils puissent appréhender les métiers proposés par la profession.



LIRE PLUS

Lancement du premier salon virtuel consacré à la profession de commissaire de justice – Cybermag



Les engagements de la profession en matière de cybersécurité

12^{ème} édition du Cybermoi/s pour sensibiliser aux risques numériques

12^{ème} édition du Cybermoi/s pour sensibiliser aux risques numériques

Pour la deuxième année consécutive, la Chambre nationale des commissaires de justice a participé au Cybermoi/s, le mois de la sensibilisation aux risques numériques. La 12^e édition de cet événement européen s'est déroulée tout au long du mois d'octobre 2024, sous l'égide de l'ENISA. Les particuliers, entreprises, administrations, collectivités et associations ont été encouragés à adopter les bonnes pratiques pour se protéger en ligne. Plusieurs actions telles que des ateliers, conférences, webinaires et autres initiatives ont été organisées pour former et accompagner les citoyens et les entreprises. Le coup d'envoi officiel a été donné à l'Assemblée nationale le 1^{er} octobre.

Dans le cadre de cet événement, la CNCJ a partagé des publications sur les réseaux sociaux avec le hashtag #CyberEngagés. Elle a également organisé une campagne de communication par newsletters hebdomadaires pendant tout le cybermoi/s pour rappeler les bonnes pratiques et les actions à effectuer en cas d'attaque. De plus, le service informatique de la CNCJ a réalisé deux tests de phishing sur les messageries afin de préparer la profession aux menaces numériques et promouvoir les meilleures pratiques de sécurité informatique.

En participant au Cybermoi/s, la Chambre nationale des commissaires de justice réaffirme son engagement pour la

cybersécurité. Par ses actions de formation et de prévention, la CNCJ souhaite renforcer la résilience de la profession et sensibiliser aux enjeux essentiels de la sécurité numérique.

Renforcement de la sensibilisation à la cybersécurité

La CNCJ renforce sa politique de sensibilisation à la cybersécurité en intégrant des publications régulières sur le portail professionnel et en menant des campagnes de communication intensives, notamment l'envoi de newsletters : l'une au cours du premier semestre et l'autre pendant le Cybermoi/s au second semestre. Des processus d'alerte ont également été mis en place pour permettre des réactions rapides.

Pour vous aider à mieux identifier les tentatives d'hameçonnage, la CNCJ réalise régulièrement des tests de phishing. Les résultats encourageants témoignent des efforts de la CNCJ et de votre engagement. Nous vous rappelons que la protection contre les cybermenaces est l'affaire de tous. La mobilisation de chacun profitera à l'ensemble de la communauté et renforcera notre sécurité collective, nous rapprochant ainsi d'une véritable cyber-résilience.

SENSIBILISATION AUX RISQUES NUMÉRIQUES

À l'ère du numérique, la cybersécurité est un enjeu crucial pour tous. Les cybermenaces touchent aussi bien les individus que les entreprises, et leur impact ne cesse de croître avec la digitalisation de notre société. Usurpation d'identité, vol de données personnelles, tentatives de phishing ou logiciels malveillants : les risques se multiplient.

Pour contrer ces menaces, des initiatives telles que Cybermalveillance.gouv.fr ont été instaurées. Lancé en 2017, Cybermalveillance.gouv.fr assiste les victimes de cybermalveillance et sensibilise aux risques des attaques en ligne. Dans cette optique, la Chambre nationale des commissaires de justice s'engage à informer, sensibiliser et protéger ses membres contre les dangers numériques.

À travers ces pages, découvrez comment éviter les tentatives de phishing, vous protéger contre les logiciels malveillants et adopter des mots de passe robustes. Chaque geste compte pour renforcer la sécurité de vos informations personnelles et professionnelles. En prenant conscience des risques et en adoptant des pratiques simples mais efficaces, vous devenez acteur de votre propre sécurité numérique.

Ensemble, contribuons à un environnement numérique plus sûr pour tous.

A PROPOS DE CYBERMALVEILLANCE.GOUV.FR

Cybermalveillance.gouv.fr est le dispositif national d'assistance aux victimes de cybermalveillance. Ce dispositif a été incubé par l'Agence nationale de sécurité des systèmes d'information (ANSSI) en copilotage avec le ministère de l'Intérieur et le soutien des ministères de l'Économie et des Finances, de la Justice et du secrétariat d'État chargé du Numérique. Il est désormais piloté par le Groupement d'Intérêt Public ACYMA.

Retrouvez toutes les publications de Cybermalveillance.gouv sur le site Internet : www.cybermalveillance.gouv.fr

