GUIDE

Bonnes pratiques pour sécuriser ma messagerie

01 SENSIBILISER

Et oui ! La règle de sécurité la plus importante est de sensibiliser un maximum vos collaborateurs. Sachez que la vulnérabilité la plus grande dans une entreprise est l'utilisateur. Une fois vos contacts avertis, le risque de cyberattaque sera fortement diminué. Alors, n'hésitez pas à partager cette infographie !

02 UTILISER UN MOT DE PASSE ROBUSTE

Un mot de passe simple peut être piraté en quelques secondes. Nous vous recommandons d'en choisir un difficile à déchiffrer. Pour cela, il doit comporter 12 caractères avec au moins 3 caractères spéciaux, ne comporter aucune donnée personnelle (date de naissance, nom, prénom...), être unique et mis à jour fréquemment et ne surtout pas être communiqué par email. Vous trouvez ça contraignant ? Sachez qu'il existe des générateurs de mot de passe robuste et des gestionnaires qui permettent de les garder en mémoire comme KeePass.

03 FAIRE LES MISES À JOUR

Les mises à jour corrigent les failles de sécurité au fur et à mesure de leur détection, c'est pour cela qu'il est important de mettre à jour chaque logiciel lié à votre messagerie. Activez la procédure de mise à jour automatique pour plus de tranquillité.

04 NE PAS FAIRE CONFIANCE AU NOM ET À L'ADRESSE EMAIL DE L'EXPÉDITEUR

Votre adresse email peut être utilisée pour envoyer un virus sans que vous ne vous en rendiez compte. Cette technique s'appelle l'usurpation d'identité numérique. Les spammeurs cachent leur identité en utilisant une adresse email connue du destinataire dans le but de le tromper. Ils ciblent des collaborateurs pour accéder à des données sensibles comme des comptes bancaires ou pour détourner des fonds. Des actes qui peuvent porter atteinte à la réputation de votre entreprise.

05 FAIRE ATTENTION AUX PIÈCES JOINTES

Ce sont souvent dans les pièces jointes que se cachent les virus ou des logiciels espions. Un CV, une photo, un document (zip, pdf, jpg, exe, word...), n'importe quel fichier peut contaminer tout un système après une simple ouverture.

06 SE MÉFIER DES LIENS

En cas de lien dans un message douteux, vous pouvez vérifier sa validité en le survolant avec votre souris, le lien cliquable s'affiche au-dessus de votre curseur. Dans le cas d'un email frauduleux, les deux liens seront différents.

07 NE JAMAIS RÉPONDRE À UNE DEMANDE D'INFORMATIONS CONFIDENTIELLES

Une demande d'informations confidentielles légitime (mots de passe, code PIN, coordonnées bancaires...) ne se fait jamais par email ! Si vous recevez ce type de demande de votre directeur, un collaborateur ou bien un service en ligne, sachez que vous êtes victime d'une tentative d'escroquerie. Les pirates se servent de toutes vos données, jusqu'aux réseaux sociaux pour vous tromper.

08 RESTER VIGILANT

Soyez attentif à tout indice mettant en doute l'origine réelle de l'email. Vérifiez la cohérence entre l'expéditeur et le contenu. Vérifiez également la qualité du langage utilisé. Des fautes d'orthographe, de grammaire ou des caractères mal accentués peuvent indiquer un email frauduleux. Toutefois, on constate un nombre croissant d'attaques employant un français correct. Alors, en cas de doute, ne relayez surtout pas le message, demandez à votre correspondant légitime de confirmer sa demande ou informez votre DSI.

09 SE DOTER D'UN ANTI-SPAM | ANTI-VIRUS DE MESSAGERIE

Plusieurs types de solutions existent pour faire face à une cyberattaque. À la différence d'un système anti-spam ou anti-virus classique, Mailinblack combine les technologies en intégrant des filtres traditionnels de sécurité, de l'analyse prédictive, de l'intelligence artificielle et de l'intelligence humaine grâce au principe d'authentification des expéditeurs. Ne prenez plus aucun risque pour votre entreprise : Mailinblack sécurise votre messagerie contre toutes formes de virus, stoppe les emails indésirables de type spams et trie automatiquement les newsletters. Vous retrouvez enfin une messagerie propre et sécurisée, sans aucune perte d'email.

MAILINBLACK