



AVOCATS
BARREAU
• PARIS

CYBERSÉCURITÉ

LES BONNES PRATIQUES



PRINCIPES DE BASE
POUR LES AVOCATS

sommaire .



Sécurité des comptes
et accès



Sécurité du poste de
travail



Sécurité des
données



Sécurité des
emails



Focus phishing



Sécurité internet



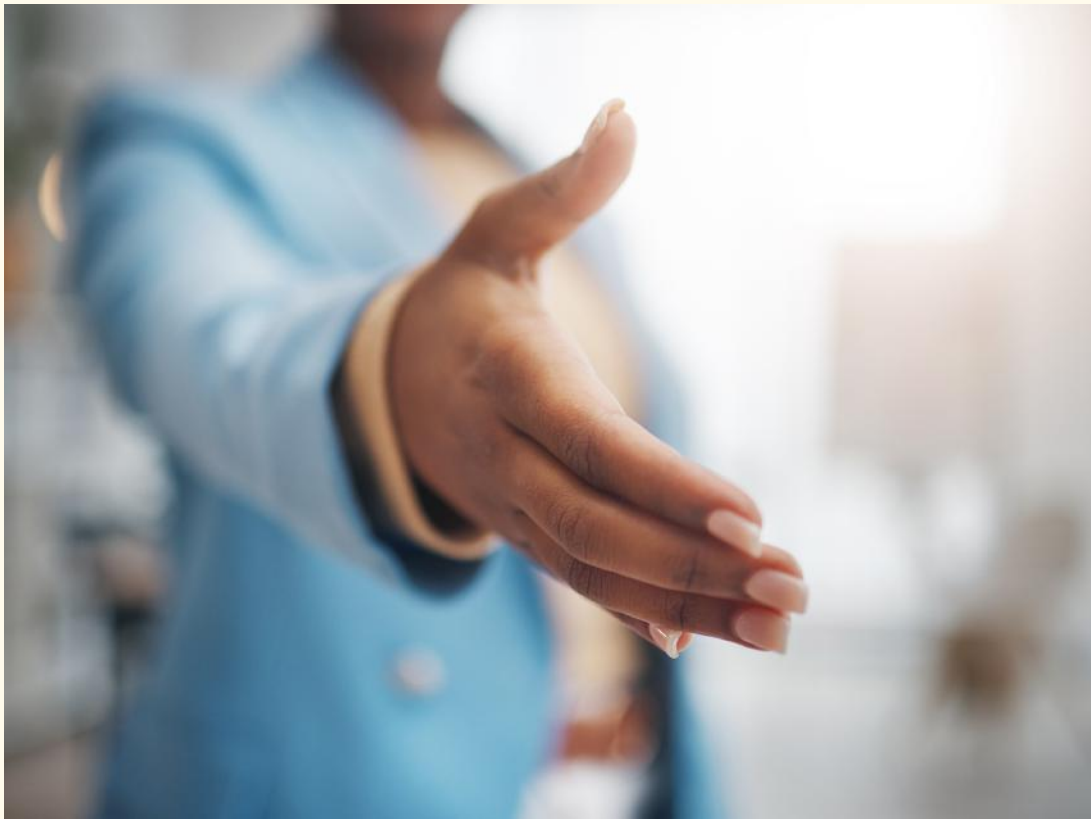
Ingénierie
sociale



En déplacement



Bon pour la
planète



MOT DU RSI

Ce document rappelle les principes de base de la sécurité de l'information au bureau.

La plupart de ces règles peuvent également s'appliquer dans la vie personnelle, cela peut éviter de nombreux cyber-problèmes.



SÉCURITÉ DES COMPTES

Les moyens d'identification (nom utilisateur (login), clés avocats, etc.) et les mots de passe associés sont la première ligne de défense pour sécuriser les données d'un cabinet.

Ils doivent rester strictement confidentiels et ne doivent en aucun cas être partagés. Si vous les communiquez, vous êtes responsable des actions commises sous votre identité.

Personne ne doit vous demander votre mot de passe !



ET DES ACCÈS

- Choisissez des mots de passe longs et complexes : minimum 12 caractères mélangeant des majuscules, minuscules, chiffres et caractères spéciaux.
- Vos mots de passe doivent être facilement mémorisables mais difficiles à deviner ; n'utilisez pas de noms communs, de séries numériques logiques (ex : 123) ni de données à caractère personnelle (date de naissance, nom de famille etc.).
- Changez vos mots de passe régulièrement et modifiez toujours les mots de passe qui vous sont fournis par défaut.

