telecomservices
SOLUTIONS INFORMATIQUES

Sécurité informatique

Sensibilisation aux bonnes pratiques

Module i231

Brochure sur la sécurité informatique de l'entreprise

MOTA DIAS Bruno, NICOLET Jean-Pierre

telecomservices
SOLUTIONS INFORMATIQUES

Bonjour à toutes et tous,

La sécurité est l'affaire de tous.

La sécurité physique et la sécurité informatique est un élément **crucial** dans une entreprise.

Notre Groupe, à l'image de beaucoup d'autres entreprises, est confronté régulièrement à des vols de matériels et pertes de données. Dans ce contexte, nous devons toutes et tous redoubler de vigilance.

Pour cela, nous vous présentons cette brochure informative de sécurité pour la protection de l'ensemble de notre groupe.

Protection physique du matériel

Pour éviter des ou vols, ce qui entraîne automatiquement des pertes de données sensibles. Le service informatique va mettre en place différents systèmes de sécurité physique, comme un cadenas pour les Laptop, la sécurisation des bureaux avec des badges à accès restreints, etc.…

Nous vous demandons également d'être responsable du matériel mis à disposition pour la sécurité de l'entreprise.

Pour cela, voici les bonnes pratiques à prendre pour la protection physique :

- Toujours fermer sa fenêtre et la porte de son bureau pendant les absences.
- Protéger le matériel avec le sac fourni pour les interventions extérieures.
- Pas de liquide ou récipient proche des postes de travail.
- Film de protection contre le regard indélicat d'autrui.
- Utilisation de disque dur et support amovibles sur un support stable.
- Mettre à l'abri des températures extrêmes.

Supports amovibles

En ce qui concerne les supports amovibles nous allons mettre en place BitLocker pour plus de sécurité et un logiciel de protection par mot de passe.

Nous vous invitons également à suivre les recommandations suivantes :

- Utilisation des supports amovibles uniquement internes propres à l'entreprise, pas de supports externes ou personnels.
- Protection par mot de passe des supports.
- Éviter les sources de chaleur ou à côté d'une fenêtre au soleil etc.
- Éjecter correctement les supports amovibles.
- Lancer systématiquement une analyse antivirus à l'introduction du support.
- Ranger après utilisation dans leur protection respective.
- Cartes SD: utiliser la protection en écriture.

Webcam, assistants vocaux et autres objets connectés

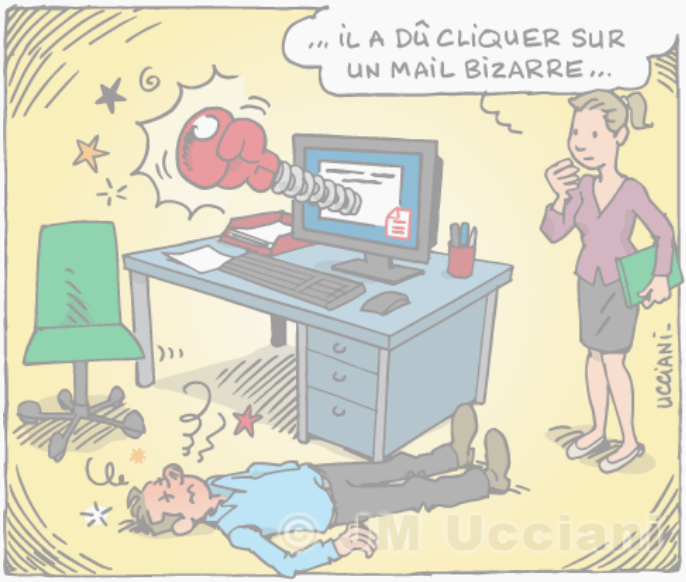
L'utilisation de webcam, assistant vocaux et objets connectés peuvent également poser des problèmes de sécurité.

