MÉMO SÉCURITÉ

CHEF D'ENTREPRISE

ENTREPRISES ARTISANALES DU BTP ET DU PAYSAGE

LA CYBERSECURITÉ

Comment lutter contre le risque de cybercriminalité ?

L'utilisation quasi quotidienne des portables, ordinateurs, tablettes etc. multiplie le risque de cyberattaque. Il est important de mettre en place de bons réflexes afin d'en limiter les risques pour votre entreprise et pour vous.

IRIS ST
L'EXPERT SANTÉ-SÉCURITÉ
BY CAPEB & CNATP

LES DIFFÉRENTES MENACES

LOGICIEL MALVEILLANT OU MALWARE

Il s'agit de logiciels spécialement conçus dans le but d'endommager ou désactiver les ordinateurs et les systèmes informatiques (exemple : récupérer des informations personnelles, supprimer des fichiers, prendre le contrôle de votre ordinateur).

Comment ?
Un logiciel malveillant peut se trouver dans des logiciels de téléchargement gratuits (site web non fiable), dans une clé USB dont vous ne connaissez pas la provenance, dans une pièce jointe d'un mail.

HAMEÇONNAGE OU PHISHING

Personne qui se fait passer pour une personne de confiance (institution ou personne légitime) afin de soutirer des informations personnelles (exemple : données bancaires, mot de passe).

Comment ?
Par mail, appel téléphonique, sms, ou par le biais des réseaux sociaux. Le message contient généralement un lien qui dirige la victime vers un faux site web qui semble identique au site légitime.

VOL DE MOT DE PASSE

Utilisation d'un logiciel qui tentera un maximum de combinaisons possibles dans l'objectif de trouver votre mot de passe.

LES DIFFÉRENTES MENACES

RANÇONGICIEL OU RANSOMWARE

Logiciel malveillant qui bloque l'accès à vos fichiers ou à votre ordinateur en les chiffrant et qui réclame le paiement d'une rançon pour en obtenir de nouveau l'accès.

Comment ?
Si vous cliquez sur une pièce jointe ou un lien frauduleux, malveillant, parfois en navigant sur des sites compromis ou dû à une intrusion dans le système.

FRAUDE AU VIREMENT / FAUX RIB

Cela commence par le piratage de la messagerie. Le hacker va usurper l'identité du créancier et envoyer à ses contacts un mail avec la facture et un « faux rib » contenant les informations bancaires d'un autre compte pour dérober l'argent.

WIFI OUVERT ET GRATUIT

Des réseaux wifi ouverts à tous et qui sont piégés. Les victimes se connectent dessus ce qui permet au hacker d'accéder à l'ensemble des informations que vous consultez.

VICTIME DE CYBERATTAQUE

Le site du gouvernement www.cybermalveillance.gouv.fr met à votre disposition un dispositif d'aide et d'orientation des victimes. Leur outil vous proposera un diagnostic, des conseils personnalisés et si nécessaire, vous mettra en contact avec un spécialiste. Vous y trouverez également plein de conseils.

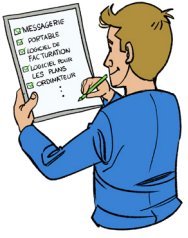
L'ENTREPRISE

CYBERATTAQUE, LES CONSÉQUENCES POUR L'ENTREPRISE

- Perte immédiate d'argent (ex : la fraude au RIB).
- Perte d'exploitation, avec l'arrêt de l'entreprise pendant plusieurs jours suite par exemple au cryptage de données.
- Perte des données clients, fournisseurs, salariales ...
- Des coûts directs et indirects :
  - Remise en état du système / coût de reconstruction des informations perdues (ex : fichier client, la facturation, devis etc).
  - Parfois des coûts liés à la perte de confiance des clients par exemple.

RÉALISER UN ÉTAT DES LIEUX DE VOS SYSTÈMES NUMÉRIQUES

- De quels équipements/logiciels disposez-vous ?
- Quelle information vous permettent-ils d'avoir ?
- Que se passerait-il si ces informations me sont volées ou détruites ?
- Quelles mesures ai-je prises pour essayer d'empêcher un hacker d'accéder à chacun de ces éléments (mot de passe, anti-virus, mise à jour des logiciels...) ?



Cet état des lieux vous permet d'avoir une vision globale de vos informations et solutions mises en place et les potentielles améliorations.