Gardez en tête la règle : “1 compte, 1 mot de passe”.

- Privilégiez la double authentification lorsqu'elle est proposée. Cela permet de sécuriser votre compte avec, en plus du mot de passe, un second moyen d'identification (envoi d'un code par SMS ou par l'application mobile MS Authenticator).

Pour gérer facilement vos mots de passe, privilégiez surtout un coffre-fort numérique (Keeper par exemple, évoqué sur le site <https://numerique.avocatparis.org/>)



SÉCURITÉ DU

Votre poste de travail est un point d'accès privilégié aux datas de votre cabinet.

Vous avez la responsabilité de sa sécurité, y compris à l'extérieur. Utilisez uniquement les équipements mis à votre disposition par votre cabinet, n'utilisez jamais ceux qui vous sont offerts (clés USB...) ou prêtés (partage de connexion...).

- Utilisez seulement un **poste de travail configuré et approuvé** pour travailler.
- Servez-vous **uniquement des programmes autorisés et fournis par le cabinet.**
- **Ne désinstallez pas et ne modifiez aucun logiciel de sécurité standard**, en particulier les logiciels antivirus.
- **Ne contournez pas ou ne changez pas les configurations de sécurité** des équipements du cabinet.
- Lorsque **vous quittez votre poste de travail**, même pour quelques minutes :
 - **Sécurisez** vos équipements (câble anti-vol si vous en disposez) ainsi que vos documents sensibles
 - **Conservez sur vous** vos badges, clés et téléphones portables.
 - **Verrouillez** votre session.
 - **Fermez** à clé vos casiers et placards.
- **Ne laissez pas vos documents à la portée de tous** dans les espaces communs (espaces imprimantes, cafétéria...).
- **Détruisez** les documents dont vous n'avez plus l'utilité en utilisant les conteneurs dédiés.

- **Conservez sur vous vos badges, clés et téléphones portables.**
- **Verrouillez votre session.**
- **Fermez à clé vos casiers et placards.**



POSTE DE TRAVAIL

- Eteindre le poste de travail **tous les soirs**.
- **Signalez tout dysfonctionnement** ou comportement vous paraissant anormal à votre assistance.
- **Ne créez pas de compte utilisateur** en local.
- **N'interrompez pas les processus automatiques** de mises à jour lorsqu'ils s'exécutent.
- **Ne communiquez jamais d'information confidentielle** ou secrète lors de vos conversations téléphoniques.



SÉCURITÉ DE

N'utilisez pas de périphériques de stockage non autorisés par votre cabinet.

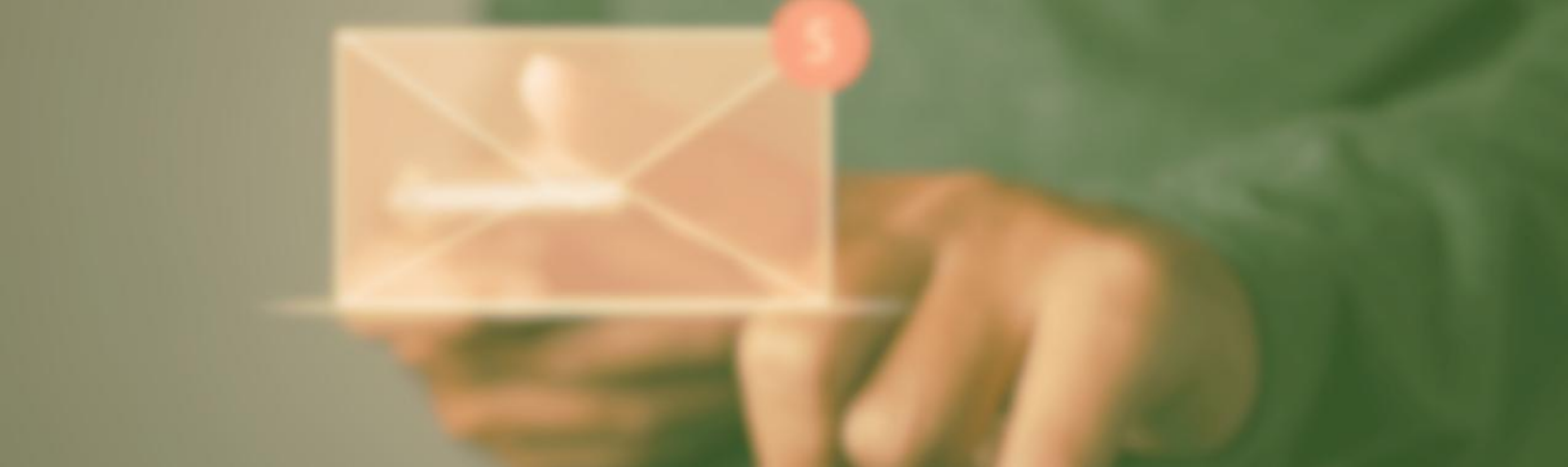
La sensibilité d'une donnée et/ou de son traitement est évaluée en fonction des risques encourus par le cabinet, notamment en cas de destruction ou de perte de celle-ci, d'accès non autorisé, etc.