Le service informatique va effectuer les actions suivantes :

- Mettre à disposition des Laptops avec volet cache-caméra.
- Désactiver les assistants vocaux tels que Cortana, Google, Siri, etc.
- Interdire les appareils connectés lors de réunions confidentielles.
- Changer les mots de passe par défaut des appareils connectés.
- Installer antivirus à jour, antimalware.
- Désactiver le Bluetooth et la localisation des appareils qui se situent au sein de l'entreprise.
- Vérification des mises à jour régulière du logiciel et driver caméra.

Pour la sécurité côté employé nous vous invitons à suivre les recommandations suivantes :

- Utiliser des webcams uniquement en cas de besoin (réunions, meeting, ...).
- Quand elle n'est pas utilisée, cacher la webcam du laptop avec le volet.
- Ne pas cliquer sur des liens suspects dans des e-mails.



Mise à jour des logiciels

Le service informatique va gérer les points suivants :

- Stratégie de mise à jour automatique de la base des signatures virales pour antivirus et ensuite analyse du terminal.
- Stratégie de mise à jour des applications (logiciel antivirus, bancaire, navigateur Internet, etc.
- Stratégie de mise à jour du système d'exploitation.
- Mise à jour des pares-feux.
- Mise à jour des périphériques.
- Analyse systématique des fichiers

Pour tous les utilisateurs, voici les bonnes pratiques à prendre en compte :

- Ne pas sûr réagir à une alerte (message alarmiste).

- Si une notification de mise à jour ou autre apparaît, veuillez le signaler auprès du service informatique et nous ferons le nécessaire.
- Être attentif au mail de phishing et ne pas cliquer sur les liens ou boutons disponible sur un mail.

telecomservices
SOLUTIONS INFORMATIQUES

Stratégie de sauvegarde des données

Afin de garantir la sécurité ainsi que la protection de vos données, nous vous conseillons vivement de les sauvegarder.

Pour commencer il faut se procurer un support de stockage de données. Un disque dur externe ou un serveur de stockage en réseau (NAS). Il est également possible de louer un espace Cloud (il faut évidemment une bonne connexion internet).

Pour faire des sauvegardes, nous vous conseillons fortement d'utiliser les différents logiciels ci-dessous :

- Acronis
- Paragon
- Ashampoo
- Bvckup 2
- Backblaze

Vous avez différentes possibilités de créer des sauvegardes de vos données. Plusieurs méthodes de sauvegarde sont disponibles en rapport avec les besoins, la taille des données, et la fréquence des sauvegardes.

Deux sites distincts (coffre anti-feu, etc.) Deux supports de sauvegarde.

⚠ Tester la restauration que vous avez créé !

Mots de passes et sauvegarde

Afin de créer des mots de passe sécurisé, nous vous invitons à utiliser la politique de mot de passe suivante :

- 12 caractères minimum
- Des majuscules et minuscules
- Des caractères spéciaux
- Des chiffres

Ne pas enregistrer les mots de passe en général sur les navigateurs mais sur des logiciels sécurisés. Pour cela nous vous recommandons d'utiliser ces quelques gestionnaires de mots de passe :

- Bitwarden
- KeePass
- LastPass
- SecureSafe

Ces applications sont également disponibles sur smartphone.

Bonnes pratiques :

Nous mettons à votre disposition quelques bonnes pratiques à mettre en œuvre afin de garantir une meilleure sécurité que se soit pour la vie professionnelle ou personnelle.

Sessions

- Toujours verrouiller sa session pendant les absences, même courte (touche Windows + L).
- Changer régulièrement son mot de passe quand il est demandé.
- Utiliser un gestionnaire de mot de passe.
- Ne jamais mettre le même mot de passe pour différents comptes.
- Choisir des mots de passe complexes (ne pas utiliser des informations concernant l'utilisateur).
- Ne jamais divulguer son mot de passe.
- Ouverture de session par reconnaissance biométrique (empreinte ou faciale).
- Activer l'authentification à la reprise.

telecomservices
SOLUTIONS INFORMATIQUES

Navigation Internet

- Ne pas mémoriser les mots de passe dans un navigateur.
- Utiliser un gestionnaire de mot de passe.
- Utiliser la navigation privée.
- Refuser les cookies facultatifs.
- Être très vigilant quand on navigue sur internet.
- Mettre à jour le navigateur.
- Utiliser les extensions (antivirus, blocage de pubs, ...).
- Vérifier si le site est avec le protocole https.