Un e-mail malveillant :
www.signal-spam.fr



Un SMS malveillant :
www.33700.fr



Un contenu illicite :
www.internet-signalement.gouv.fr

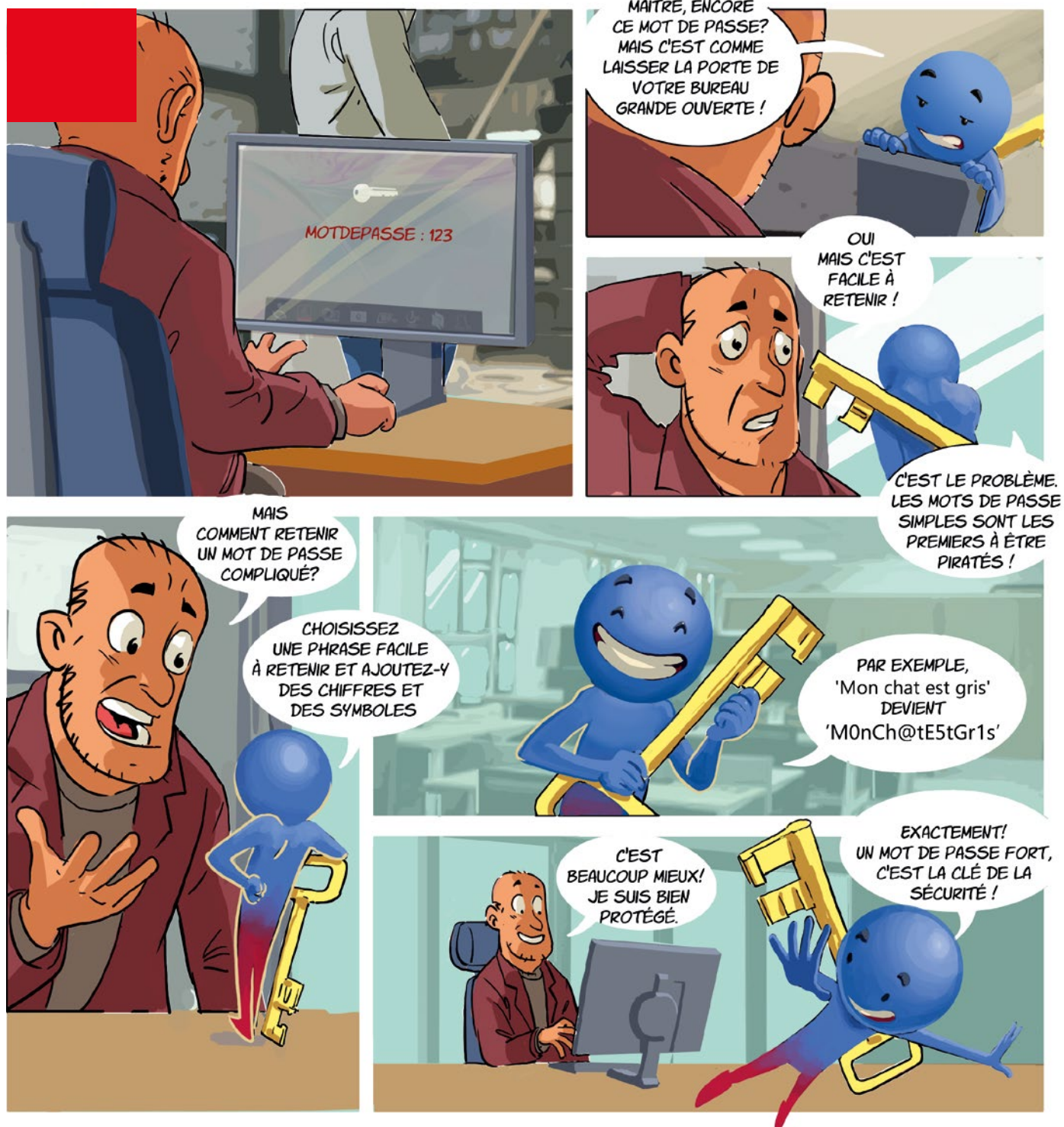
Besoin d'assistance si vous êtes victime ?
www.cybermalveillance.gouv.fr



Une question sur vos données personnelles ?
www.cnil.fr/fr/cnil-direct



Dans tous les cas, veuillez signaler à la CNCJ toute suspicion ou attaque avérée à : digitalalerte@cncj.fr.



CONSEILS PRATIQUES

Utilisez des phrases faciles à retenir issues de vos chansons préférées ou de poèmes, mais avec des caractères aléatoires insérés. Si vous aimez la chanson «Je te promets» de Johnny Hallyday et son texte «Je te promets le sel au baiser de ma bouche», vous pourriez le transformer en mot de passe ainsi : `**J3_t3_pR0m&t$L3$el_Ba!ser#2m@b0uche**`

- Gardez la structure de la phrase avec des underscores (` \_ `).
- Remplacez des lettres par des chiffres ou symboles (` e ` → ` 3 ` , ` o ` → ` 0 ` , ` s ` → ` \$ `).
- Ajoutez des majuscules pour renforcer la sécurité.

RESSOURCES

Pourquoi et comment bien gérer ses mots de passe ?



Renforcez vos mots de passe





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 mot 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





CONSEILS PRATIQUES

Appliquez la règle du 3-2-1 : gardez trois copies de vos données sur deux supports différents (ex. : disque dur externe et cloud), avec une copie en dehors de votre lieu principal (en cas de sinistre). Pensez à utiliser des supports physiques, comme des clés USB cryptées, que vous stockez dans un endroit sûr (ex : un coffre sécurisé chez vous, une boîte en fer en bas d'une armoire...). Cela ajoute une couche de sécurité physique, permettant de restaurer facilement vos données en cas de cyberattaque ou de panne.

RESSOURCES

Pourquoi et comment bien gérer ses sauvegardes ?



Comment protéger ses données numériques grâce aux sauvegardes ?





10 CONSEILS POUR FAIRE VOS SAUVEGARDES

1

Effectuez des sauvegardes régulières de vos données



2

Identifiez les appareils et supports qui contiennent des données



3

Déterminez quelles données doivent être sauvegardées



4

Choisissez une solution de sauvegarde adaptée à vos besoins



5

Planifiez vos sauvegardes



6

Déconnectez votre support de sauvegarde après utilisation



7

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



8

Testez vos sauvegardes



9

Vérifiez le support de sauvegarde



10
Pro

Sauvegardez les logiciels indispensables à l'exploitation de vos données





CONSEILS PRATIQUES

L'augmentation spectaculaire des deepfakes diminue la confiance dans les ressources en ligne. Apprenez à les détecter. Repérez les clignements anormaux des yeux, les ombres étranges, les lèvres décalées, les détails flous pour analyser les vidéos suspectes.