Pour la protection des données, les informations relatives au cabinet doivent être uniquement stockées sur des équipements autorisés par l'établissement.

- Ne prenez pas de photos contenant des informations confidentielles.
- Ne stockez pas de documents dont vous n'avez pas les droits de diffusion ou d'utilisation (copyright).
- Sauvegardez vos données et documents sur des espaces de stockage logiques validés par l'établissement (ex : partage réseau, un cloud sécurisé).
- Sécurisez vos documents en fonction de leur sensibilité et des outils établissement mis à disposition.
- Plusieurs solutions sont disponibles pour partager des documents (Cloud avocats de Paris), selon leur niveau de confidentialité, sans utiliser de périphérique de stockage.

S DONNÉES

- Ne partagez pas de documents professionnels par SMS ou sur un outil de messagerie instantanée, même si ces outils sont homologués par l'établissement.
- Avant de communiquer une information, assurez-vous de connaître son niveau de sensibilité.
- Faites attention à la confidentialité des informations que vous traitez, attention aux regards et aux oreilles indiscrètes (ex : évitez les discussions à caractère professionnel dans les transports en commun).
- Lorsque vous travaillez, au bureau, en télétravail ou en déplacement, veillez à ne pas vous placer dans un espace exposé ou visible de l'extérieur (fenêtre, terrasse...) ou devant une caméra connectée (système de surveillance). N'hésitez pas à utiliser votre filtre de confidentialité. Isolez-vous lors de vos conversations professionnelles



SÉCURITÉ DES EMAILS

Les mails ne sont pas un canal de transmission sécurisé.

- Utilisez exclusivement une messagerie sécurisée pour vos mails professionnels et utilisez vos messageries et terminaux personnels pour vos besoins privés.
- Les transferts de documents de vos équipements professionnels vers vos équipements personnels sont dangereux.
- Limitez l'envoi d'emails uniquement aux destinataires ayant besoin de l'information (attention aux homonymes et aux saisies automatiques des adresses).
- Lorsque vous activez votre message d'absence, ne pas préciser votre période d'absence afin d'éviter la transmission d'informations internes à des tiers.
- Eviter d'utiliser la messagerie pour des opérations bancaires ou transactionnelles. Utilisez le logiciel de la Carpa.
- N'envoyez jamais des informations confidentielles par email



FOCUS PHISHING

Le terme phishing désigne une technique utilisée par des escrocs pour obtenir des informations qui pourraient être exploitables, en se servant de la messagerie. Ils se font souvent passer pour un organisme de confiance (institution financière, PayPal, eBay, Amazon), dans le but d'obtenir des données confidentielles.

- N'ouvrez pas et ne répondez pas aux emails de provenance inconnue, ou dont le sujet ou le contenu sont suspects (fautes d'orthographe, mauvaise formulation, incohérences, histoire rocambolesque...).
- Ne cliquez pas sur les liens Internet et n'ouvrez pas les fichiers attachés si vous n'êtes pas certain de la provenance du courriel.
- En cas de doute, vérifiez l'identité de l'expéditeur en affichant les détails de l'email et contactez le RSSI de l'Ordre : rsssi@avocatparis.org.
- Si vous constatez que votre ordinateur est infecté, débranchez immédiatement votre câble réseau ou coupez le réseau WiFi si vous êtes connectée à distance et n'éteignez surtout pas votre machine.



