Ordre des Avocats Hauts-de-Seine

LES 10 CYBER-COMMANDEMENTS DE L'AVOCAT

Guide d'hygiène numérique du Barreau des Hauts-de-Seine

1. Choix, gestion et sécurité des mots de passe

Choisir des mots de passe robustes et uniques

Utilisez des mots de passe de 12 caractères minimum, incluant majuscules, minuscules, chiffres et caractères spéciaux. Évitez les informations personnelles (nom, date de naissance) et les mots du dictionnaire.

Méthode phonétique

Exemple : « J'ai acheté 5 CDs pour cent euros cet après-midi » devient ght5CDs%E7am.

Méthode des premières lettres

Exemple : « Allons enfants de la patrie, le jour de gloire est arrivé » devient aE2IP,lJ2Géa!.

Ne pas pré-enregistrer les mots de passe dans les navigateurs

Utilisez des solutions de stockage certifiées (CSPN).

2. Mise à jour et sécurité des logiciels

Maintenir les logiciels à jour

Configurez les mises à jour automatiques, surtout pour les logiciels de messagerie. Assurez-vous que vos systèmes d'exploitation, navigateurs et logiciels antivirus sont à jour pour bénéficier des dernières protections contre les menaces

Télécharger les mises à jour depuis les sites officiels

Activer l'antivirus

Pour identifier et supprimer les logiciels malveillants.

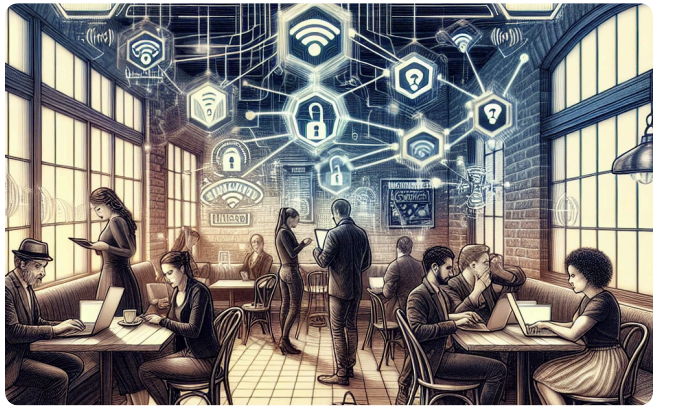
3. Protection de la connexion internet

Utiliser un VPN

Pour masquer l'adresse IP et maintenir la confidentialité en ligne.

Préférer la connexion par câble ou Wi-Fi avec protocole WPA2 ou WPA-AES

Pour garantir une connexion sécurisée et fiable.



Ne pas utiliser les Wi-Fi publics

Pour éviter l'interception de données sensibles par des tiers malveillants.

4. Sauvegarde des données

Sur un support externe

Réservé exclusivement à cet usage et non connecté en permanence au système d'information. Rangez ce support dans un lieu éloigné de l'ordinateur pour éviter que la destruction des données d'origine ne s'accompagne de la destruction de la copie de sauvegarde (incendie, inondation, vol). Accordez une attention particulière à la durée de vie du support.

Sur un cloud externe

Protégé par un mot de passe robuste. Gardez à l'esprit que ces espaces peuvent être ciblés par des attaques. Consultez les conditions générales d'utilisation et préférez le recours à des spécialistes pour des contrats personnalisés. Idéalement, chiffrez les données avant de les copier dans le cloud à l'aide d'un logiciel de chiffrement.

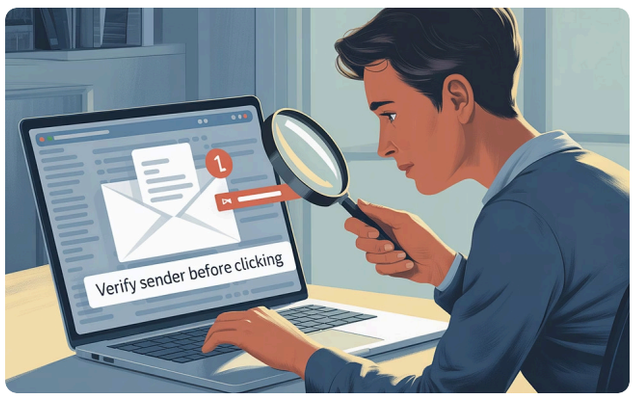
5. Utilisation de la messagerie et sécurité des emails

Messagerie non sécurisée (à éviter)

- Éviter de partager des informations sensibles.
- Utiliser des mots de passe forts et uniques.
- Être vigilant face aux tentatives de phishing.
- Activer l'authentification à deux facteurs (2FA).

Messagerie sécurisée (à privilégier)

- Utiliser des services offrant le chiffrement de bout en bout.
- Vérifier les certificats de sécurité.
- Utiliser des mots de passe forts et uniques.
- Activer la 2FA.



Sécurité des emails

- Vérifier l'expéditeur : Assurez-vous de la bonne orthographe de l'adresse e-mail et de l'identité de l'expéditeur.
- Ne pas ouvrir les mails d'inconnus ou à l'objet étrange.
- Ne pas ouvrir les pièces-jointes ni cliquer sur les liens suspects.
- Ne jamais répondre par courriel à une demande d'informations personnelles ou confidentielles.

6. Séparation matériel personnel/professionnel

Emails

Ne pas faire suivre des emails professionnels sur des services de messagerie personnels.

Données

Ne pas héberger des données professionnelles sur des équipements personnels.

Périphériques

Éviter de connecter des clés USB au matériel professionnel.

7. Sécurité des transactions bancaires et achats en ligne

Vérifier que le site est sécurisé

Cadenas dans la barre d'adresse, mention https.

Utiliser l'authentification bancaire

Ou l'envoi de code par SMS.

Protéger ses informations

Ne jamais partager ses identifiants bancaires.

8. Protection du profil utilisateur

Créer une adresse secondaire

Différente de l'adresse professionnelle pour la création de profils utilisateurs.

Utiliser des pseudonymes

Ne pas communiquer d'informations superflues

Exemple : date de naissance fictive.

9. Sécurité des smartphones

Sécuriser l'accès

Utiliser un schéma ou un mot de passe

Gérer les applications

Installer uniquement les applications nécessaires

Sauvegarder régulièrement

Sur un support externe

Protéger les mots de passe

Ne pas les pré-enregistrer

10. Premiers réflexes en cas de cyberattaque

Se déconnecter d'internet sans éteindre le terminal

Signaler l'attaque

Au service informatique, au prestataire, et à l'autorité de régulation (et au barreau ?).

Ne jamais payer la rançon