RESSOURCES

L'intelligence artificielle (IA), entre menaces et opportunités



Que faire en cas de fraude au faux conseiller bancaire ?





DEEPPFAKE

10 CONSEILS POUR VOTRE SÉCURITÉ

- 1 Vérifiez la source des vidéos 
- 2 Méfiez-vous des contenus trop invraisemblables 
- 3 Analysez les détails visuels 
- 4 Écoutez attentivement le son 
- 5 Assurez-vous de l'identité réelle de votre interlocuteur 
- 6 Faites attention aux vidéos virales 
- 7 Protégez vos propres images et vidéos 
- 8 Tenez-vous informé des nouvelles techniques de deepfake 
- 9 Privilégiez les sources d'information vérifiées 
- 10 Dénoncez les deepfakes 





CONSEILS PRATIQUES

Activez les mises à jour automatiques dans les paramètres de vos logiciels afin de garantir que vous disposez toujours des correctifs de sécurité les plus récents. Windows, macOS, et Android proposent des notifications pour les nouvelles mises à jour. Assurez-vous également que les notifications de mises à jour sont activées dans les paramètres de vos logiciels.

RESSOURCES

Pourquoi et comment bien gérer ses mises à jour ?





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

Pro

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

Pro

5

Définissez les règles de réalisation des mises à jour



10

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

Pro





CONSEILS PRATIQUES

Pour protéger vos objets connectés, désactivez le Wi-Fi et le Bluetooth quand ils ne sont pas utilisés pour réduire les risques d'accès non autorisé. Changez aussi régulièrement le mot de passe du routeur Wi-Fi en choisissant un mot de passe complexe pour sécuriser votre réseau.

RESSOURCES

La sécurité des objets connectés (IoT)





10 CONSEILS POUR SÉCURISER VOS OBJETS CONNECTÉS

1

Avant l'achat, renseignez-vous sur la sécurité de l'objet connecté



6

Éteignez vos objets lorsque vous ne les utilisez pas



2

Modifiez les mots de passes par défaut



7

Mettez à jour les appareils raccordés à vos objets connectés



3

Mettez à jour sans tarder vos objets connectés et leurs applications



8

Sécurisez votre connexion Wi-fi



4

Protégez vos informations personnelles



9

Limitez l'accès de vos objets connectés aux autres appareils



5

Contrôlez les paramètres de sécurité de vos objets et de leurs applications



10

Supprimez vos données et réinitialisez votre objet lorsque vous ne vous en servez plus





CONSEILS PRATIQUES

Protégez vos appareils mobiles en activant « Localiser mon iPhone » pour iOS ou « Trouver mon appareil » pour Android. Cela vous permet de localiser, verrouiller ou effacer votre appareil à distance en cas de perte ou de vol.

