WOOXO
IT security for business continuity

YOONITED
TOGETHER AGAINST CYBERCRIME

MANUEL DE SURVIE NUMÉRIQUE

A l'attention des organisations professionnelles
et de leurs collaborateurs

EDITO

En quelques années, **la cybermalveillance s'est arrogée la première place sur le podium des fléaux économiques.**

Racket, atteinte à l'image, espionnage, sabotage… les mobiles des cybercriminels sont multiples mais les conséquences de ces attaques pour les entreprises sont souvent identiques : **fuites ou pertes de données susceptibles d'engendrer d'importantes perturbations temporaires ou un arrêt définitif de l'exploitation.**

Un système efficace de défense contre la cybercriminalité repose sur 3 piliers complémentaires :

» **La pédagogie** : Une politique efficace de prévention menée auprès des collaborateurs.

» **Un arsenal préventif** pour contrer les cyberattaques connues : antispam, antivirus, firewall, politique de mise à jour de toutes les applications.

» **Un système curatif professionnel** pour contrer les cyberattaques non filtrées : un système de sauvegarde et plan de reprise d'activité après sinistre aux standards professionnels.

Le présent Manuel entend fournir aux Dirigeants et Directeurs des Ressources Humaines en PME, **un support didactique simple, intelligible et efficace** pour mettre en place une première approche pédagogique dans l'entreprise.

Nous espérons qu'il vous sera utile et largement diffusé auprès de vos collaborateurs.

Des trois piliers sur lesquels doit reposer une politique de cybersécurité, **la pédagogie constitue sans nul doute possible le pilier maître.** C'est pourtant le moins coûteux à implémenter dans une organisation.

Qui veut la paix, prépare la cyberguerre ! Bonne lecture.

Luc d'URSO
Président Directeur Général
WOOXO SAS

SOMMAIRE

BIEN GERER SES MOTS DE PASSE

A quoi ça sert ?

Le mot de passe est un identifiant. **Il permet de s'assurer que la personne derrière l'équipement connecté** (PC, Tablette, Smartphone…) **est bien celle autorisée** à accéder aux ressources (documents, base de données, applications, équipements).

Ces ressources peuvent également être partagées avec d'autres personnes également autorisées (sur un serveur informatique par exemple).

Pourquoi intéressent-ils les cybercriminels ?

En usurpant votre identité des personnes malintentionnées peuvent :

» **Dérober ou détruire les ressources protégées** pour vous faire chanter ou nuire à votre réputation.

» **Effectuer des opérations en votre nom** (envoi d'un mail, d'une instruction en votre nom).

» **Espionner vos faits et gestes.**

Comment les obtiennent-ils ?

» **Pour les attaques en masse :** en faisant l'acquisition sur le marché du cybercrime d'une base de données dérobée à un prestataire qui détient ces informations (opérateur télécom, fournisseur de solutions cloud, réseau social, site de rencontres…).

» **Pour les attaques ciblées :** en les déduisant à partir d'informations publiées, collectées et agrégées sur votre vie privée : surnom, date de naissance, prénom du conjoint ou des enfants, animal de compagnie… ou à l'aide d'un logiciel espion, un enregistreur de frappe (keylogger), installé à votre insu sur l'un de vos équipements par un maliciel (malware) véhiculé par un site internet, une bannière publicitaire ou une pièce jointe infectée à dessein.

Bonnes pratiques

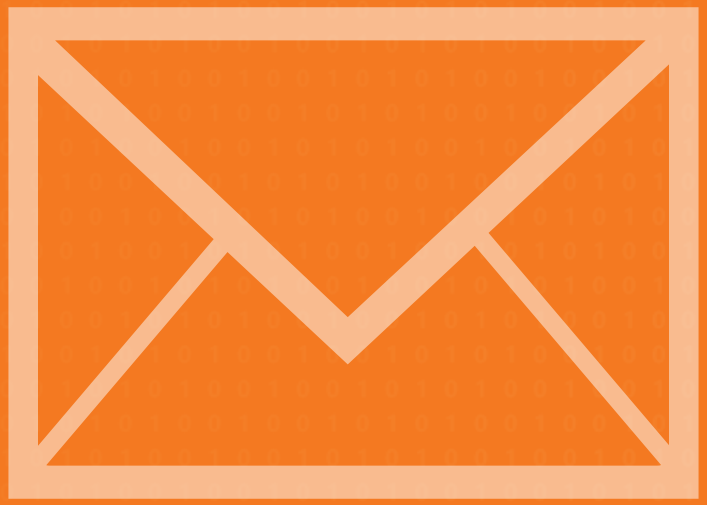
» **Choisissez des mots de passe avec au moins 8 caractères incluant des majuscules, des minuscules, des chiffres, des caractères spéciaux et renouvelez-les a minima tous les 6 mois.**

