Elliot Schmid
DEVA1A

jobtrek

Bienvenue dans votre guide de sécurité, votre allié pour une navigation numérique sûre et sereine. Explorez différents conseils efficaces pour protéger vos données et appareils dans le monde de la technologie. Que vous soyez un novice ou un expert, découvrez des astuces accessibles qui renforceront votre sécurité en ligne. Ensemble, embrassons la tranquillité numérique.

BROCHURE DE SÉCURITÉ

jobtrek

+41 24 426 14 14

AV. DES DÉCOUVERTES 3
1400 YVERDON-LES-BAINS

INFO@JOBTREK.CH

Protection physique du matériel

La sécurité de nos équipements électroniques est essentielle pour prévenir les risques liés au vol, à la perte, à la casse. Ces conseils vous fourniront des choses pratiques pour protéger vos outils de travail

Protection contre le vol

- **Verrouillez correctement votre appareil** : Préconisez un déverouillage avec votre empreinte digitale, si vous possèdez un laptop avec cette fonctionnalité
- **Ne laisser pas vos dispositifs visibles dans votre voiture :** Rangez-les, dans un sac qui est sous les siéges, dans le coffre, mais surtout à l'abris de tout les regards
- **Utilisez des câbles antivols :** Lorsque vous travaillez dans un espace public, utilisez les câbles antivols pour attacher votre appareil à un objet fixe, pour dissuader les tentations

Protection contre la perte et l'oubli

- **Établissez une routine :** Prenez l'habitude de vérifier si vous avez tous vos dispositifs avec lequels vous êtes venu avant de quitter un endroit
- **Utilisez des trackers Bluetooth** : Utilisez ces dispositifs qu'on vous met à disposition pour afin de localiser vos appareils en cas de perte

Protection contre la casse

- **Utilisez les étuis de protection** : Utilisez ceux que l'entreprise vont on mit à disposition pour protéger vos appareils, cela évitera la casse
- **Protection contre la chaleur et la surchauffe :** Évitez de laisser vos dispositifs exposés en plein soleil pendant de longues périodes, afin d'éviter tout problème futur avec votre laptop

Astuces pour des supports amovibles

On adore nos clés USB, disques durs externes et autres petits gadgets, mais soyons un peu malins pour éviter les bobos. Voici quelques conseils rapides pour que vos données restent en sécurité et soient heureuses.

Vigilance contre les Virus

- **Stop à l'exécution automatique :** Les fichiers ne devraient pas se lancer automatiquement. Désactivez cette fonction pour éviter toute surprise.
- **Un petit check-up antivirus :** Avant de brancher votre support, faites-lui passer un test sur notre antivirus. Comme une visite chez le docteur, mais pour votre ordinateur !

Protégez vos données

- **Pas de prêt de supports :** Ne prêter pas vos clés USB, vos disques dur et autres supports
- **Sécurisez vos dossiers avec un mot de passe :** Mettez un petit cadenas numérique sur vos fichiers importants !
- **Utiliser BitLocker** :
  - 1. Sélectionnez le dossier que vous souhaitez protéger.
  - 2 .Clic droit sur le dossier et choisissez "Chiffrer le contenu pour sécuriser les données".
  - 3,Suivez les instructions pour activer BitLocker et définir un mot de passe.

Gardez vos données tranquilles

- **Pas de formatage express :** Si vous devez formater, faites-le avec précaution pour ne pas perdre vos souvenirs numériques.
- **Trouvez-leur une maison sûre :** Vos supports méritent un endroit sûr, comme un coffre-fort. Ne les laissez pas traîner n'importe où ! (One Drive de l'entreprise, Google Drive, Dropbox)

Webcam, assistants vocaux et autres objets connectés

Soyez le chef de votre webcam/micro

- **Utilisez un autocollant ou un cache** : Collez un petit autocollant si vous ne possèdez pas de cache sinon couvrez votre webcam avec un cache quand vous ne l'utilisez pas.
- **Éteignez votre webcam et votre micro** depuis le menu de votre ordinateur et activez les manuellement.

Stop aux Assistants Vocaux qui vous écoutent

- **Éteignez Siri, Google Assistant, etc. :** Si vous ne les utilisez pas, désactivez-les.

Loin de l'action

- **Prière de mettre vos appareils connectés en pause pour des conversations importantes :** Lorsque vous avez des conversations importantes, éloignez les téléphones, vos montres connectées, etc..
- **Si vous soupçonnez un logiciel espion, repartez à zéro :** Si quelque chose semble bizarre, sauvegardez vos données et réinitialisez tout comme au premier jour.