RESSOURCES

Protéger ses appareils mobiles





10 CONSEILS POUR SÉCURISER VOS APPAREILS MOBILES

1

Mettez en place les codes d'accès



6

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



2

Chiffrez les données de l'appareil



7

Contrôlez les autorisations de vos applications



3

Appliquez les mises à jour de sécurité



8

Ne laissez pas votre appareil sans surveillance



4

Faites des sauvegardes



9

Évitez les réseaux Wi-Fi publics ou inconnus



5

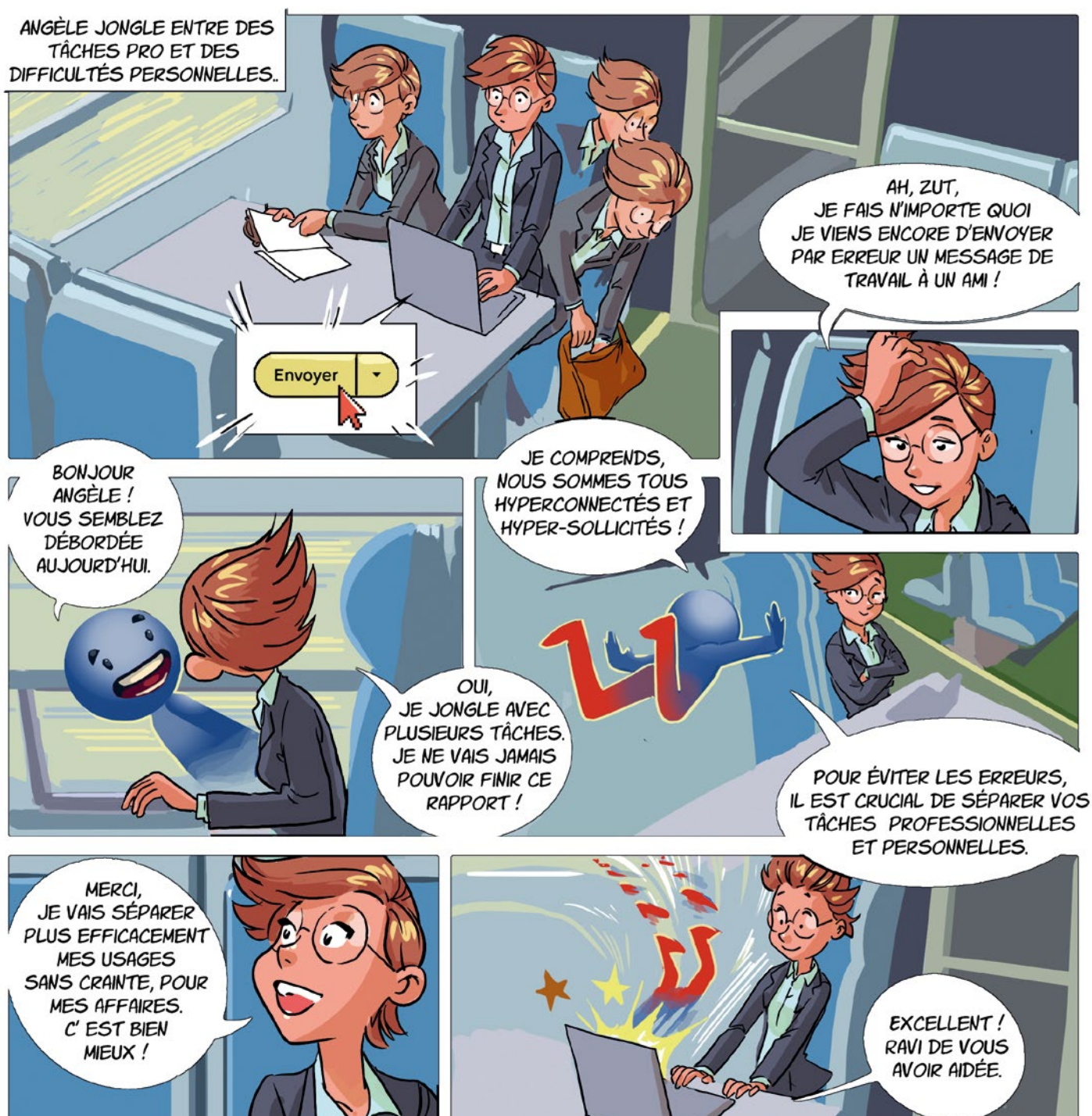
Utilisez une solution de sécurité contre les virus et autres attaques



10

Ne stockez pas d'informations confidentielles sans protection





CONSEILS PRATIQUES

Séparez vos usages professionnels et personnels en créant des comptes utilisateurs distincts sur votre appareil. Utilisez un compte pour le travail et un autre pour vos affaires personnelles. Certains smartphones offrent également des modes de profil (comme le mode travail) pour différencier les applications et notifications.

RESSOURCES

Apprendre à séparer ses usages pro-perso





10 CONSEILS POUR SÉCURISER VOS USAGES PRO ET PERSO

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





CONSEILS PRATIQUES

La restauration à partir de sauvegardes est souvent la seule solution contre les rançongiciels. Vérifiez régulièrement vos sauvegardes et testez leur restauration pour garantir leur fonctionnement rapide. Si nécessaire, demandez à votre prestataire informatique d'inclure ces tests dans ses services.

RESSOURCES

Rançongiciel ou ransomware, que faire ?





CYBERCRIMINEL



EXTORSION D'ARGENT

Vous ne pouvez plus accéder à vos fichiers et on vous demande une rançon ? Vous êtes victime d'une attaque par rançongiciel (*ransomware*, en anglais) !

BUT

Réclamer le paiement d'une rançon pour rendre l'accès aux fichiers verrouillés.

TECHNIQUE

Blocage de l'accès à des données par envoi d'un message contenant des liens ou pièces jointes malveillantes ou par intrusion sur le système.



VICTIME



COMMENT RÉAGIR ?

- Débranchez la machine d'Internet et du réseau local
- En entreprise, alertez le support informatique
- Ne payez pas la rançon
- Déposez plainte
- Identifiez et corrigez l'origine de l'infection
- Essayez de désinfecter le système et de déchiffrer les fichiers
- Réinstallez le système et restaurez les données
- Faites-vous assister par des professionnels



CONSEILS PRATIQUES

Vérifiez que votre messagerie bénéficie d'un filtre anti-spam, cela permet de réduire les risques d'hameçonnage. Pour les autres critères d'identification d'une tentative d'hameçonnage, nous pouvons vous conseiller la vigilance pour identifier les mails frauduleux (vérifier le nom, la conformité de l'adresse mail, la mise en page, les fautes d'orthographe). Dans tous les cas, même si le message est légitime, évitez autant que possible de transmettre des informations personnelles ou sensibles (coordonnées bancaires, copies de pièces d'identité).

RESSOURCES

Procédure pour protéger sa messagerie avec SpamTitan



Que faire en cas de phishing ou hameçonnage ?





L'HAMEÇONNAGE

CYBERCRIMINEL



VOL DE DONNÉES

Vous recevez un message ou un appel inattendu, voire alarmant, d'une organisation connue et d'apparence officielle qui vous demande des informations personnelles ou bancaires? Vous êtes peut-être victime d'une attaque par hameçonnage (phishing en anglais)!

BUT

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

TECHNIQUE

Leurre envoyé via un faux message, SMS ou appel téléphonique d'administrations, de banques, d'opérateurs, de réseaux sociaux, de sites d'e-commerce...



VICTIME



COMMENT RÉAGIR?