Deux méthodes simples pour définir et retenir vos mots de passe : La méthode phonétique : « t'as pas cent balle = tapa100bal» ou la méthode des premières lettres : « les 101 dalmatiens sont des chiens ! =l101dsdc! »

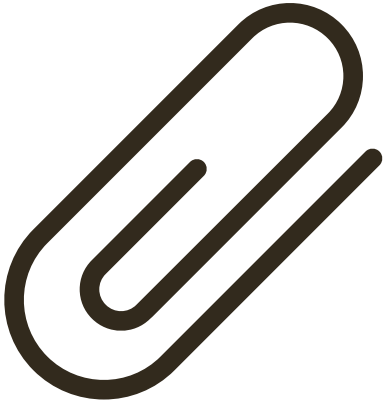
» Pour votre smartphone, **modifiez dès la première session** le mot de passe ou code PIN par défaut.

» **N'utilisez pas le même mot de passe pour toutes vos sessions**, notamment les applications sensibles permettant d'utiliser un de vos moyens de paiement (CB, Compte bitcoin...).

» **Ne confiez jamais les identifiants de votre station de travail à un collègue** de bureau, il pourra accéder à tous vos mots de passe enregistrés dans les paramètres avancés de votre navigateur.



CONTROLER L'ORIGINE ET LE CONTENU DE SES MAILS



A quoi ça sert ?

La messagerie est un des principaux vecteurs de diffusion des attaques cybercriminelles.

Et pour cause, près de la moitié des habitants de la planète dispose d'un accès internet et d'un compte de messagerie.

Pourquoi intéressent-ils les cybercriminels ?

En vous adressant un courriel malveillant on peut très simplement :

» **Infecter votre équipement pour crypter vos données** et vous demander une rançon pour les déchiffrer (Rançongiciel).

» **Dérober des données** sur votre station de travail ou sur le réseau si votre ordinateur est en réseau (informations confidentielles ou privées).

» **Vous espionner** (en enregistrant vos frappes clavier) et même activer des ressources à distance (caméra, micro…).

Comment les infections se propagent-elles ?

Les programmes malveillants sont **embarqués dans une pièce jointe ou un bouton cliquable inséré dans le corps du courriel.**

Le programme s'exécutera, ou se téléchargera sur un serveur distant, à l'ouverture de la pièce jointe ou lorsque vous cliquerez sur le bouton.

Bonnes pratiques

» Demandez à votre employeur que **votre boîte mail soit protégée par un anti-spam**, cela vous mettra à l'abri de la grande majorité des attaques en masse.

» **N'inscrivez vos identifiants nulle part** (post-it, dos du clavier, fichier, ni même dans un contact de votre messagerie).

» **Ne répondez jamais à des courriels vous demandant des informations personnelles ou confidentielles**, ou de ressaisir ces informations en ligne même si l'adresse de l'expéditeur vous paraît être un tiers de confiance (opérateur télécom, banque, organisme public…) et que l'identité visuelle du mail vous rappelle les codes visuels d'un prestataire connu.

» Si des liens figurent dans un courriel, passez votre souris dessus et **vérifiez l'adresse complète du site émetteur**, vérifiez la cohérence et méfiez-vous des URL maquillées ou transformées destinées à tromper votre vigilance (edf.xx.org, orange.xyz.fr, canolplus.fr...).

» **Gardez le sens critique** si un mail d'un destinataire bien connu de vous (collègue, ami) embarque une pièce jointe douteuse (une prétendue photo avec une extension de fichier inhabituelle .svg par exemple).

» **Ne relayez aucun message viral émis par une organisation inconnue** : demandes de don, information à faire circuler…

EN MOBILITÉ NE SOYEZ PAS NAIFS !

Pourquoi redoubler de vigilance lors de vos déplacements ?

