VAINCRE LE COVID-19 : ON DOIT TOUS Y TRAVAILLER

LE MEDEF VOUS ACCOMPAGNE PENDANT LA CRISE COVID-19

CHEFS D'ENTREPRISE : VEILLEZ À LA CYBERSÉCURITÉ

La crise sanitaire et les mesures de confinement ont obligé les entreprises à mettre très rapidement en place du télétravail généralisé. Il est important de noter que contrairement au télétravail qui se pratique habituellement en entreprise, celui-ci est subi et non choisi, qu'il se fait à temps plein et pour une durée illimitée, qu'il est généralisé à l'ensemble des équipes quand le métier le permet (hors chômage partiel) et qu'il est accompli à domicile avec parfois d'autres membres de la famille ou de l'entourage. Autant dire qu'il n'a rien à voir avec le télétravail serein qui aurait dû être la norme…

Comme à chaque événement exceptionnel, il faut avoir conscience que les cybercriminels cherchent à tirer profit de la précipitation et de la baisse de vigilance des personnes directement ou indirectement concernées pour les abuser et qui va se retrouver amplifiée par l'accroissement de l'usage numérique lié aux mesures de confinement. Il est donc primordial de redoubler d'attention pour ne pas tomber dans leurs pièges.

En cas de cyberattaque ou pour tout conseil sur la cybersécurité :
Cybermalveillance.gouv.fr
avec notamment un kit de sensibilisation à disposition.

Ne baissez pas la garde, au contraire, montez-là !

L'activité des entreprises et des organisations est déjà impactée par la crise du Covid-19. La préservation des actifs doit donc relever de la priorité de tous et aux premiers rangs desquelles la préservation de la sécurité des systèmes d'information qui sont souvent au cœur de leur fonctionnement. Une intensification des cybers-attaques de type « vol de données » et/ou rançongiciels (ransomware) sur les réseaux d'entreprises, cherchant à jouer sur leur possible baisse de vigilance ou défaut d'organisation, est donc prévisible. Les mesures de sécurité visant à détecter ou éviter les cyberattaques doivent donc être renforcées : mises à jour de sécurité, renforcement des procédures d'authentification pour le télétravail, supervision de sécurité, sensibilisation du personnel.

Soyez attentifs aux fausses commandes ou aux modifications de virements bancaires frauduleux :

L'accroissement de l'usage du télétravail et de la dématérialisation des procédures qui en découlent, associé aux difficultés économiques inhérentes à la situation de crise du Covid-19 présentent un risque accru d'escroqueries à la fausse commande ou aux modifications de coordonnées de virement bancaire (FOVI/BEC) en usurpant l'identité d'un employé pour récupérer son salaire ou d'un fournisseur pour régler les factures ou encore émanant d'un dirigeant sous le sceau du secret. Avant toute prise en compte de commande suspecte, de demande de changement de RIB ou de demande de virement « exceptionnel », faites confirmer en contactant directement le demandeur et faites valider l'opération par votre hiérarchie.

Appliquez les gestes élémentaires de cybersécurité pour rester protégés :

- Ne vous précipitez pas et prenez toujours le temps de la réflexion/confirmation
- Faites régulièrement des sauvegardes de vos données (ordinateurs, téléphone…) et gardez en une copie déconnectée
- Appliquez les mises à jour de sécurité sur vos équipements connectés (serveurs, ordinateurs, téléphones…) dès qu'elles sont disponibles
- Utilisez des mots de passe uniques et solides et activez la double authentification chaque fois que possible.

Quelques règles essentielles à transmettre à vos collaborateurs pour prévenir les risques au quotidien :

Choisir avec soin ses mots de passe et les garder confidentiels :
Astuce 1 : choisir 12 caractères de types variés (ex : « J'ai acheté 5 CDs pour cent euros cet après-midi » = ght5CDs%E7am)
Astuce 2 : Ne jamais inscrire ses mots de passe sur un post-it, même bien caché

Séparer les usages personnels des usages professionnels :
Astuce : ne pas héberger de données professionnelles sur ses équipements personnels (clé USB, téléphone, etc.) ou sur des moyens personnels de stockage en ligne

Prendre soin de ses informations personnelles, professionnelles et de son identité numérique :
Astuce : utiliser plusieurs adresses électroniques : une réservée aux activités sécurisées (banques, recherche d'emploi…) et l'autre destinée aux loisirs.

Être aussi prudent avec son smartphone/tablette qu'avec son ordinateur :
Astuce 1 : ne jamais préenregistrer ses mots de passe ou utiliser un gestionnaire de mots de passe
Astuce 2 : verrouiller systématiquement sa session avant de quitter son poste informatique

Être prudent lors de l'utilisation de sa messagerie :
Astuce : désactiver l'ouverture automatique des documents téléchargés et lancer une analyse antivirus avant de les ouvrir

Bien connaitre ses utilisateurs et ses prestataires :
Lorsque vous accédez à votre ordinateur, vous bénéficiez de droits d'utilisation plus ou moins élevés sur celui-ci. On distingue généralement les droits dits « d'utilisateur » et les droits dits « d'administrateur »
Astuce : prendre un compte utilisateur pour l'usage quotidien de son ordinateur (naviguer sur Internet, etc.) et restreindre l'utilisation du compte administrateur

Être vigilant lors d'un paiement sur Internet :
Astuce : s'assurer que la mention « https:// » (et non « http:// ») apparait au début de l'adresse du site Internet et vérifier sa fiabilité en prenant garde aux fautes d'orthographe par exemple

Effectuer des sauvegardes régulières :
Astuce : les cloud (stockage en ligne) peuvent aussi faire l'objet de cyberattaques, effectuer des sauvegardes sur un périphérique extérieur (ex : disque dure externe)

Mettre à jour ses logiciels, y compris les antivirus :
Astuce : effectuer régulièrement les mises à jour et faire en sorte qu'elles puissent s'installer automatiquement

Télécharger ses programmes sur les sites officiels des éditeurs :
Astuce : éviter les téléchargements de contenus annexes (logiciels complémentaires, toolbars, etc.)

Sécuriser son accès Wifi :
Astuce : modifier dès la première connexion le mot de passe de connexion à la borne Internet

RESSOURCES :

- Guide de l'Agence nationale de sécurité des systèmes d'information (ANSSI) sur le nomadisme numérique

- Test cybersécurité du MEDEF à destination des chefs d'entreprise pour tester son niveau de connaissance des enjeux de cybersécurité, avec des guides et bonnes pratiques à disposition.

- Le guide complet des bonnes pratiques de l'informatique de l'ANSSI.