- Ne communiquez jamais d'information sensible suite à un message ou un appel téléphonique
- Au moindre doute, contactez directement l'organisme concerné pour confirmer
- Faites opposition immédiatement (en cas d'arnaque bancaire)
- Changez vos mots de passe divulgués/compromis
- Déposez plainte
- Signalez-le sur les sites spécialisés (voir ci-dessous)

LIENS UTILES

[Signal-spam.fr](https://www.signal-spam.fr)

[Phishing-initiative.fr](https://www.phishing-initiative.fr)

[Info Escroqueries](https://www.info-escroqueries.fr)
0805 805 817 (gratuit)

Pour en savoir plus ou vous faire assister, rendez-vous sur [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr)



QUE FAIRE EN CAS DE CYBERATTAQUE ? (dirigeants)

1 PREMIERS RÉFLEXES



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.



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



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...

**NE PAYEZ PAS
DE RANÇON!**

Par des prestataires spécialisés en cybersécurité que vous pourrez trouver sur 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 à 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.

Cette fiche provient de Cybermalveillance.gouv.fr et a été personnalisée selon les processus de la CNCJ.



CONTACTS UTILES



Conseils et assistance

Dispositif national de prévention et d'assistance
aux victimes de cybermalveillance
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

Police – gendarmerie : 17

CNCJ : digitalalerte@cncj.fr

Assureur Fidélia / CNCJ

Numéro vert 01 47 11 70 29, préciser le N° de contrat 144 195 098
et le N° de protocole 100.381 (contrat Cyber Risques de la CNCJ).

Votre support informatique

Raison sociale

Référent

Téléphone

CONSIGNES EN CAS DE CYBERATTAQUE

1 

**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.*

2 

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.*

3 

**ALERTEZ AU PLUS VITE
VOTRE SUPPORT INFORMATIQUE**

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

4 

**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.*

5 

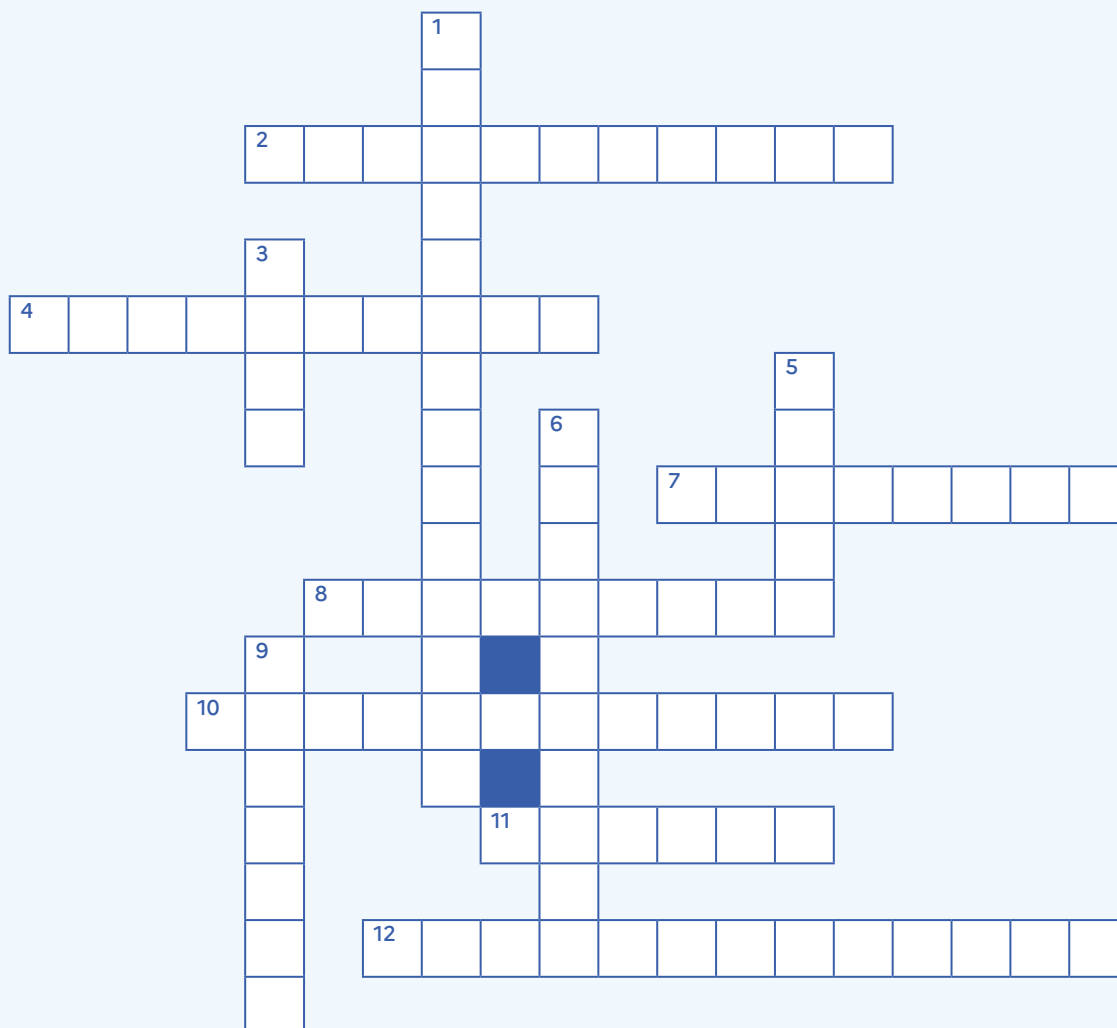
**PRÉVEENEZ VOS COLLÈGUES
DE L'ATTAQUE EN COURS**

*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

GRILLE DE MOTS CROISÉS



Horizontalement

2. Technique pour voler des informations en se faisant passer pour une institution ou une personne légitime.

4. Technique utilisée pour tromper quelqu'un en se faisant passer pour un autre afin d'obtenir des informations confidentielles.