BON À SAVOIR

La responsabilité juridique civile et pénale du chef d'entreprise peut être engagée en cas de manquement à ses obligations de protection des informations à caractère personnel et des systèmes informatiques.

LES BONNES PRATIQUES

LE RISQUE ZÉRO N'EXISTE PAS, CEPENDANT UN CERTAIN NOMBRE DE BONNES PRATIQUES SONT À METTRE EN PLACE POUR LIMITER LES RISQUES.

- **Doute sur le destinataire :** ne cliquez pas sur la pièce jointe et/ou sur le lien figurant dans le mail.
- **Demande de payer une facture avec un RIB en pièce jointe :** appelez la personne pour qu'elle vous confirme l'envoi du mail avec un nouveau RIB. Ne pas demander par mail car si sa boite mail est piratée c'est le hacker qui vous répondra.
- **La mise à jour de vos logiciels et ordinateurs.** Ces mises à jour visent notament à corriger les failles de sécurité des systèmes. Méfiez-vous des fausses mises à jour en naviguant sur Internet, il arrive que des messages prenants l'apparence d'alertes de mises à jour apparaissent à l'écran. Il peut s'agir d'une technique pour vous inciter à installer une prétendue mise à jour qui serait en réalité un virus.
- **Vigilance lorsque vous naviguez sur le web :** site « https », pour tout paiement en ligne, avoir le logo du cadenas fermé.
- La mise en place d'un anti-virus.
- Dans les espaces publics, ne pas se connecter au wifi ouvert et gratuit ou sinon seulement pour faire des recherches internet mais ne vous connectez à aucun compte professionnel ou personnel. Privilégiez l'utilisation de votre 4G ou 5G dans les espaces publics.

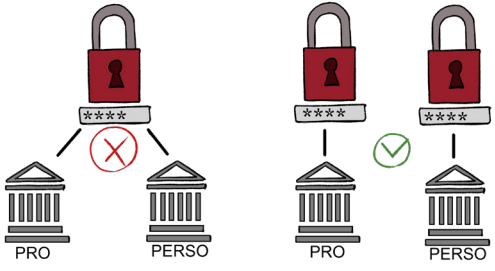
PENSEZ-Y !

Les cyber criminels savent vous mettre en situation de stress ! Gardez votre calme en cas de mail frauduleux incitant à cliquer sur un lien pour mettre à jour des données personnelles (carte vitale, rib, compte CPF, paiement sur une plateforme…).

LES USAGES PRO - PERSO

LES TABLETTES, ORDINATEURS ET TÉLÉPHONES PORTABLES PERMETTENT D'ACCÉDER, DEPUIS PRESQUE N'IMPORTE OÙ, À NOS INFORMATIONS PERSONNELLES MAIS AUSSI À NOS SYSTÈMES INFORMATIQUES PROFESSIONNELS. LA DISTINCTION PRO-PERSO EST DE MOINS EN MOINS PRÉSENTE. QUELQUES MESURES SONT À METTRE EN PLACE :

- Si vous utilisez le même ordinateur, si possible, créer deux sessions; une personnelle et une pour le travail. Il est toutefois préférable d'utiliser un ordinateur pour le travail et un ordinateur pour la vie privée.
- Utilisez des mots de passe différents pour les services professionnels et personnels.
- Dissociez votre messagerie professionnelle et votre messagerie personnelle.
- Méfiez-vous des supports USB : Si vous en avez besoin, utilisez une clé USB dédiée aux affaires professionnels et une autre dédiée aux affaires personnelles. Ne jamais brancher une clé USB dont vous ne connaissez pas la provenance sur votre ordinateur.



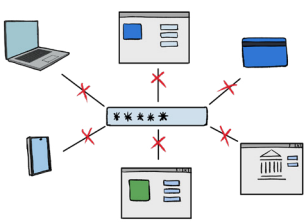
- Si vous utilisez des services de stockage en ligne d'information (Cloud), dissocier les informations professionnelles et privées. Ne pas les stocker au même endroit.

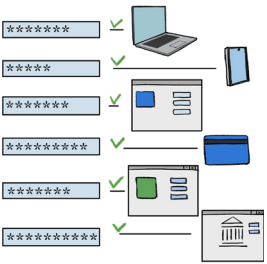
LES MOTS DE PASSE

LA CONSULTATION DES SERVICES EN LIGNE ET DES APPLICATIONS (MESSAGERIE, BANQUE, ASSURANCE, RÉSEAUX SOCIAUX…) NÉCESSITE L'UTILISATION DE MOTS DE PASSE POUR SÉCURISER LEURS ACCÈS.

