9. INTERNET

Un formidable outil de productivité mais qui peut apporter son lot de problèmes.

Internet est-il forcément votre ami ?

- Internet est peuplé d'inconnus qui sont tous vos "amis" !
- Internet n'est pas sans foi ni loi.
- Le droit du monde réel s'applique à l'Internet.
- Ne pas aller sur des sites à risques (utiliser un outil comme WOT pour être informé).
- Attention aux propositions alléchantes, la gratuité n'existe jamais, même sur Internet !
- La plupart des fichiers sur les sites de téléchargements illégaux intègrent des programmes malveillants.
- Évitez d'avoir un comportement à risque.
- Ne pas installer n'importe quoi sur votre ordinateur.
- Les logiciels gratuits ou piratés intègrent souvent des logiciels malicieux ou des failles de sécurité.

10. SENSIBILISATION

Vous êtes conscient de l'importance de la sécurité et motivé à la mettre en place.

Et vos collaborateurs ?

Votre personnel a-t-il conscience des risques ?

- Soyez conscients que les utilisateurs sont le maillon faible.
- Pensez à donner des règles de base.
- Pensez à faire signer une charte informatique (charte d'utilisation des moyens informatiques).
- Ne confondez pas usage privé et usage professionnel des outils informatiques (ordinateurs portables, smartphones...).
- Attention à la divulgation de données professionnelles.
- Communiquez régulièrement sur les risques et les nouveaux dangers.

11. LES RÉSEAUX SOCIAUX

Les internautes se dévoilent souvent imprudemment sur les réseaux sociaux, compromettant ainsi gravement la sécurité et donc la prospérité de leur entreprise.

La concurrence sait tout le profit qu'elle peut tirer de cette manne d'information.

La divulgation non autorisée de projets en cours ou d'informations sensibles et stratégiques peut porter atteinte aux intérêts de l'entreprise et constituer une faute professionnelle grave.

Quelques règles :

- Ne mettez pas d'informations trop personnelles (date de naissance, adresse, n° de téléphone, photos de vous ou de vos proches...).
- Soyez vigilants quant aux sollicitations reçues à travers les réseaux sociaux (supposées amies).
- Créez une adresse courriel spécifique.
- Évitez les mots de passe facilement devinables (ex : quel est votre sport favori ?)
- Évitez les groupes de commentaires qui pourraient engager votre responsabilité pénale (diffamation, négationnisme, racisme, xénophobie, pédophilie, ...).
- Restez discrets sur vos activités professionnelles.
- Ne mettez jamais de commentaires ou de photos que vous pourriez regretter dans un autre cadre que celui des réseaux sociaux.

Vos correspondants :

☎ : 03.80.70.65.64
: eco.rgbourg@gendarmerie.interieur.gouv.fr

DIRECCTE
☎ : 03.80.76.29.44
: bourg.intel-eco@direccte.gouv.fr

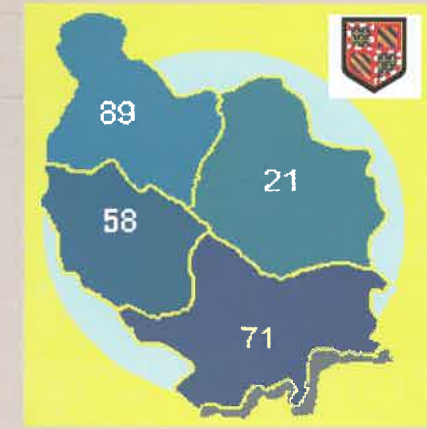
☎ : 03.80.44.57.10
: intel.eco-dijon@interieur.gouv.fr

dpsd
☎ : 03.80.11.23.27
: bur.etude@wanadoo.fr

SDIG 12-30483-10 000

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
PRÉFET DE LA RÉGION BOURGOGNE

SECURITE DES ENTREPRISES



Même si la sécurité à 100 % n'existe pas, certaines recommandations de base sont utiles pour se protéger des risques les plus courants.

Les PME-PMI sont particulièrement vulnérables tant en matière d'intrusion physique que vis-à-vis des attaques informatiques visant à récupérer des données sensibles ou à paralyser leur système d'information.

1. INVENTAIRE DU PATRIMOINE

Bien identifier les données vitales de l'entreprise.

Quelles sont les données vitales pour votre société ?

- Documents (bureautique, financiers, marketing …).
- Listes de clients, fournisseurs…
- Images, vidéos, favoris de votre navigateur.
- Brevets, plans, courriels.