7. Accès non autorisé à un système informatique dans le but de voler ou d'endommager des données.

8. Outil utilisé pour protéger un appareil contre les programmes malveillants.

10. Attaque qui bloque l'accès aux fichiers et demande une rançon pour les restaurer.

11. Action malveillante visant à obtenir des fonds ou des informations par tromperie.

12. Pratiques pour se défendre contre les menaces sur Internet.

Verticalement

1. Processus permettant de vérifier l'identité d'un utilisateur sur un appareil ou un service.

3. Envoi massifs de courriels non sollicités, souvent à caractère publicitaire ou frauduleux.

5. Programme malveillant qui se propage via des emails ou des fichiers infectés.

6. Action qui permet de conserver des copies de ses données pour éviter leur perte.

9. Terme général anglais pour désigner les logiciels malveillants.

Pour voir les solutions, flashez ce QR Code !



TESTEZ VOS CONNAISSANCES

GÉRER SES MOTS DE PASSE



1/ Bonnes pratiques

Parmi les propositions, quelles sont les deux bonnes pratiques à mettre en œuvre pour assurer la sécurité de vos mots de passe ?

- ☐ A Les noter sur un post-it pour s'en souvenir
- ☐ B Choisir un mot de passe suffisamment complexe
- ☐ C Les confier à un tiers en cas de besoin
- ☐ D Utiliser un mot de passe différent pour chaque accès

2/ Vrai ou Faux

J'ai un mot de passe très sécurisé. Je peux donc l'utiliser sur tous mes comptes et services.

- ☐ Vrai ☐ Faux

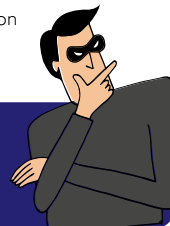
3/ Cherchez l'intrus

Un mot de passe sécurisé :

- ☐ A est facile (suite logique, le prénom de mes enfants, ma date de naissance, etc.)
- ☐ B comporte 12 caractères mélangeant des majuscules, des minuscules, des chiffres et des caractères spéciaux
- ☐ C suit un moyen mnémotechnique

4/ Reliez les situations à leurs solutions

- | | | |
|--|----------------------------|--|
| Je ne me souviens jamais de mes mots de passe | A ☐ | 1 Je n'enregistre pas les mots de passe et me déconnecte après utilisation |
| Je soupçonne qu'un de mes comptes ait été piraté | B ☐ | 2 Je fais confiance à Keepass, mon gestionnaire de mots de passe |
| Je travaille sur un ordinateur à la bibliothèque | C ☐ | 3 Je change immédiatement de mot de passe |



RÉPONSES

1/B et D – Vos mots de passe sont la porte d'entrée de vos appareils numériques et de l'accès à vos comptes, qui peuvent contenir des données sensibles. Protégez vos accès en utilisant un mot de passe complexe et unique pour chaque accès.

2/FAUX – Il vaut mieux utiliser un mot de passe différent et complexe pour chaque accès ou service. En effet, en cas de perte ou de vol d'un de vos mots de passe, vous

limitez les risques d'accès frauduleux au seul compte lié à ce mot de passe.

3/A – Un mot de passe trop simple ou facile à deviner n'offre pas un niveau de sécurité suffisant, ce qui pourrait faciliter la tâche des cybercriminels.

4/A – 2 B – 3 C – 1

HAMEÇONNAGE



1/ Bonnes pratiques

Sur mon compte bancaire, je découvre un débit que je ne reconnais pas. Je crains d'être victime d'un « hameçonnage » lié à un message douteux auquel j'ai répondu il y a deux semaines. Parmi les propositions, quelles sont les deux bonnes pratiques à mettre en œuvre ?

- ☐ A Je vérifie auprès de ma banque l'origine du débit et fais opposition à celui-ci
- ☐ B Je laisse passer quelques jours pour m'assurer qu'il s'agit vraiment d'un débit frauduleux
- ☐ C Je dépose plainte au commissariat de police ou à la gendarmerie la plus proche

2/ Vrai ou Faux

Il est inutile de déposer plainte pour un message d'hameçonnage auquel j'ai répondu.

- ☐ Vrai ☐ Faux

3/ Cherchez l'intrus

Comment se prémunir de l'hameçonnage ?

- ☐ A Si j'ai un doute concernant un message électronique ou un appel, je contacte directement l'organisme concerné pour en confirmer l'authenticité
- ☐ B Je vérifie qu'il y ait bien un logo officiel dans le message reçu
- ☐ C Avant de fournir toute information sur un site, je vérifie son adresse afin de m'assurer que je suis sur un site légitime
- ☐ D Je ne communique jamais d'informations sensibles par téléphone ou messagerie électronique

4/ Reliez les situations à leurs solutions

- | | | |
|---|----------------------------|---|
| Mon adresse de messagerie a été usurpée | A ☐ | 1 Je fais opposition auprès de ma banque et je dépose plainte |
| J'ai malencontreusement communiqué mon numéro de carte bancaire | B ☐ | 2 Je la signale à Phishing Initiative |
| J'identifie une adresse de site d'hameçonnage | C ☐ | 3 Je change immédiatement de mot de passe |

RÉPONSES

1/A et C

2/FAUX – Si vous avez malencontreusement communiqué des informations sensibles, comme votre numéro de carte bancaire, déposez plainte au commissariat de police ou à la gendarmerie la plus proche. Les cybercriminels pourraient, en effet, en faire un usage frauduleux. Pour être conseillé en cas d'hameçonnage, contactez le service Info Escroqueries au 0805 805817 (appel gratuit).