Cette multitude de mots de passe peut vous inciter à vouloir mettre le même mot de passe, pour plusieurs services différents. Or en cas de piratage d'un mot de passe le malfaiteur aura accès à l'ensemble des sites ayant le même mot de passe.

- Ne notez pas vos mots de passe sur une feuille de papier, dans vos notes de téléphone etc.
- Ne communiquez jamais votre mot de passe à un tiers.
- Si possible, activez la double authentification. En plus de votre mot de passe, certains sites vous envoient un code par mail ou sms vous permettant de confirmer l'accès à votre compte.
- Changez votre mot de passe au moindre soupçon.
- Evitez d'utiliser vos comptes nécessitant des mots de passe sur les ordinateurs partagés (ordinateur dans des hôtels, cybercafé), sinon mettez-vous en navigation privée pour laisser le moins de trace.





LES MOTS DE PASSE

- Evitez les mots de passe faciles, avec des informations que pourraient trouver les malfaiteurs sur les réseaux sociaux par exemple (prénom des personnes de votre famille, animal de compagnie, code postal...) ou des mots de passe courants (ex : azerty1 ou abcde...). Utilisez des mots de passe longs et complexes, c'est-à-dire mélanger majuscule, minuscule, chiffre, caractères spéciaux. Un mot de passe pas suffisamment robuste est démasqué en quelques secondes.

PENSEZ-Y !

Apple, par exemple, propose de vous générer des mots de passe complexes automatiquement lorsque vous devez créer un nouveau compte sur un site / application.

IL EXISTE DIFFÉRENTES ASTUCES POUR CRÉER UN MOT DE PASSE :

- **La méthode des premières lettres**
  Un tien vaut mieux que deux tu l'auras » = 1tvmQ2tl'A
- **Méthode phonétique**
  J'ai acheté huit CD pour cent euros cet après-midi = ght8CD%E7am

- Trouvez votre propre méthode pour créer des mots de passe robustes.
- Utilisez un gestionnaire de mot de passe qui retiendra l'ensemble de vos mots de passe.

BON À SAVOIR

KEEPASS est un gestionnaire de mot de passe sécurisé, gratuit et en français. Ce logiciel permet de stocker en sécurité vos mots de passe pour les utiliser dans vos applications. Il dispose aussi d'une fonction permettant de générer des mots de passe complexes aléatoires.

LA SAUVERGARDE

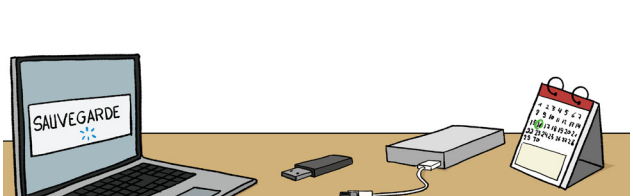
SUITE À VOTRE ÉTAT DES LIEUX DES APPAREILS ET SUPPORTS QUI CONTIENNENT DES DONNÉES, DÉTERMINEZ CELLES QUI DOIVENT ÊTRE SAUVEGARDÉES ET LES HIÉRARCHISER.

Vous pouvez vous poser les questions suivantes :

- Quelles données peuvent être récupérées ailleurs en cas de perte ?
- Quelles sont les données que je consulte régulièrement ou celles qui me sont le plus souvent demandées ?

Déterminez le support de sauvegarde :

- Outil de sauvegarde physique (clé usb / disque dur externe).
- Outil de sauvegarde en ligne (Cloud).



Réalisez des sauvegardes régulières et si besoin, pensez à planifier vos sauvegardes.

PENSEZ-Y !

Pour les données importantes, on recommande 3 sauvegardes :
le fichier original + 2 copies.

EN SAVOIR PLUS

IRIS-ST, pôle prévention des artisans du BTP et Paysage
www.iris-st.org

Avec le soutien de la CNAM et de Béranger Développement

L'Assurance Maladie – Risques professionnels

Développement Béranger

RETROUVEZ LES MÉMOS DE L'IRIS-ST SUR L'APPLICATION « LES MÉMOS ».

ANDROID **APPLE**

IRIS-ST
2 RUE BÉRANGER
75003 PARIS

IRIS ST – L'expert santé-sécurité by CAPEB & CNATP

Rédigé par l'IRIS-ST en collaboration avec les métiers de la CAPEB et CNATP