INFO MAINTENANCE
INFORMATIQUE PROFESSIONNELLE

Réalisé par l'équipe d'INFO'MAINTENANCE, ces bonnes pratiques ont pour objectif de vous informer sur les risques et les réflexes à avoir afin de protéger l'informatique de votre entreprise.

INFO'MAINTENANCE vous conseille ces bonnes pratiques

N'hésitez pas à les relayer à vos collaborateurs

Pour rappel le règlement général sur la protection des données encadre et protège le traitement des données personnelles et plus largement l'intégrité des données numériques.
Les entreprises sont soumises à des obligations et se doivent de traiter correctement les données numériques qu'elles détiennent. Les sanctions liées à l'absence de mise en conformité peuvent être lourdes de conséquences. Il reste difficile aujourd'hui pour les entreprises de se prémunir contre des risques qui se multiplient chaque jour.

PROFESSIONNEL RÉFÉRENCÉ
CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

L'informatique est un sujet sérieux.
Le choix de votre partenaire est stratégique

Le choix du mot de passe

Un mot de passe est un mot ou une série de caractères utilisés comme moyen d'authentification pour prouver son identité lorsque l'on désire d'accéder à un lieu protégé, à un compte informatique, un ordinateur, un logiciel ou à un service dont l'accès est limité et sécurisé.
Pour bien protéger vos informations, choisissez un mot de passe difficile à trouver par une tierce personne :

- ➔ De 8 à 12 caractères
- ➔ Majuscules, minuscules
- ➔ Chiffres
- ➔ Caractères spéciaux
- ➔ Aucun lien avec vous-même *(nom, date de naissance…)*

Plusieurs méthodes existent pour définir un bon mot de passe, par exemple :
On peut utiliser la phonétique : chaque son génère l'un des caractères du mot de passe.
Exemple : «J'ai acheté trois œufs et deux BD ce matin». On obtient : gHt3Eé2BdCeMaT1.

Il est important de définir un mot de passe différent pour chaque utilisation d'un site internet soumise à identification, il doit aussi être changé régulièrement. Il est judicieux de ne pas conserver les mots de passe dans des fichiers ou sur des Post-its.

Mises à jour des logiciels

Les mises à jour consistent à télécharger la version la plus récente d'un logiciel, d'un programme ou d'un système d'exploitation afin de bénéficier des dernières modifications et mesures de sécurité.

Il est important de respecter certaines règles :

- ✓ Mises à jour régulières par le service informatique ou le prestataire après vérification de l'intégrité de fonctionnement de celles-ci
- ✓ Une bonne configuration de vos logiciels permettra aux mises à jour de se faire automatiquement,
- ✓ Les mises à jour se font à partir des sites officiels des éditeurs.

L'attribution des droits d'accès

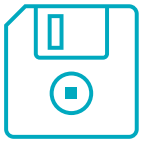
Le droit d'accès est le droit nécessaire à un utilisateur pour l'accès à des ressources : ordinateur, données, imprimante, etc.
On distingue les droits d'utilisateurs et d'administrateurs.

Utilisateurs : L'utilisation quotidienne de votre ordinateur *(lire les courriels, naviguer sur internet, utilisations des logiciels métiers…)*

Administrateurs : Ce compte est fortement stratégique. Il permet l'accès aux fondements des stratégies de sécurité. Il est donc important de définir à qui convient ce mode d'accès sans dérogations mûrement réfléchies.

Les sauvegardes

Point culminant de la sécurité, les sauvegardes offrent la seule certitude de récupération des données. S'assurer de leur pérennité est primordial. Externalisées dans le cloud ou sur support physique le choix du modèle et de la technologie conditionne le délai nécessaire à une reprise d'activité.



Il est primordial de prévoir un plan de reprise d'activité pour limiter les délais de retour à la production suite à une panne matérielle, panne logicielle, panne de backup, cyberattaque, erreur humaine, catastrophe naturelle, etc.

INFO'MAINTENANCE se chargera de vous conseiller et de vous installer les équipements nécessaires à vos sauvegardes sur sites ou externalisées.

L'accès Wifi

Partenaire indispensable du nomadisme des ordinateurs dans l'entreprise, le Wifi reste le maillon faible de la sécurité. Il est important de s'exempter du matériel tel que les box peu sécurisés des fournisseurs d'accès.

Les bornes Wifi professionnelles associées à des systèmes pare-feu et des switchs manageables permettent le bénéfice de l'utilisation du Wifi en toute sécurité.

Accès aux données en extérieur

Si vous êtes amenés à utiliser un ordinateur portable, une tablette ou un smartphone pour travailler lors de vos déplacements professionnels, il est important de mettre en place des règles de sécurité :

- ✓ Penser à sauvegarder vos fichiers avant de vous déplacer,
- ✓ Marquez vos appareils avec un signe distinctif pour les reconnaître en cas d'échange,
- ✓ N'utilisez pas de clé USB non validée par vos services informatiques *(Exemple : offerte lors d'un salon, publicitaire…)*,
- ✓ Refusez les partages de connexion simplifiés de la part d'un tiers,
- ✓ Évitez toutes transactions stratégiques à l'aide d'un Wifi public *(Exemple : transaction bancaire…)*,
- ✓ En règle générale, évitez toutes transactions bancaires en dehors du réseau sécurisé de votre entreprise,
- ✓ Rester vigilants sur la confidentialité des données que l'on consulte en zone publique *(utilisation éventuelle d'un filtre-écran)*.

