PROTECT

YOUR DATA
YOUR BUSINESS
YOURSELF

MOT DE PASSE DE QUALITÉ ET ROBUSTE

- Changez de mot de passe au minimum une fois par an.
- Différenciez vos mots de passe professionnels et privés.
- Au moindre doute, changez votre mot de passe et alertez les instances responsables de la sécurité.
- Ne sauvegardez pas votre mot de passe dans votre navigateur internet et encore moins sur un post-it collé sur votre écran.
- Préférez une double authentification pour vos données très confidentielles.

SURFEZ EN TOUTE SÉCURITÉ

- Ne cliquez pas sur des liens dont vous ne connaissez pas la fiabilité.
- Evitez de passer par une connexion publique ou un appareil non sécurisé pour transmettre des données personnelles.
- Contrôlez la diffusion de vos informations personnelles (si c'est gratuit c'est vous le produit).
- Désactiver par défaut les composants ActiveX et JavaScript.
- N'utilisez jamais un compte administrateur pour naviguer sur internet.

EMAILS

- Séparez/cloisonnez les courriers et adresses professionnelles et personnelles.
- Ne relayez jamais des canulars, des messages de type chaînes de lettres, porte-bonheur ou pyramides financières, appel à solidarité, alertes virales, etc.
- Ne cliquez pas par « défaut » sur les pièces jointes et liens dans les emails.
- Alertez et rapportez les incidents ou comportements suspicieux

Bisoft

www.bisoft.be
+32 2 880 12 00 I info@bisoft.be

PROTECT

YOUR DATA
YOUR BUSINESS
YOURSELF

SECURITÉ DE L'INFORMATION AU TRAVAIL

- La perte d'information et la perturbation de l'activité sont les principales conséquences pour les entreprises victimes de cybercriminalité.
  Mieux vaut élaborer une politique de sécurité et un code de conduite pour protéger votre entreprise (gestion du risque).
- Désignez un responsable de la sécurité de l'information et/ou un délégué à la protection des données.
- Sensibilisez les utilisateurs à la sécurité informatique et aux obligations en matière de protection des données personnelles (instaurez une semaine de la sécurité par exemple).
- N'acceptez aucun support de stockage amovible sauf si il est encrypté ou protégé.
- Identifiez et détruisez les documents confidentiels (destructeur de documents).
- Identifiez et accompagnez les visiteurs.
- Prévoyez un plan de continuité et de reprise des activités, ainsi qu'un processus de gestion des incidents.

SUR VOTRE POSTE DE TRAVAIL

- Effectuez des sauvegardes régulières sur les appareils mobiles (pc portables et smartphones) surtout en cas de vol.
- Veillez à avoir un système d'exploitation et des logiciels à jour : navigateur, antivirus, bureautique, pare-feu, etc.
- Envisagez de travailler dans le cloud avec une politique de back up.
- En cas de doute, sollicitez les instances responsables de la sécurité.
- N'abordez pas de sujet confidentiel dans les endroits publics ou sur les médias sociaux.
- Sécurisez l'information confidentielle : Clean and Clear Desk, armoires et bureaux fermés à clé.
- Verrouillez votre PC en cas d'absence (veille automatique ou manuelle).

Bisoft

www.bisoft.be
+32 2 880 12 00 I info@bisoft.be