Règles de bonne conduite à retenir en matière de sécurité de l'information

—

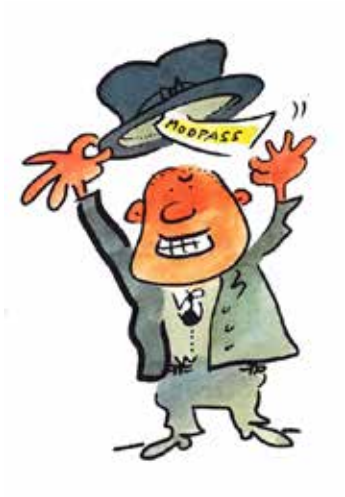
ETAT DE FRIBOURG
STAAT FREIBURG

Autorité cantonale de la transparence et de la protection des données ATPrD
Kantonale Behörde für Öffentlichkeit und Datenschutz ÖDSB

Mots de passe

Votre mot de passe, c'est comme votre brosse à dents.

- Ne le partagez jamais.
- Choisissez-le avec soin.
- Changez-le régulièrement.



Composez vos mots de passe avec un mélange de chiffres, de lettres et de caractères spéciaux.

- Un bon mot de passe contient 10 caractères au minimum.
- Il est composé de **chiffres**, de **lettres** et de **symboles** (caractères spéciaux, caractères accentués, ponctuation, etc.).
- Il ne doit pas être associé à une quelconque information liée à votre personne (prénom, date de naissance, etc.).
- Il ne doit pas être un mot du dictionnaire (même tiré d'un dictionnaire d'une langue étrangère). Par contre, il peut être composé d'une phrase d'au moins 4 mots (sans espace) mais toujours composée de chiffres, de lettres et de symboles. On appelle cela une «**passphrase**» ou une **phrase secrète.**

Ne donnez JAMAIS votre mot de passe et ne l'écrivez pas.

- Ne donnez JAMAIS votre mot de passe **ni à un collègue** (même en cas de remplacement pendant vos vacances), **ni à un supérieur, ni à votre conjoint.**
- Un mot de passe ne doit pas être partagé entre plusieurs personnes.
- Un mot de passe ne doit jamais être divulgué quelles que soient les circonstances.

Utilisez des mots de passe différents pour accéder à différentes applications, notamment lors de l'utilisation de services en ligne.

—

- Lors de l'utilisation de services en ligne, employez à **chaque fois** un mot de passe **différent**.
- N'utilisez surtout pas un mot de passe employé pour un **autre type d'accès** (comme le mot de passe de Windows, celui de votre messagerie ou encore celui d'une application métier).
- Plus vous utilisez des **applications informatiques à accès restreints,** plus vous devez créer des mots de passe différents.

Rappel: *utiliser le même mot de passe augmente les risques de se faire voler des informations personnelles et d'être victime d'usurpation d'identité.*

Changez fréquemment vos mots de passe, selon des intervalles réguliers.

—

- La durée de vie maximale d'un mot de passe dépend de l'application à protéger, mais elle ne devrait pas dépasser **90 jours.**
- Si votre mot de passe protège un accès de moindre importance, il n'est pas nécessaire de le changer fréquemment.
- En revanche, si votre mot de passe protège des accès importants, comme par exemple l'accès à votre ordinateur ou à vos comptes bancaires sur Internet, changez-le régulièrement.

Rappel: *si vous pensez que quelqu'un d'autre que vous connaît votre mot de passe, changez-le de suite.*

Changez les mots de passe attribués par défaut le plus vite possible.

—

- Lorsque l'on vous attribue un mot de passe par défaut, **changez-le immédiatement.**
- **Un nouveau mot de passe doit toujours être saisi 2 fois** pour vérifier que vous n'avez pas fait d'erreur de frappe.

Rappel: *vous devez d'autant plus vous méfier si vous utilisez un ordinateur public. En effet, vous ne savez pas si les mots de passe saisis sont enregistrés.*

Lorsque vous créez un compte sur une application Web (forum, application commerçante, etc.), on vous demande un e mail et un mot de passe pour sécuriser l'accès.

- **N'utilisez JAMAIS celui de votre compte Windows, de votre messagerie ou encore d'une application métier.**
- En faisant cela, l'administrateur du site Web peut accéder aux informations saisies, dont votre nom d'utilisateur (login) et votre mot de passe (si le site Internet est mal sécurisé).

Conseil: *si vous devez utiliser plusieurs mots de passe, utilisez un coffre-fort à mot de passe.*

Comment vous souvenir d'un bon mot de passe?

