cara.
connecté à ma santé

Bonnes pratiques en matière de sécurité informatique

Pourquoi la sécurité informatique est-elle si importante ?

- **Pour assurer votre travail**
  En cas de problème de sécurité vous ne pourriez plus travailler avec votre matériel informatique et vos données pendant une longue période.

- **Pour garantir la protection des données des personnes qui vous font confiance**
  La confiance est essentielle. Les personnes vous ayant confié leurs données comptent sur vous pour en assurer la protection.

- **Pour respecter votre engagement contractuel vis-à-vis de CARA**
  Vous vous êtes engagés, lors de votre affiliation à CARA, à respecter des exigences minimales en matière de sécurité.

- **Parce qu'encore trop souvent, ces règles de base ne sont pas appliquées**
  Ce guide ne doit donc pas seulement être lu, mais son contenu doit être réellement appliqué par votre organisation, vos utilisatrices et vos utilisateurs.

20 bonnes pratiques pour renforcer la sécurité de vos informations

Vous pouvez réellement et efficacement augmenter votre sécurité en suivant les vingt bonnes pratiques ci-dessous, réparties en six domaines :

A. Le matériel
B. La gestion de vos utilisateurs
C. Les pratiques
D. Les mots de passe
E. La vigilance
F. La sensibilisation de vos utilisateurs

A. LE MATERIEL

Bonne pratique n° 1

Mettez systématiquement à jour vos logiciels, en particulier le système d'exploitation (Windows, MacOS, Android, iOS) et le navigateur internet utilisé pour accéder au DEP afin de corriger les failles de sécurité.

Si vous avez une entreprise qui gère votre informatique, demandez-lui de réaliser des mises-à-jour régulières, idéalement chaque fois qu'une nouvelle version est disponible.

Bonne pratique n° 2

Utilisez un logiciel antivirus à jour.

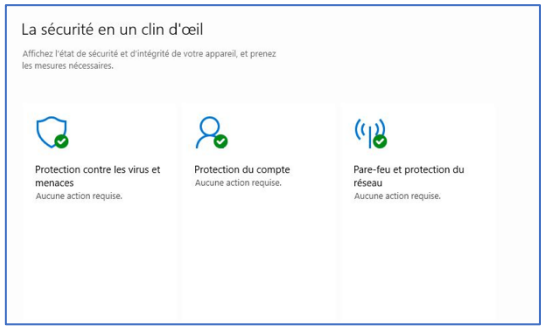
Vous pouvez ouvrir votre antivirus pour vérifier la date de mise à jour, et si ce n'est pas déjà le cas, activer les mises à jour automatique.

Bonne pratique n° 3

Utilisez un pare-feu.

Vous pouvez par exemple utiliser le pare-feu (ou coupe-feu, ou encore *firewall*) proposé par votre système d'exploitation. Celui-ci doit être activé.

Exemple sur Windows



Exemple sur Mac

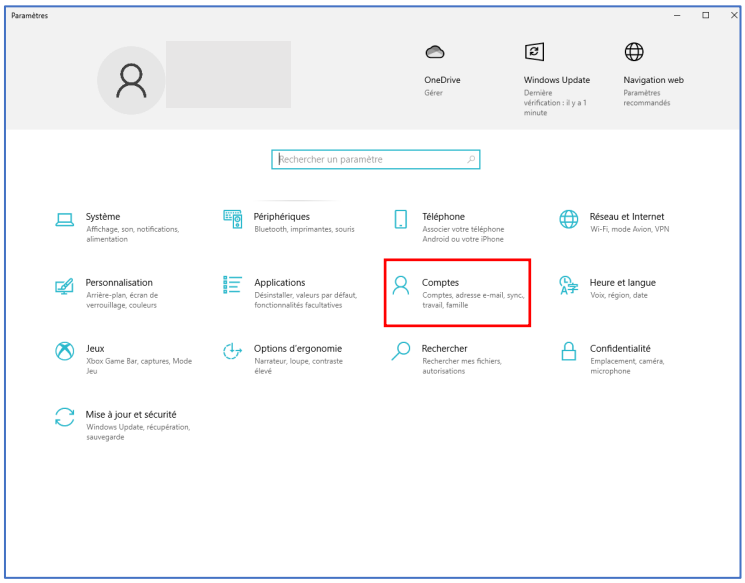
Un pare-feu physique ou sur votre modem peut également être mis en place.

Bonne pratique n° 4

Ne travaillez pas dans une session avec les droits administrateur.

Sur votre ordinateur, vous pouvez avoir différents types de sessions. Une session avec les droits administrateur vous permet d'apporter des modifications au fonctionnement de votre ordinateur, alors que ce n'est pas le cas avec une session utilisateur (ou standard). Afin d'éviter l'installation d'un logiciel malveillant sans que vous l'ayez approuvé, il est exigé de travailler dans une session pour laquelle vous n'êtes pas administrateur. Cela ne change rien dans votre travail courant mais lorsqu'un logiciel nécessitera une installation ou une mise à jour, vous devrez entrer un mot de passe administrateur. Vous avez ainsi un meilleur contrôle de ce qui est installé sur votre appareil.

Exemple sur Windows



Exemple sur Mac

Bonne pratique n° 5
N'accédez à la plateforme CARA que depuis des ordinateurs qui ont été sécurisés selon les points ci-dessus.

B. LA GESTION DE VOS UTILISATRICES ET DE VOS UTILISATEURS

Bonne pratique n° 6
Pensez ainsi à supprimer les accès des personnes qui quittent votre organisation.