Au bureau, vous travaillez dans un environnement relativement contrôlé et maîtrisé. L'accès au site est filtré, les personnes étrangères ou indésirables sont rapidement identifiées. Les stations de travail sont équipées de dispositifs de sécurité (anti-spam, antivirus…) et le réseau informatique est privé et protégé (parefeu et proxy).

A l'extérieur de l'entreprise, vous côtoyez sans le savoir des personnes mal intentionnées, vous vous connectez sur des réseaux publics souvent très mal sécurisés (Wifi d'Hôtels, Centres d'affaires, cybercafés...), vous empruntez des réseaux télécoms hautement surveillés dans certains pays.

En bref, vous évoluez dans la jungle numérique !

Pourquoi cela intéresse les cybercriminels ?

Espionnage industriel, chantage en vue d'une demande de rançon, **injection d'informations malveillantes** afin de vous compromettre, de vous recruter en tant que source si vous travaillez dans une entreprise sensible… les raisons de s'intéresser à vos équipements informatiques ne manquent pas.

Comment les cybercriminels s'introduisent-ils dans vos équipements ?

» **Lors de vos connexions à internet sur un Wifi public** : un pirate « renifleur » sur un réseau Wifi peut facilement connaître les sites que vous visitez, les identifiants (login et mot de passe) que vous utilisez, les documents et les messages que vous envoyez, etc.

» **En connectant votre équipement à un dispositif infecté** : borne de rechargement pour terminaux mobile, clé USB gracieusement prêtée par la société ou l'organisation que vous visitez .

Bonnes pratiques

» Si vous devez vous séparer de vos équipements, **ôtez la carte sim et la batterie.**

» **Configurez votre smartphone pour qu'il se verrouille automatiquement.**

» Dans les transports ou lieux publics, **utilisez un filtre écran si vous consultez des documents confidentiels** (ils évitent la lecture ou la photographie par-dessus votre épaule).

» Les Wifi d'hôtels, centres d'affaires, cybercafés… n'offrent pas de connexion internet garantissant votre sécurité et la confidentialité de vos communications. Pour toute communication confidentielle, **utilisez votre smartphone comme routeur et optez pour un partage de connexion** avec votre ordinateur.

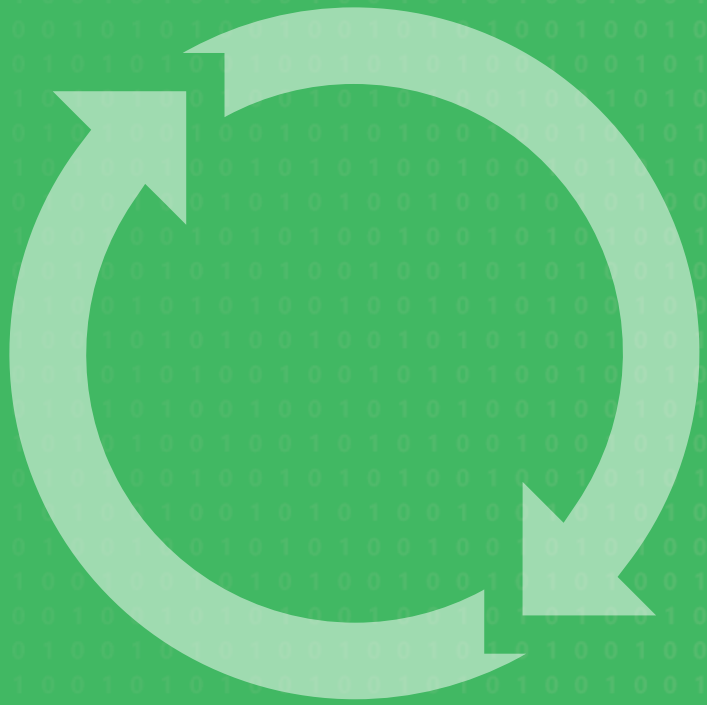
» Si vous devez télécharger des documents professionnels lors de vos déplacements, veillez à **utiliser une connexion sécurisée (Https)** et récupérer des fichiers chiffrés.

» **Pensez à effacer l'historique** de vos appels et consultations internet. Dans certains pays, les libertés individuelles sont plus réduites qu'en Europe et ces informations pourront être utilisées à charge contre vous si vos équipements sont saisis. Dans d'autres, les bagages et chambres d'hôtel sont fouillés. **Ne laissez pas vos terminaux** dans vos bagages en soute, ni dans la chambre d'hôtel, même dans les coffres d'hôtel.