3/B – Le fait qu'il y ait dans un message le logo officiel d'un organisme ne signifie pas nécessairement que le message ait été envoyé par l'organisme concerné.

4/A – 3 B – 1 C – 2

SÉCURITÉ DES APPAREILS MOBILES

1/ Bonnes pratiques

Parmi les propositions, quelles sont les deux bonnes pratiques à mettre en œuvre pour assurer au mieux la sécurité numérique de vos appareils mobiles ?

- ☐ A Je ne fais jamais fonctionner le Wi-Fi et le Bluetooth en même temps
- ☐ B Je mets régulièrement mes appareils à jour
- ☐ C Je les verrouille avec un code d'accès difficile à deviner, en plus du code PIN
- ☐ D J'équipe mes appareils d'une coque et d'une protection d'écran

2/ Vrai ou Faux

Je n'ai pas besoin de faire des sauvegardes de mon téléphone.

- ☐ Vrai ☐ Faux

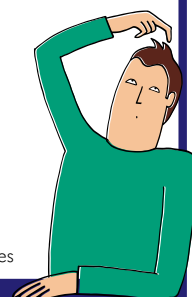
3/ Cherchez l'intrus

J'ai besoin d'une application mobile. Je la télécharge :

- ☐ A sur le site officiel du fournisseur
- ☐ B sur les magasins officiels d'applications comme Google Play ou App Store, par exemple
- ☐ C sur n'importe quel autre site

4/ Reliez les situations à leurs solutions

- | | | |
|---|-----------------------------------|---|
| Je travaille régulièrement à l'extérieur | A ☐ | 1 Je bloque ma ligne en appelant mon opérateur et mon téléphone en communiquant mon code IMEI et je dépose plainte |
| J'ai perdu ou je me suis fait voler mon téléphone | B ☐ | 2 J'évite de me connecter à un réseau Wi-Fi public |
| Je télécharge un jeu sur mon téléphone | C ☐ | 3 Je n'autorise pas l'accès à mes photos, mes contacts et mes messages |



RÉPONSES

1/B et C

2/FAUX – Votre appareil mobile contient de nombreuses données, comme votre répertoire de contacts, vos messages, vos photos et vidéos. En cas de perte, de panne ou de vol de votre appareil, vous pourriez ne plus retrouver vos données.

3/C – Seuls les sites ou les magasins officiels vérifient que les applications que vous installez ne sont pas piégées.

4/A – 2 B – 1 C – 3

SÉCURITÉ DES USAGES PRO / PERSO

1/ Bonnes pratiques

Parmi les propositions, quelles sont les deux bonnes pratiques à mettre en œuvre pour sécuriser au mieux mes usages numériques pro/perso ?

- ☐ A J'utilise des mots de passe différents pour tous les services professionnels ou personnels auxquels j'accède
- ☐ B Peu importe l'usage, je n'utilise que mes dossiers professionnels
- ☐ C Au travail, je mélange fichiers personnels et professionnels
- ☐ D Je ne mélange pas mes messages pro et perso dans ma messagerie personnelle

2/ Vrai ou Faux

J'ai le droit de m'exprimer sur mon travail ou mon entreprise sur les réseaux sociaux lorsque j'utilise mon ordinateur personnel.

- ☐ Vrai ☐ Faux

3/ Cherchez l'intrus

Pour protéger mes usages numériques pro/perso :

- ☐ A J'utilise un stockage de données professionnelles distinct du stockage de données personnelles
- ☐ B J'utilise ma connexion professionnelle uniquement pour mes besoins professionnels
- ☐ C J'utilise mon matériel professionnel pour des besoins personnels
- ☐ D J'effectue les mises à jour de mes systèmes très régulièrement

4/ Reliez les situations à leurs solutions

- | | | |
|---|-----------------------------------|--|
| Je suis à la maison et je consulte mes messages professionnels | A ☐ | 1 Je demande l'autorisation à mon employeur et prends des mesures de sécurité supplémentaires |
| Je stocke des documents professionnels sur un service en ligne personnel | B ☐ | 2 Je ne le fais qu'à partir de mon ordinateur professionnel |
| Je réalise parfois des téléchargements illégaux depuis mon ordinateur professionnel | C ☐ | 3 Mon entreprise pourrait contrôler mon utilisation de la connexion Internet professionnelle et se retourner contre moi |



RÉPONSES

1/A et D

2/VRAI – Uniquement si vos propos ne portent pas préjudice à l'entreprise. Dans le cas contraire, vous risqueriez des poursuites judiciaires.

3/C – Bien que l'utilisation d'une connexion Internet professionnelle à des fins personnelles soit

tolérée, gardez à l'esprit que votre utilisation peut mettre en cause votre entreprise. Elle pourrait se retourner contre vous si vous commettiez des actes répréhensibles. Par ailleurs, votre entreprise est en droit de contrôler l'utilisation de la connexion qu'elle met à votre disposition.

4/A – 2 B – 1 C – 3

RÉSEAUX SOCIAUX



1/ Bonnes pratiques

Parmi les propositions, quelles sont les deux bonnes pratiques à mettre en œuvre pour éviter le piratage de compte ?