Dans le cadre du télétravail, ne pas négliger la sécurisation des tunnels d'accès *(VPN, Pare-feu)*.

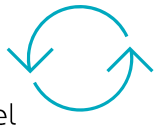
La messagerie

Au préalable :

- ✓ Vérifier l'identité du destinataire et la réalité de l'expéditeur,
- ✓ Ne pas ouvrir spontanément les pièces jointes et les liens de navigation,
- ✓ Penser à désactiver l'ouverture automatique des pièces jointes téléchargées,
- ✓ S'assurer de la qualité de son antivirus et de son antispam,
- ✓ Ne jamais transmettre par simple mail des données d'accès lier à des transactions de données sécurisées,
- ✓ Privilégier le doute à la certitude, il vaut mieux ne pas ouvrir un mail inoffensif que d'ouvrir un mail agressif.

Téléchargement

Avant de télécharger un contenu numérique, il faut vérifier la sécurité et la viabilité du site internet afin d'éviter l'installation de programmes malveillants pouvant contenir des virus ou des chevaux de Troie.



Soyez vigilants avant d'ouvrir un lien sponsorisé. Un pare-feu professionnel est le seul outil efficace pour se prémunir contre cet aspect du danger numérique.

Paiement sur internet

Devenus incontournables dans la vie de l'entreprise, les règlements directs par internet hors site bancaire doivent faire l'objet de précautions.
Avant de procéder à un paiement sur un site internet, il est important de vérifier les points suivants :

- ✓ Vérifier la présence d'un cadenas dans la barre d'adresse,
- ✓ La mention «https:// » doit apparaître,
- ✓ Toujours vérifier au préalable la réalité et l'intégrité du vendeur *(situation géographique, avis extérieurs, fautes d'orthographe, numéro de téléphone, possibilité de prise de commande traditionnelle…).*

Vous pouvez privilégier la méthode impliquant l'envoi d'un code de confirmation pour valider le paiement.
Si votre intuition est négative, n'effectuez pas l'achat.

Distinction entre le professionnel et le privé

Certaines entreprises appliquent le AVEC *(Apportez Votre Équipement de Communication)* ou BYOD *(Bring Your Own Device)* qui consiste à apporter votre matériel personnel pour une utilisation professionnelle. Elle s'avère très peu sécurisée en matière de protection de données *(vol ou perte des appareils, intrusions, manque de contrôle sur l'utilisation des appareils par les collaborateurs, fuite de données lors du départ du collaborateur)*. Nous déconseillons cette pratique qui permettrait aux enfants du propriétaire d'utiliser le même ordinateur le soir pour effectuer leurs travaux scolaires.

Nous vous recommandons de ne pas faire suivre vos courriels professionnels sur votre messagerie personnelle, de même pour vos données et pour la connexion de vos supports amovibles, sans avoir fait sécuriser cette pratique par un professionnel agréé.

En conclusion

En cas d'incident ou de doutes avérés, voici quelques bons réflexes à avoir :

- ✓ Déconnecter votre PC du réseau, mais ne l'éteignez pas,
- ✓ Déconnecter les médias de sauvegardes du réseau,
- ✓ Prévenir les services habilités,
- ✓ Contacter le support technique d'INFO'MAINTENANCE qui en tant que professionnel de la gestion et de la sécurisation des réseaux vous guidera dans la démarche à suivre.

INFO'MAINTENANCE professionnel référencé dans la lutte contre la cyber malveillance distribue et maintien les organes de sécurité en partenariat avec FORTINET, BITDEFENDER, VEEAM, AZURE, TITAN, et MICROSOFT.

FORTINET

veeam Value-Added Reseller Silver

TitanHQ SpamTitan

Bitdefender RESELLER BRONZE

Microsoft Azure

Microsoft Partner | Silver Solutions cloud pour les PME

INFO MAINTENANCE
INFORMATIQUE PROFESSIONNELLE

Les bonnes pratiques INFO'MAINTENANCE

Choisir des mots de passe complexes

Ne jamais ouvrir un mail / pièces jointes d'un destinataire suspect, toujours donner la priorité au doute

En cas de problème prévenir les services habilités

Effectuer des sauvegardes régulières des données décentralisées

Ne pas travailler en wifi non certifié privilégier le partage de connexion de votre téléphone en cas de doute

Installation d'un anti-virus / pare-feu / antispam professionnels

Verrouiller votre session lors de votre absence

Ne jamais divulguer d'informations confidentielles

Contacter le support technique d'INFO'MAINTENANCE en cas de problème ou de simple doute