» En cas de perte ou de vol, **demandez conseil à votre consulat** avant d'alerter le personnel de votre lieu de résidence ou les autorités locales.

» **Ne connectez aucun support amovible qui vous est proposé.** Il peut contenir des programmes malveillants susceptibles d'infecter votre terminal ou de surveiller vos agissements.

» Ne rechargez pas votre terminal sur des bornes publiques prévues à cet effet. **Utilisez exclusivement votre chargeur.**



MAINTENIR A JOUR SON SYSTEME

Pourquoi ?

Les systèmes d'exploitation (Windows, MacOS, Linux, Android, IOS…), les logiciels et les applications **comportent des vulnérabilités**.

Ces vulnérabilités, sitôt découvertes par les cybercriminels, sont **autant de failles qu'ils se pressent d'exploiter.** Elles sont progressivement corrigées par les éditeurs qui proposent des mises à jour aux utilisateurs.

Bonnes pratiques

» Configurez vos logiciels pour que les **mises à jour de sécurité s'installent automatiquement** quand cela est possible.

» **Acceptez les mises à jour proposées par les éditeurs.**

» Si vous devez télécharger une mise à jour, **connectez-vous exclusivement au site internet officiel de l'éditeur.**

ATTENTION AUX ACHATS EN LIGNE

Pourquoi ?

Lors d'un achat en ligne effectué à partir d'une station de travail ou d'un smartphone, **les coordonnées bancaires de l'entreprise sont susceptibles d'être interceptées** par des cybercriminels soit sur votre ordinateur, soit dans les bases de données clients du site marchand.

Pourquoi cela intéresse les cybercriminels ?

- **Pour soutirer de l'argent sur le compte de l'entreprise.**
- **Pour revendre ces informations sur le marché des données « dérobées ».**

Bonnes pratiques

- **Ne transmettez jamais par téléphone le cryptogramme au dos de votre carte bancaire.**
- **Contrôlez la présence d'un cadenas dans la barre d'adresse** ou en bas à droite de la fenêtre de votre navigateur Internet (remarque : ce cadenas n'est pas visible sur tous les navigateurs).
- **Vérifiez que l'adresse du site commence par « https:// »**
- **Contrôlez le contenu de la page du site Internet et les indices vous appelant à la vigilance** : fautes d'orthographe, syntaxe approximative…
- **Privilégiez la méthode impliquant l'envoi d'un code de confirmation de la commande par SMS.**

BESOIN D'UN AVIS D'EXPERT ?

N'HÉSITEZ PAS À NOUS CONTACTER

Le Pôle Conseil Cybersécurité Wooxo et ses consultants sont à votre entière disposition du lundi au vendredi de **9H00 à 12H30** et de **13H30 à 17H30**

+33 4 42 01 65 76 **ConseilsCybersecurite@wooxo.fr**

Ou planifiez directement un RDV avec un de nos consultants en cybersécurité en fonction de vos disponibilités :

www.wooxo.fr/Programme-Yoonited/Conseiller

NOTES

HEXATRUST
CYBERSECURITY & DIGITAL TRUST

WOOXO
IT security for business continuity

515 av. de la tramontane - ZAC Athélia IV
13600 La Ciotat - FRANCE
Tél : 0811 140 160
(inter.) +33 442 016 579
Fax : 0811 481 507
Email : info@wooxo.fr

A Propos de Wooxo :

Wooxo édite des solutions logicielles pour éliminer les risques d'interruption d'activité liés à la perte de données informatiques et accroît la productivité des organisations de petite et moyenne taille en permettant à leurs collaborateurs d'exploiter les documents professionnels en tout lieu, à tout instant et de façon sécurisée. Membre du Pôle mondial des Solutions Communicantes Sécurisées, de l'Afdel et de l'association EuroCloud, Wooxo a été labellisée entreprise innovante en 2011, lauréate des Trophées Innovation TIC PACA 2012, nommée deux années consécutives aux Trophées EY des Entreprises d'Avenir et figure depuis trois ans dans le TOP 250 EY Syntec des éditeurs de logiciels et dans le TOP 7 des éditeurs leaders du marché de la sauvegarde en 2014 selon le cabinet d'étude Markess.

L'entreprise est également partenaire du Programme gouvernemental Transition Numérique depuis le lancement du programme par le gouvernement.