Bonne pratique n° 7
Informez également CARA quand des utilisatrices ou des utilisateurs quittent votre organisation, via le formulaire en ligne https://forms.cara.ch/institution/staff-mutation. Ainsi, la liste des utilisateurs est également à jour sur la plateforme CARA.

Bonne pratique n° 8
Ne donnez à vos utilisatrices et à vos utilisateurs uniquement les accès nécessaires à l'accomplissement de leurs tâches.

C. LES PRATIQUES

Bonne pratique n° 9
Utilisez une connexion réseau sécurisée.

- Assurez-vous de vous connecter à un réseau que vous connaissez.
- Assurez-vous que votre réseau habituel est sécurisé avec un mot de passe (voir chapitre D).
- Assurez-vous que seuls vos collègues et vous-même avez accès à ce réseau.

Bonne pratique n° 10
Verrouillez systématiquement votre session dès que vous vous absentez, même pour un court instant.

Bonne pratique n° 11
Ne connectez pas à votre ordinateur de support externe (par exemple un disque dur ou une clé USB) provenant de personnes externes à votre organisation.

Bonne pratique n° 12
Ne laissez pas de tiers non autorisés vous approcher lorsque vous accédez à la plateforme CARA ou à votre système d'information clinique (votre logiciel de cabinet, par exemple).

D. LES MOTS DE PASSE

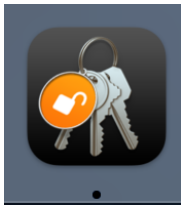
Bonne pratique n° 13
Créez des mots de passe uniques et complexes combinant majuscules, minuscules, chiffres, caractères spéciaux, pour chacun de vos comptes.

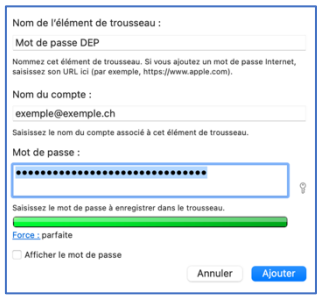
CARA recommande des mots de passe d'une longueur minimum de 10 caractères comportant au moins une majuscule, une minuscule, un chiffre et un caractère spécial. Vous pouvez par exemple choisir une phrase entière qui fait sens pour vous et donc qui vous est facile de vous rappeler.

Bonne pratique n° 14
N'inscrivez jamais vos mots de passes sur un support physique (post-it, cahier, sous le clavier, etc.).

Vous pouvez en revanche les enregistrer dans un système de trousseau sur votre ordinateur ou votre téléphone pour autant qu'il ne soit accessible que par vous.

Exemple sur Mac
Il s'agit du « Trousseau »





Bonne pratique n° 15
Ne communiquez jamais vos mots de passe à quiconque.

CARA et tous les prestataires sérieux ne vous demandent jamais votre mot de passe, que ce soit par téléphone, par e-mail ou par courrier. Si CARA, un fournisseur d'identité électronique (par exemple Hin, GenèveID ou VaudID santé) ou tout autre prestataire, vous demande quelque chose qui vous parait suspect, n'hésitez pas à téléphoner via le numéro sur le site officiel du fournisseur.

Vous pouvez contacter CARA au 021 566 84 51.

Il est également interdit de transmettre son moyen d'identification électronique à une tierce personne, même au sein de votre organisation.

E. LA VIGILANCE

Bonne pratique n° 16
Ne vous laissez pas tromper ou distraire. Si quelque chose vous parait anormal ou inhabituel, agissez avec prudence.

Bonne pratique n° 17
N'ouvrez pas les pièces jointes d'e-mails dont vous doutez de la provenance. Si vous ne connaissez pas l'expéditeur, ou que vous ne voyez pas votre nom parmi les destinataires, ou que le message est formulé bizarrement (langue étrangère, nombreuses fautes d'orthographe, formulations inhabituelles), supprimez le message.

En cas de doute ou si vous avez déjà cliqué sur la pièce jointe, contactez immédiatement votre fournisseur informatique ou votre responsable informatique.

Bonne pratique n° 18
Ne cliquez pas sur un lien figurant dans un e-mail ou dans un message sans avoir vérifié au préalable la fiabilité de l'expéditeur. Vous pouvez par exemple passer la souris sur le lien sans cliquer et l'URL du lien s'affiche. Si vous ne connaissez pas le site ou doutez de l'expéditeur, supprimez le message.

En cas de doute ou si vous avez déjà cliqué, contactez immédiatement votre fournisseur informatique ou votre responsable informatique.

F. LA SENSIBILISATION DE VOS UTILISATRICES ET DE VOS UTILISATEURS

Bonne pratique n° 19
Parlez de sécurité avec vos collègues, en particulier de ces bonnes pratiques.

La sécurité informatique, via notamment ces quelques points, passe par une vigilance collective. Partagez ces points en expliquant pourquoi c'est important.

Vous pouvez par exemple utiliser notre page « règles d'or en matière de sécurité » pour en parler à vos collègues et l'afficher clairement dans vos locaux.

Bonne pratique n° 20
Parlez régulièrement de sécurité à vos collègues, à vos collaboratrices et vos collaborateurs.

Pensez à régulièrement faire des rappels et discuter de ce sujet avec vos collègues, par exemple lors de l'arrivée d'une nouvelle ou d'un nouveau collaborateur, ou encore deux fois dans l'année à des dates fixes. Même si ces règles de bonne conduite sont simples et évidentes, une vigilance accrue permet de prévenir bien des risques.

Assistance
Pour toute question concernant les bonnes pratiques, n'hésitez pas à nous contacter :
www.cara.ch/assistance