- ☐ A J'utilise des mots de passe complexes
- ☐ B J'utilise le même mot de passe sur tous mes réseaux sociaux car c'est plus simple à retenir
- ☐ C J'active la double authentification
- ☐ D Ce n'est pas utile de sécuriser mes réseaux sociaux car seuls mes amis peuvent voir mon profil

2/ Vrai ou Faux

Je peux publier ce que je veux sur Internet si j'utilise un pseudonyme.

- ☐ Vrai ☐ Faux

3/ Cherchez l'intrus

Quelles sont les bonnes pratiques d'utilisation des réseaux sociaux :

- ☐ A Je fais preuve de discernement lorsque j'évoque mon travail car cela pourrait me porter préjudice ainsi qu'à mon entreprise
- ☐ B Sur les réseaux sociaux, je peux m'exprimer sans crainte que mes propos soient interprétés ou rediffusés
- ☐ C Je suis vigilant sur les contenus partagés par mes contacts, qui peuvent publier des contenus malveillants à leur insu
- ☐ D Je vérifie régulièrement qu'il n'y a aucune connexion sur mon compte depuis un appareil inconnu

4/ Reliez les situations à leurs solutions

- | | | |
|---|----------------------------|---|
| Je n'utilise plus mon compte de réseau social | A ☐ | ☐ 1 En faisant preuve de discernement et sans diffuser d'informations personnelle |
| Je publie régulièrement sur les réseaux sociaux | B ☐ | ☐ 2 Je le supprime pour éviter que mon compte soit utilisé à mon insu ou que mes informations ne soient récupérées par des tiers |
| En cas de publication gênante ou compromettante sur les réseaux sociaux | C ☐ | ☐ 3 Je vais régler la configuration de mon compte dans les paramètres |
| Je souhaite restreindre la visibilité de mes informations personnelles et de mes publications | D ☐ | ☐ 4 Je demande la suppression du contenu au réseau social concerné |

RÉPONSES

1/ A et C

2/ FAUX – Internet n'est pas une zone de non-droit et l'anonymat n'y est pas absolu : les propos incitant à la haine ou à la violence, la pédophilie, le cyberharcèlement, l'atteinte au droit à l'image ou au droit d'auteur... sont punis par la loi.

3/ B – Même dans un cercle que l'on pense restreint, vos publications peuvent vous échapper et être rediffusées ou interprétées au-delà de ce que vous envisagez

4/A2 B 1 C4 D3

PIRATAGE DE COMPTE



1/ Bonnes pratiques

Parmi les propositions, quelles sont les trois bonnes pratiques à mettre en œuvre pour éviter le piratage de compte en ligne ?

- ☐ A J'utilise des mots de passe complexes et différents pour chaque site et application
- ☐ B Je ne fais jamais mes mises à jour
- ☐ C Je ne communique jamais mes mots de passe à un tiers
- ☐ D J'active la double authentification lorsqu'elle est disponible

2/ Vrai ou Faux

Si votre boîte mail est piratée, il est utile de prévenir tous vos contacts

- ☐ Vrai ☐ Faux

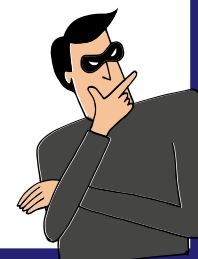
3/ Cherchez l'intrus

Parmi ces bonnes pratiques, quel est l'intrus :

- ☐ A J'applique de manière régulière et systématique mes mises à jour système et logiciels
- ☐ B J'utilise les réseaux WiFi publics en toute confiance
- ☐ C J'installe un antivirus et je vérifie qu'il fonctionne
- ☐ D J'évite les sites illicites ou non sûrs

4/ Reliez les situations à leurs solutions

- | | | |
|--|----------------------------|---|
| Mon compte vient d'être piraté et je n'arrive plus à m'y connecter | A ☐ | ☐ 1 Je n'ouvre pas la pièce jointe |
| Je viens de recevoir un e-mail suspect contenant une pièce jointe | B ☐ | ☐ 2 Je change sans tarder le mot de passe du compte piraté sur tous les sites et comptes sur lesquels je l'utilisais |
| Je suis victime d'un piratage d'un de mes comptes | C ☐ | ☐ 3 Je me déconnecte systématiquement après chaque utilisation pour éviter que quelqu'un puisse y accéder après moi |
| J'ai fini d'utiliser mon compte | D ☐ | ☐ 4 Je contacte le service concerné pour signaler le piratage et demander la réinitialisation de mon mot de passe |



RÉPONSES

1/ A, C et D

2/ VRAI – Il faut prévenir tous vos contacts pour qu'ils ne soient pas victimes à leur tour des cybercriminels qui les contacteraient en usurpant votre identité.

3/ B – En effet, les réseaux Wifi publics sont souvent mal sécurisés et peuvent parfois être contrôlés voire usurpés par des cybercriminels.

4/ A4 B1 C2 D3

*Je m'en vais préparer
le prochain numéro,
au plaisir de vous
retrouver très vite !*



Cybermag - Édition spéciale Congrès / Décembre 2024

Éditions juridiques et techniques - 73, boulevard de Clichy - 75009 Paris

Directeur de publication : Olivier Baret - Secrétaire national de la Chambre nationale des commissaires de justice

Responsable de la publication : Bruno Le Nozer

Responsable d'édition : Vincent Gauchevertu

Secrétaire de rédaction : Ségolène Quentin

Crédits photos : © AdobeStock - Dessinateur des bandes dessinées : BDShong@gmail.com - Création et mise en page : Nordcompo