SÉCURITÉ INTERNET

- Ne laissez pas votre adresse email professionnelle ni d'autres informations confidentielles (exemples : données client, code source etc.) sur des sites externes à l'établissement tels que les forums et autres réseaux sociaux. Elles pourraient être récupérées automatiquement par des robots à des fins commerciales ou dans l'objectif délibéré de nuire.
- Privilégiez les réseaux WiFi d'entreprises, domestiques ou, à défaut, les services de données cellulaires lorsque les conditions le permettent. Ne vous connectez jamais à un WiFi public avec vos équipements professionnels.
- Désactivez les options WiFi et Bluetooth quand vous ne les utilisez pas afin de limiter le temps de connexion et donc les risques de piratage.
- Si vous devez accéder à un site contenant des informations sensibles (exemple : transactions financières), assurez-vous qu'il est indiqué https:// dans la barre d'adresse. S'il n'y a pas le "s", cela signifie que le flux n'est pas chiffré et donc non sécurisé.



INGÉNIERIE SOCIALE

Il s'agit d'une forme de manipulation psychologique consistant à obtenir un bien ou une information en exploitant la confiance et la naïveté des personnes.

Les attaques sont souvent précédées d'une recherche d'informations en interne, pour connaître les process de l'entreprise ciblée (indiscrétion sur les réseaux sociaux, personnes ayant travaillé un temps dans la société).

- Limitez la diffusion d'informations professionnelles sur les réseaux sociaux.

COMMENT DÉCELER UNE ATTAQUE ?

- Apprenez-en plus sur votre interlocuteur : demandez-lui des précisions sur son activité, son nom, la manière dont il a obtenu votre contact, etc.
- Vous demande-t-il des informations confidentielles ? (Mot de passe, RIB, organigramme...)
- Vous presse-t-il à prendre une décision ou à faire une action importante ?



EN DÉPLACEMENT

Dans les situations de mobilité, quotidienne ou ponctuelle, il est primordial de redoubler de vigilance et d'appliquer scrupuleusement les règles d'or de la cybersécurité.

Pour un hacker, l'accès à un équipement informatique (ex. ordinateur, téléphone portable, tablette) est une porte d'entrée sur le réseau de l'établissement.

- Évitez de tout emporter dans un seul bagage (ordinateur, smartphone, badge d'accès, clé avocat ...).
- Évitez le transport de données superflues et limitez le stockage de vos données dans votre disque local.
- Évitez au maximum le transport de documents professionnels en version papier
- Ne communiquez pas d'informations concernant votre voyage sur les réseaux sociaux.
- Gardez toujours vos équipements (ordinateur, smartphones, tablettes, badge d'accès, clé avocat...) avec vous. A l'hôtel, évitez de les laisser dans votre chambre si vous vous absentez, utilisez un coffre-fort si possible.



De manière générale, limitez l'usage de vos équipements dans les lieux publics et dans les transports.

- Ne rechargez pas vos équipements professionnels (poste de travail, smartphones, tablettes ...) sur les bornes USB en libre-service. Utilisez les prises électriques.
- En voyage, ne vous connectez jamais aux réseaux ou équipements inconnus, notamment aux WiFi publics (gare, aéroport...). Dans les paramètres réseaux de votre terminal, vous pouvez choisir de ne pas vous connecter automatiquement au Wi-Fi.
- N'hésitez pas à utiliser votre filtre de confidentialité. Leur usage est vivement recommandé lors des déplacements.

AU RETOUR ET AU MOINDRE DOUTE !

- Changez tous les mots de passe (professionnels et personnels) que vous avez utilisés pendant votre voyage.
- Faites analyser vos équipements par votre support informatique s'il y a des raisons de penser qu'ils ont pu être compromis.
- Méfiez-vous des emails de phishing qui pourraient vous être envoyés en tirant parti des informations récupérées lors de votre voyage: envoyez ces e-mails suspects à notre RSSI.



BON POUR LA PLANÈTE

Le numérique représenterait aujourd'hui 3 à 4% des émissions de gaz à effet de serre dans le monde et 2,5% de l'empreinte carbone en France (source GreenIT). Côté courriels, quelques 363 milliards de messages sont envoyés et reçus chaque jour dans le monde. Il est peut-être temps d'ajuster nos comportements et comme tous les gestes comptent, voici quelques conseils pour réduire l'impact écologique de nos mails :

- Eteindre son ordinateur et son écran systématiquement le soir.
- Ne pas multiplier les destinataires en répondant à "tous".
- Vider sa corbeille régulièrement.
- Utiliser le cloud ODA pour les fichiers lourds plutôt que le mail.
- Supprimer les documents dont vous n'avez plus l'utilité.
- Imprimer avec modération, n'imprimez vos messages et pièces jointes qu'en cas de nécessité.



AVOCATS
BARREAU
• **PARIS**



Mai 2025

David Di Mascio - RSSI

Pamela Gardel - Conduite du changement