Charte de bonnes pratiques en sécurité économique

Solutions&co souhaite sensibiliser son personnel au respect de bonnes pratiques qui participent à la sécurité économique de notre entité. Cette liste n'est évidemment pas exhaustive. Pour aller plus loin : https://sisse.entreprises.gouv.fr/fr/outils/la-securite-economique-au-quotidien-26-fiches-thematiques

Je travaille

Je verrouille mon poste quand je m'éloigne de mon ordinateur + L

Je gère correctement mes mots de passe : choix, renouvellement, protection, non-divulgation.

Je récupère rapidement les documents sortis de l'imprimante ou je les stocke (fichiers enregistrés).

J'utilise les outils préconisés par l'Informatique. ex : Onedrive Vs We Transfer/Drop Box, Teams Vs Zoom

Je redouble de vigilance en télétravail car l'environnement de mon poste est moins sécurisé

Je consulte de préférence ma boite email personnelle sur mon smartphone personnel.

Je n'ouvre pas spontanément des liens ou des pièces jointes dans des emails, sans lien avec mon activité, même provenant de mes collègues.

J'informe le service Informatique d'emails suspectés frauduleux et des alertes de l'antivirus.

Je suis prudent(e) sur les réseaux sociaux professionnels. Je n'accepte pas dans mon réseau des personnes que je ne connais pas.

Je reçois des visiteurs

Je vais les chercher à l'accueil et je les raccompagne jusqu'à la porte d'entrée du bâtiment.

Je les reçois idéalement dans une salle de réunion.

Je partage uniquement l'information utile à un projet avec des partenaires.

J'encadre les personnels temporaires et stagiaires afin qu'ils aient un accès limité aux ressources.

Bonus : j'interpelle des visiteurs seuls dans les locaux.

Je pars en déplacement

Je conserve le verrouillage automatique de mon smartphone professionnel.

J'utilise un filtre de confidentialité dans les transports, les lieux publics et si nécessaire en réunion.

Je ne quitte pas mon ordinateur et mon smartphone et je ne les prête à personne.

J'évite d'emporter des supports amovibles pendant mes déplacements.

Je coupe le wifi et le bluetooth de mon ordinateur et de mon smartphone dans les lieux publics.

Je sécurise la connexion à un wifi public en activant mon VPN.

Je refuse de connecter à mon ordinateur des supports amovibles de tiers de non-confiance.

J'évite de parler de sujets professionnels dans les transports en commun et les espaces publics.

Des exemples de cyberattaques

Les conséquences d'attaques peuvent être graves pour les entreprises. Voici quelques exemples de cyberattaques identifiées dans l'actualité des entreprises ligériennes :

☛LACTALIS *(53, collecte, négoce et transformation de produits laitiers)*
Le 26 février 2021, le groupe agroalimentaire Lactalis a été victime d'une cyberattaque. Une intrusion a été détectée sur une partie du réseau informatique. Par mesure de précaution, Lactalis a restreint son accès au réseau internet public.

☛BENETEAU *(85, constructeur de bateaux)*
Dans la nuit du 18 au 19 février 2021, le groupe vendéen a détecté l'intrusion d'un logiciel malveillant sur certains de ses serveurs. Par mesure de précaution, l'ensemble des systèmes d'information a été déconnecté pour éviter toute propagation.

☛FLEURY MICHON *(85, fabrication de charcuterie, de plats cuisinés)*
En avril 2019, la production de plusieurs sites vendéens de Fleury Michon a été mis à l'arrêt en raison d'un virus informatique, ayant touché les installations de l'entreprise. Le virus aurait notamment bloqué l'édition des bons de livraison, empêchant l'expédition des produits.

☛EUROFINS *(44, laboratoire d'analyse biologique)*
Eurofins, a été victime d'un rançongiciel en juin 2019. Il a fallu deux semaines à l'entreprise pour que la plupart des opérations du groupe reprennent normalement.

☛MMA *(72, assurances)*
Le 17 juillet 2020, la MMA a été victime d'une cyberattaque. L'entreprise a pris la décision d'arrêter les serveurs pour limiter la contagion. La remise en route a demandé une dizaine de jours. Tous les serveurs ont ensuite été auscultés, ainsi que les ordinateurs du personnel.

☛FOUSSIER *(72, quincaillerie, outillage et fixation)*
L'entreprise a été victime d'une attaque informatique le 24 juillet 2020. Cela a eu pour effet de paralyser l'entreprise ainsi que le site internet jusqu'au système de communication. En collaboration avec le prestataire informatique de l'entreprise et avec l'implication de nombreux salariés, les équipes de cybersécurité ont réussi à remettre progressivement en fonction les systèmes.

☛EOLANE *(49, électronique)*
En septembre 2020, le groupe Eolane a été victime d'une attaque informatique. Cette dernière a rapidement été stoppée et n'aurait pas causée de dommages majeurs. Tous les ordinateurs ont dû être vérifiés. En conséquence, une partie du personnel a été placée au chômage partiel pour quelques jours.

La sphère publique n'est pas épargnée :

☛**Angers Ville et Métropole**
En janvier 2021, une cyberattaque de type rançongiciel a ciblé le système d'information de la ville d'Angers et de la métropole. De nombreux services rendus aux usagers ont été affectés par la panne occasionnée par les pirates informatiques et par le fait que les services municipaux ont préféré couper certains serveurs pour éviter que le virus ne s'y propage et que la situation ne s'aggrave.

☛**Mairie de Suze-sur-Sarthe**
En janvier 2021, l'adresse e-mail de la mairie a été piratée. La collectivité a été victime d'un acte de cybermalveillance. Des milliers de mails auraient été envoyés dans toute la France.

☛**Mairie de Bouchemaine**
La municipalité a alerté fin janvier 2021 sur la diffusion de mails frauduleux concernant la mise à disposition de vaccins contre la COVID 19. L'e-mail indiquait que de nouveaux vaccins étaient disponibles et invitait à cliquer sur un lien pour prendre rendez-vous. La mairie a été victime d'une usurpation d'identité.