–

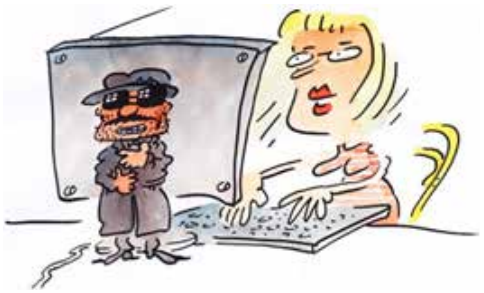
- **N'inscrivez pas** vos mots de passe sur un **bout de papier,** caché dans votre bureau ou dans votre portefeuille.
- Choisissez une **phrase secrète** comme expliqué plus haut.
- Vous pouvez aussi choisir une phrase comme **«Il était une fois 3 petits cochons: Pim Pam Poum».**
- Prenez les premiers caractères de chaque mot et les ponctuations, ce qui donne: **Iéuf3pc:PPP.**
- Si nécessaire, adaptez le mot de passe obtenu en ajoutant des **caractères spéciaux,** comme par exemple @ à la place de a.

Messagerie électronique (e-mail)

Votre adresse e mail, c'est comme votre numéro de téléphone.

- Ne la donnez pas à n'importe qui.
- Gardez l'esprit critique.
- Soyez prudent avec vos interlocuteurs.

Gardez l'esprit critique quand vous traitez des messages électroniques.

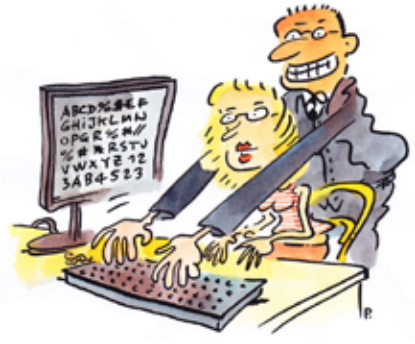


- Lorsque vous recevez un message, demandez-vous si c'est normal et si le contenu est conforme à ce que vous pouvez attendre de cet émetteur.
- Avant d'effectuer une action requise dans un e mail, en cas de doute sur l'émetteur ou sur l'action demandée, assurez-vous de l'origine de ce message en appelant l'expéditeur par exemple.

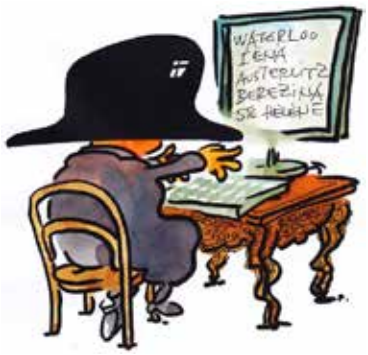
Lorsque vous recevez un message (e mail) important, nous vous suggérons de toujours demander une confirmation.

Rappel: avec l'e mail, comme avec le téléphone, il est important de rester constamment centré sur l'identification de la demande et du demandeur, ainsi que sur la vérification du motif prépondérant.

Une adresse e mail n'est pas un moyen efficace d'identification.



Une adresse e mail peut être facilement usurpée, et donc utilisée par une personne à qui elle n'appartient pas.



Conseil: *pour accéder à un site non professionnel, utilisez un e mail «incognito», contenant un pseudonyme et un autre nom que celui de votre organisation (bill@bluewin.ch par exemple).*

Ne divulguez pas publiquement votre adresse e mail.

—

- Ne **divulguez pas** vos adresses e mail, ni professionnelles, ni privées.
- Utilisez votre e mail professionnel exclusivement à des fins professionnelles.
- Réservez votre e mail privé à des **personnes de confiance.**

Remarque: *dans certains cas, vous êtes obligé de cliquer sur un lien dans un e mail (exemple du mot de passe oublié), mais cela doit être fait dans un laps de temps très court, suite à une sollicitation de votre part.*

Méfiez-vous des e mails contenant des liens sur des sites Internet qui peuvent cacher des virus, des demandes de rançons (ransomwares) ou des tentatives de phishing.

—

- Ne cliquez JAMAIS sur un **lien externe** contenu dans un e mail.
- Si vous souhaitez accéder à un site contenu dans un lien externe, **saisissez** vous-même, dans votre navigateur Web, **l'adresse officielle** de ce site.
- En effet, le destinataire de ce site peut chercher à vous **piéger** en vous dirigeant vers un **site falsifié.**

Important: *n'ouvrez aucun fichier joint à un e mail contenant 2 extensions comme par exemple «picture.bmp.vb».*

Attention aux photos, aux diapositives PowerPoint, aux animations, etc., car tout fichier envoyé par e mail peut être infecté à l'insu de l'expéditeur.

Faites attention aux fichiers joints aux e mails, car ils peuvent contenir des virus.

—

- Si possible, **n'ouvrez pas** le fichier attaché à un e mail dont vous ne connaissez pas **l'émetteur.**
- Si vous devez ouvrir des fichiers provenant de **personnes inconnues,** assurez-vous que ces fichiers ont été **scannés** par un antivirus. Vous pouvez aussi utiliser votre antivirus pour les scanner vous-même.

Faites attention aux informations professionnelles à caractère confidentiel.