2. ACCÈS PHYSIQUES

Ne laissez pas certains secteurs de l'entreprise en libre accès.

Pensez-vous à fermer les portes et les fenêtres ?

- L'accès physique à votre entreprise doit être contrôlé.
- Les locaux informatiques, techniques, recelant des informations sensibles et stratégiques doivent faire l'objet d'une attention particulière (accès par clé et/ou par badge, traçabilité, nombre réduit de personnes habilitées, coffre-fort, alarme, vidéo protection).
- Privilégiez les bureaux sans-papier le soir, le week-end et pendant les vacances.
- Utilisez des broyeurs de papier pour les documents confidentiels.

3. PRESTATAIRES

Travailler ensemble, c'est une confiance à mettre en place et des règles à suivre.

Avez-vous pris toutes les précautions vis-à-vis de vos partenaires ?

- Accord de confidentialité.
- Charte informatique.
- Attention aux données à caractère personnel auxquelles ils pourraient avoir accès.
- Attention à l'accès Internet.
- Ne laissez pas des prestataires seuls dans vos locaux notamment les locaux informatiques.
- Attention aux accès distants pour la maintenance (serveurs, centraux téléphoniques, photocopieurs…).
- Attention aux prestataires travaillant pendant les heures et jours non-ouvrés.

4. VISITES CONSENTIES

Quelles précautions prendre avant de faire visiter vos locaux ?

- Assurez-vous de l'identité des visiteurs. Qui les emploie, quelles sont leurs motivations ?
- Identifiez les visiteurs avec un badge spécifique.

- Interdisez l'utilisation de téléphone portable ou autres matériels capteurs d'images ou de son.
- Préparez un parcours de visite et l'encadrer, ne laissez pas de visiteurs s'écarter du groupe ou s'entretenir seuls avec des employés.
- Présentez le strict nécessaire et n'effectuez pas d'essai sur de nouveaux projets.

5. SÉCURISER LE POSTE DE TRAVAIL

Un seul poste de travail non sécurisé et le réseau tout entier peut être affecté.

Votre poste de travail est-il sûr ?

- Utilisez-vous un antivirus ? Se met-il à jour automatiquement ?
- Votre système d'exploitation, votre navigateur et vos plug-ins sont-ils à jour ? Se mettent-ils à jour automatiquement ?
- Avez-vous un pare-feu personnel ?
- Attention aux périphériques USB, vecteurs de codes malveillants (clés, disques durs…).

6. MOT DE PASSE

Indispensable, incontournable et pourtant ....

Êtes-vous sûr d'avoir un mot de passe robuste ?

- Utilisez au moins 8 caractères.
- Utilisez au moins 1 chiffre et 1 caractère accentué.
- Facile à retenir mais difficile à deviner.
- N'utilisez pas un mot de passe qui contient des informations personnelles (date de naissance, de mariage…).
- Renouvelez régulièrement (tous les 3 mois).
- Utilisez différents mots de passe suivant les accès (compte bancaire, messagerie...).
- Ne stockez pas les mots de passe dans un fichier ou sur un support papier.

7. SAUVEGARDES

C'est évident, mais encore faut-il les rendre systématiques, ciblées et fiables.

Avez-vous pensé à sauvegarder vos données ?

- Triez, classez et donnez des noms pertinents à vos documents.
- Recherchez l'exhaustivité maximale de vos données à sauvegarder.
- Utilisez un logiciel de sauvegarde dédié.
- Faites au moins une sauvegarde par jour.
- Externalisez vos sauvegardes hors de l'entreprise.
- Testez vos sauvegardes régulièrement.
- Pensez aux outils de synchronisation si vous avez plusieurs ordinateurs.

8. COURRIELS, PIECES JOINTES, CANULARS

75% des attaques et infiltrations passent par les courriels.

Êtes-vous vigilant ?

- N'ouvrez pas, ne répondez pas, mais supprimez directement les courriels provenant d'expéditeurs inconnus.
- Ne cliquez pas sur les liens inclus dans les courriels si vous avez le moindre doute.
- Ne cliquez pas sur les pièces jointes incluses dans les courriels si vous avez le moindre doute.
- Ne relayez pas les messages de type chaînes de lettres, porte-bonheur.
- Jamais votre banque ne vous demandera un mot de passe (ou sa réinitialisation par un lien) ou un code pin par courriel (social phishing).
- Attention aux liens malveillants sur les médias sociaux.