Mise à jour des logiciels, Ajout d'un antivirus

Protéger votre ordinateur, c'est prendre soin de votre maison numérique

Nous nous occupons de vous installer

- **D'installer un anti-virus**
- **Mettre à jour vos signatures virales à jour**
- **Toutes les mise à jour qui touche aux logiciels sensibles**
- **Implémenter un sytème de vérification de fichiers**

De votre côté nous souhaitons que vous fassiez

Voici des conseils simples, même si vous n'êtes pas expert en informatique, pour éviter les ennuis

- **Mettre vos logiciels à jour :** Les logiciels ont parfois besoin de petites mises à jour. C'est comme donner des bonbons à votre ordinateur pour qu'il reste content.
- **Mettre à jour votre système d'exploitation :** Le système d'exploitation, c'est comme le chef d'orchestre de votre ordinateur. Donnez-lui une nouvelle baguette avec des mises à jour régulières.

jobtrek

Stratégie de sauvegarde des données

Défendez-vous contre les pannes et les erreurs

- **Pour commencer choisir le support qui convient :** Disque dur externe fourni par l'entreprise et/ou le Cloud de l'entreprise (One Drive) , ou un autre outils. Choisissez le support qui vous semble le plus pratique
- **Adopter une stratégie de sauvegarde** : Comme un coffre-fort pour vos données, mettez en place une stratégie de sauvegarde.
  - **Voici quelques logiciels de BackUp** : EaseUS Todo Backup, FBackup, Acronis, Ashampoo Backup
- **Regrouper et classer ses données** : Imaginez vos données comme des amis. Regroupez-les et classez-les pour ne pas les perdre de vue. Et surtout nommez les correctement pour vous facilitez la tâche pour vous y retrouver !
- **Définir une fréquence de sauvegarde** : Choisir à quelle fréquence vous voulez sauvegarder vos données. Plus c'est régulier, mieux c'est. Nous vous conseillons de le faire dès que vous avez rajouté des choses importantes et de le faire au minimum hebdomadairement. Mais Cela dépend aussi du type de sauvegarde que vous voulez.
- **Choisir une méthode de sauvegarde** : Pour revenir sur le point d'avant, nous préconisons de faire soit une sauvegarde totale, différentielle, ou paritelle. Choisissez la méthode qui convient le mieux à votre situation.
- **Tester la restauration :** Voyez le comme une vérification que vos clés ouvrent la porte de chez vous, assurez-vous que vous pouvez correctement restaurer vos données. Cela serait bête de sauvegarder ses données mais que vos données soient inutilisables

jobtrek

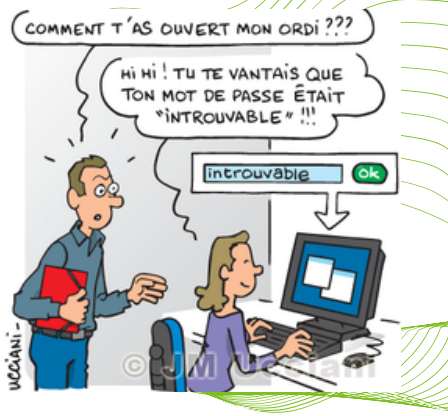
Mots de passes et sauvegarde

Avoir une bonne protection en ligne, avec les normes de l'entreprise

- **Choisir des identifiants**, pas trop évidents mais faciles à retenir (Pas de nom, prénom, animaux, ect..).
- Le mot de passe **PARFAIT** serait :
  - **12 caractères(Un mot de passe sécurisé doit comporter au moins** 12 caractères**)**
  - **des chiffres, des lettres, des caractères spéciaux**
  - **un mot de passe anonyme** (Pas de nom, prénom, animaux, date de naissance, ect**)**

Et suivre également cela :

- **Changer ses mots de passe régulièrement :** Mensuellement, hebdomaderaiment. Mais changer les regulièrement cela rendra plus difficle aux pirates de trouvé vos accès. **ET SUROUT N'UTILISEZ PAS LE MÊME MOTS DE PASSE SUR DIFFÉRENTS COMPTES !!**
- **Mettre une authentification à deux facteurs sur vos comptes**
- **Ne pas stocker ses mots de passe dans le navigateur :** Utilisez une application de coffre-fort pour vos mots de passe. (NordPass, Keeper, Dashlane, ect)
- **Ne jamais fournir son mot de passe à quiconque :** Il est impératif de ne jamais divulguer son mot de passe, même à vos collègues les plus proches, car on ne peut jamais être certain de la bienveillance de l'autre



jobtrek

Mesures et Bonnes Pratiques

Session

- **Verrouiller votre session sytématiquement** : Lorsque vous quittez votre poste, verrouillez votre session. (Touche Windows + L)
- **Ne pas désactiver le verrouillage automatique en cas d'inactivité**
- **Activer l'authentification à la reprise**
- **Utiliser l'empreinte digitale pour vos portables**
- **Ne pas utiliser son mot de passe à plusieurs endroits**

