Les bonnes pratiques de la cybersécurité au travail

Aujourd'hui, nous utilisons tous des outils numériques au travail, que ce soit pour envoyer des emails, stocker des documents ou accéder à des applications. Mais saviez-vous qu'une simple erreur peut ouvrir la porte à une cyberattaque ? Un mot de passe faible, un email piège ou un logiciel non mis à jour peuvent suffire à compromettre les données de votre entreprise. Heureusement, il existe des gestes simples pour vous protéger.

Choisissez des mots de passe solides et uniques

Un mot de passe comme "123456" ou "password" est une invitation aux pirates informatiques. Privilégiez plutôt l'utilisation d'une "phrase de passe", c'est-à-dire une phrase personnelle qui ne soit pas courante, mais facile à retenir pour vous, comme: "En2025,JePrendsMonCafeSansSucreEtAvecUneToucheDeCannelle!". Ces phrases longues sont beaucoup plus difficiles à deviner pour les hackers, car elles comportent plus de caractères tout en étant simples à retenir. Et surtout, utilisez un mot de passe différent pour chaque compte ! Pour ne pas les oublier, un gestionnaire de mots de passe peut vous aider.

Activez l'authentification à deux facteurs (2FA)

Imaginez que quelqu'un vole la clé de votre maison, mais qu'il ait besoin d'un second code pour entrer. C'est exactement ce que fait l'authentification à deux facteurs : même si un pirate a votre mot de passe, il lui manquera une étape pour accéder à votre compte. Tous les comptes doivent être munis d'une authentification à deux facteurs, soit par SMS pour confirmer chaque connexion, soit en utilisant une application comme Google Authenticator ou Microsoft Authenticator. Cette couche de sécurité supplémentaire empêche les intrus d'accéder à vos informations, même s'ils récupèrent votre mot de passe.

Méfiez-vous des emails suspects

Si vous recevez un email qui semble urgent et vous demande de cliquer sur un lien ou de partager des informations personnelles, faites une pause. Les cybercriminels imitent souvent des entreprises connues pour vous piéger. Si vous avez un doute, contactez directement l'expéditeur sans utiliser les informations de l'email. De plus, si une personne vous demande un service inhabituel par email, cherchez à la joindre par un autre moyen pour obtenir une confirmation avant de cliquer sur un lien ou d'envoyer des informations personnelles.

Association Des Experts en Sécurité et Sûreté - ADESS
4, allée des augustins 92390 Villeneuve-la-Garenne
contact@adess-france.fr
www.adess-eu.org

Faites vos mises à jour régulièrement

Un logiciel non mis à jour, c'est comme une maison avec une fenêtre cassée : les pirates peuvent s'y infiltrer. Assurez-vous que votre ordinateur, vos applications et votre antivirus sont toujours à jour. Activez les mises à jour automatiques pour ne pas oublier.

Sauvegardez vos fichiers importants

Un bug, une cyberattaque ou un vol d'ordinateur peuvent entraîner la perte de documents essentiels. Enregistrez régulièrement vos fichiers sur un disque dur externe ou un service cloud fiable. Ainsi, même en cas de problème, vous ne perdrez pas tout.

Partagez les informations sensibles avec prudence

Ne laissez pas traîner de documents confidentiels accessibles à tout le monde. Par exemple, évitez d'envoyer des données sensibles par email sans protection. Si vous devez partager un document important, utilisez un service sécurisé avec un mot de passe.

Sensibilisez vos collègues

Un simple clic sur un lien malveillant peut affecter toute une entreprise. Discutez de ces bonnes pratiques avec vos collègues et participez aux formations sur la cybersécurité. Plus tout le monde est informé, plus les risques diminuent. La cybersécurité ne concerne pas uniquement l'équipe SSI, elle est l'affaire de tous. Il est donc essentiel de se tenir à jour sur les formations en sécurité pour mieux anticiper les menaces. Les sensibilisations peuvent aussi passer par des CyberGames, des exercices ludiques permettant d'améliorer sa maturité cyber tout en s'amusant.

Protégez votre connexion, surtout en télétravail

Travailler dans un café ou un aéroport peut être agréable, mais les réseaux Wi-Fi publics ne sont pas toujours sécurisés. Si vous devez les utiliser, activez un VPN (un outil qui chiffre votre connexion) pour éviter que des personnes malintentionnées interceptent vos données. De plus, lors de vos déplacements, notamment en train, ne laissez jamais votre ordinateur de travail sans surveillance. Si vous devez vous absenter, par exemple pour aller aux toilettes, verrouillez votre session et rangez votre PC en lieu sûr jusqu'à votre retour pour éviter tout risque de vol ou d'accès non autorisé.

Respectez les règles de votre entreprise

Les entreprises mettent en place des politiques de cybersécurité pour protéger leurs données. Respectez-les en évitant d'utiliser des clés USB inconnues, en verrouillant votre ordinateur quand vous vous absentez et en signalant toute activité suspecte. Attachez toujours votre PC

avec une corde de sécurité et verrouillez votre session à chaque déplacement. Si vous manipulez des documents sensibles, veillez à fermer les tiroirs à clé, retirez la clé et conservez-la sur vous. Ne laissez jamais de documents sensibles traîner sur une imprimante. La politique de cybersécurité n'est pas seulement un document à lire lors de votre arrivée en entreprise, mais un ensemble de règles à respecter au quotidien. En appliquant ces bonnes pratiques et en accompagnant l'équipe SSI dans la protection des données et des actifs de l'entreprise, chacun contribue activement à la sécurité numérique.

La cybersécurité n'est pas une affaire réservée aux experts. Chacun d'entre nous a un rôle à jouer pour protéger les données de l'entreprise. Un simple oubli ou un clic maladroit peut avoir de grandes conséquences, comme la perte d'informations importantes ou une fraude financière. La cybersécurité est donc l'affaire de tous en entreprise. En adoptant ces bons réflexes et en les partageant avec vos collègues, vous contribuez à rendre votre environnement de travail plus sûr. Restons vigilants et protégeons ensemble nos données !

Ibrahima BAH - ID : 13245757