Messagerie

- Activer l'authentification à deux facteurs.
- Faire très attention aux mails de phishing (ex. pièce jointe qui n'est pas attendue, faux liens, etc.).
- Être attentif à l'adresse de l'expéditeur ainsi qu'à l'objet du mail.
- Ne jamais communiquer des données confidentielles.

Réseaux sociaux

- Activer l'authentification à deux facteurs.
- Protégez l’accès à vos comptes en utilisant des mots de passe différents et suffisamment forts.
- Mettre le compte en mode privé.
- Ne pas mettre en avant des informations personnelles (rue, pays, nom, etc.).
- Vérifiez vos paramètres de confidentialité. (La visibilité de vos informations personnelles et de vos publications sont ouvertes à tous).

Suspicion d'accès frauduleux

Il faut être attentif aux points suivants :

- Des e-mails et d’autres messages frauduleux qui semblent provenir d’entreprises légitimes, telles que Swisscom.
- Des fenêtres mensongères indiquant que votre appareil présente un problème de sécurité.
- Des appels ou des messages d’une personne qui se fait passer pour un conseiller d’assistance d’entreprise légitime comme Microsoft, il ne vous demandera jamais votre mot de passe.

- De fausses promotions qui proposent des produits gratuits et des récompenses.
- Des invitations de calendriers et des abonnements indésirables.

Télétravail

- Ne faites pas en télétravail ce que vous ne feriez pas au bureau.
- Si votre entreprise dispose d'une charte informatique dans le cadre du télétravail, prenez-en connaissance et appliquez-la rigoureusement.
- Si vous utilisez un Wi-Fi, créez un mot de passe long et complexe.
- Installez uniquement des applications autorisées par votre entreprise.
- Favorisez l'usage d'équipements fournis et contrôlés par votre entreprise.
- Si vous devez utiliser un ordinateur personnel, assurez-vous qu'il est suffisamment sécurisé.
- Si vous devez utiliser votre téléphone personnel, protégez vos données et limitez les accès.
- Évitez de transmettre des données confidentielles via des services grand public de stockage, de partage de fichiers en ligne ou via des messageries.

Voyages

- Sauvegardez toutes vos données en lieu sûr avant de les emporter.
- Évitez de transporter des données superflues. Il n'est pas nécessaire de posséder l'ensemble des informations relatives à votre entreprise pendant votre voyage.
- Ne pas annoncer vos déplacements où donner des détails sur vos déplacements sur internet ou sur les réseaux sociaux.
- Utilisez de préférence du matériel informatique sécurisé dédié pour vos déplacements.
- Placer un autocollant ou un sticker pour reconnaître votre matériel rapidement.
- Ne laissez pas vos équipements sans surveillance.
- Évitez les connexions sur le Wifi public.
- Désactiver en permanence toute connexion inutile, le wifi ou le Bluetooth.
- Évitez d'utiliser des équipements informatiques qui ne sont pas les vôtres.
- N'utilisez pas les câbles en libre-service dans les lieux publics pour charger votre smartphone et ne le branchez jamais dans une voiture de location.

Impressum

TELECOM SA

En Budron E9
1052 Le Mont-sur-Lausanne
☎ + 41 21 624 34 18

En cas de question ou de problèmes, vous pouvez contacter le service informatique à l'adresse et au numéro suivant :

Tél. : 021 624 34 18 Interne : 418
Mail : cybersecurite@telecom.ch