Navigation Internet

- **Ne pas stocker ses mots de passe dans le navigateur**
- **Ne transmettre aucunes informations sensibles sur les réseaux sociaux**
- **Vérifier le protocole "https" :** il suffit de vérifier la présence de l'indicateur en forme de cadenas vert placé tout à gauche de la barre d'adresse, à côté du nom de domaine (https://jobtrek.ch)
- **Effacer régulièrement votre historique : (cookies, etc.).**
- **Utiliser la navigation privée sur les sessions publiques**
- **Tenir à jour votre navigateur**

jobtrek

- **Utiliser les extensions disponibles :**
  - **Blocage pop Up :**
    - Poper Blocker (Chrome), Popup Blocker (Firefox)
    - AdGuard Ad Blocker
  - **Blocage site à risque :**
    - Malwarebytes Browser Guard (Chrome, Firefox)
    - AdBlock (Chrome, Firefox)

Messagerie

- **Détecter les e-mails frauduleux** : Soyez attentif (aux adresses mail inconnues, aux titres, aux fautes d'orthographe, aux liens, etc.
- **Rester informé des arnaques courantes** : Consultez les sources fiables pour vous tenir au courant des arnaques courantes(ncsc.admin.ch, votrepolice.ch/cybercriminalite)
- **Si vous avez un doute sur un e-mail suspect, ne répond pas et parler en avec nous**
- **Si vous détectez une arnaque**, signalez-la à l' ***"IT" et aussi à ncsc.admin.ch*** pour protéger les autres.
- **Utiliser la signature électronique** pour renforcer la sécurité. (Fichier Word, Outlook)

Réseaux Sociaux

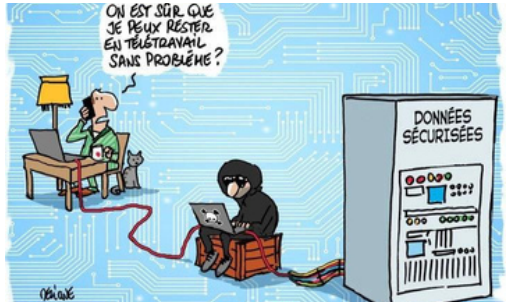
- **Éviter de partager vos infos personnelles sur les réseaux sociaux**
- **Utiliser des pseudos différents et évitez de mettre vos vraies données (Nom, Prénom, ect)**

jobtrek

- **Sécuriser vous avec une couche supplémentaire** avec l'authentification à facteurs multiple Voici des exemples : (Google Authenticator, Microsoft Authenticator, Duo Mobile, ect...)

Suspicion d'accès frauduleux

- Processus ISO de l' entreprise
- Canal d'annonce (email, téléphone, etc.)
- Délai d'annonce
- Personne de contact ou de référence (évaluation du risque)
- Informations à fournir : vol, perte, preuves, etc.
- Communication aux tiers : organismes officiels (police, ncsc), partenaires commerciaux, personnel de l'entreprise, médias, etc.



Télétravail

- **Aménager un espace de confidentialité** : Restez discret lors des appels téléphoniques ou des visioconférences.
- **Visioconférence sécurisée** : Masquez l'arrière-plan, coupez le micro, utilisez de préférence un casque/micro, limitez le volume des haut-parleurs.
- **Gestion des documents** : Ne laissez pas traîner des documents imprimés à votre domicile. Emportez uniquement les données nécessaires.
- **Utiliser une liaison filaire** : Privilégiez une connexion filaire plutôt que le Wi-Fi.
- **Sauvegarder les données sur le réseau de l'entreprise** : Évitez de stocker des données professionnelles de manière locale. Utilisez le réseau de l'entreprise pour sécuriser vos transmissions.

jobtrek

Voyage

Suivez ces astuces simples pour profiter pleinement de votre voyage en toute sérénité, des conseils pratiques pour garantir la protection de vos données lors de vos déplacements :

- **VPN :** Installer en un pour sécuriser votre connexion et protéger vos données sur les réseaux publics. Voici quelques exemples de VPN (NordVPN, CyberGhost, ExpressVPN)
- **Gardez-le en sécurité :** Verrouillez physiquement votre ordinateur portable comme expliquer auparavant dans la brochure(Verouiller son écran, garder à l'écart des regards, ect)
- **Sauvegardez vos données :** Effectuez une sauvegarde avant le départ pour éviter toute perte de données pendant le voyage avec les outils que nous avons mis à disposition
- **Évitez les Wi-Fi publics :** Limitez l'utilisation des réseaux Wi-Fi publics, souvent moins sécurisés. Si possible connecter vous en 4G avec votre téléphone.
- **Restez vigilant** : Soyez attentif dans les lieux publics pour prévenir le vol de votre ordinateur portable.
- **Protégez l'écran** : Utilisez un filtre d'écran pour éviter les regards indiscret de voisins.

Conclusion

En conclusion, en adoptant les conseils énoncés dans cette brochure, vous pouvez prévenir efficacement ces problèmes potentiels. Veillez à mettre en œuvre ces pratiques pour garantir la sécurité et la protection de vos données et des données de l'entreprise dans votre parcours numérique.