—

› N'envoyez aucun courrier électronique professionnel à des tiers qui ne seraient pas en relation d'affaires avec votre organisation, et ce, en conformité au **secret professionnel** auquel vous êtes assujetti.
› Ne stockez pas les documents relatifs à vos projets professionnels dans votre boite e mail. Utilisez **le disque partagé** sur le réseau.

Rappel: *pour envoyer des données confidentielles par e mail, utilisez un moyen de chiffrement.*

Ne répondez pas aux e mails qui demandent des informations personnelles.

—

› Les organisations sérieuses ne demandent jamais de communiquer **par e-mail** des informations **personnelles** ou liées à des **identifiants de connexion** (login, mot de passe, n° de compte bancaire, etc.).
› En cas de doute sur la provenance d'un message, contactez directement l'organisation émettrice dans le but de vérifier son **identité**.

Rappel: *ne remplissez pas de* ***formulaire en ligne*** *qui arrivent par e mail et dont la provenance est inconnue.*

N'envoyez pas de courriers électroniques en chaîne.

—

› Ne transférez JAMAIS un e mail à **tout votre carnet d'adresses** au risque de devenir vous-même un spammeur.
› Si vous recevez des chaînes de lettres, n'y répondez pas.

Rappel: *si vous faites suivre un message sans en vérifier* ***la source****, vous cautionnerez son contenu par votre réputation, le faisant apparaître plus crédible, même si ce n'est pas le cas.*

Internet

Naviguer sur Internet, c'est comme voguer en haute mer.

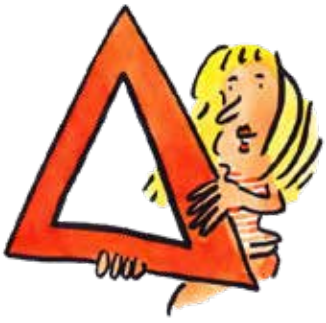
- Ne surfez pas sur n'importe quel site sans vigilance.
- Gardez l'esprit critique.
- Soyez prudent avec vos «affaires» privées.

Sur Internet, utilisez des mots de passe de qualité pour accéder à des applications sensibles (e commerce / e banking).

- Vérifiez que l'adresse du site sur lequel vous réalisez des transactions sensibles comporte le protocole «**https://...**». Avec ce protocole sécurisé, il est quasiment impossible à un pirate, qui intercepterait vos échanges, d'en déchiffrer le contenu, et donc de récupérer les informations véhiculées.
- En général, une **icône de sécurité** représentant un **cadenas fermé** s'affiche dans la fenêtre du navigateur indiquant que les communications avec le site Web consulté sont sécurisées.

Quittez les applications Web sensibles par les menus de déconnexion.

- Les navigateurs Internet ne détruisent les cookies (mouchards électroniques) que lorsque vous avez complètement fermé votre session.
- Les cookies conservent les options que vous avez cochées, afin de vous éviter de les ressaisir lors de votre prochaine visite. Malheureusement, ces informations peuvent être utilisées à mauvais escient par des personnes mal intentionnées.



N'utilisez pas l'option «Se souvenir de moi» (ou «Rester connecté»).

- L'option «Se souvenir de moi» vous permet de mémoriser vos identifiants dans votre navigateur afin d'être automatiquement connecté dès l'ouverture d'un site avec des accès protégés. **N'utilisez pas cette option sur un autre ordinateur que le vôtre** (et uniquement si vous ne le partagez avec personne) et encore moins sur un ordinateur public.
- Cette option crée un cookie (mouchard électronique) qui permet à toute personne, qui se connecte sur le même ordinateur que vous, d'accéder aux comptes des sites que vous avez ouverts.

Remarque: *cette option fonctionne uniquement si vous fermez votre navigateur ou éteignez votre ordinateur sans vous déconnecter du site protégé.*

Ne cliquez pas trop vite sur un lien hypertexte mentionné dans un message électronique.

—

› Une des attaques classiques visant à tromper l'internaute pour lui voler des informations personnelles, consiste à l'inciter à cliquer sur une adresse de site Web (URL) insérée dans un message électronique.
› Plutôt que de cliquer sur une URL présente dans un e mail, **saisissez-la vous-même dans la barre d'adresse de votre navigateur.**

Contrôlez la diffusion de vos informations personnelles.

—

› Ne saisissez jamais de **données personnelles** sur des sites Internet non sécurisés.
› Ne saisissez jamais d'informations sensibles, comme des **coordonnées bancaires**, sur des sites qui n'offrent pas toutes les garanties de protection requises.
› Ne faites pas de **commentaires déplacés** dans des **forums publics**. Sachez qu'ils sont archivés à tout jamais.

Pour naviguer sur Internet, vos logiciels doivent être mis à jour régulièrement.

—

› En général, les agresseurs recherchent les ordinateurs dont les **logiciels** ne sont pas mis à jour, afin d'utiliser les **failles de sécurité** non corrigées pour s'y introduire.
› C'est pourquoi, il est fondamental de mettre à jour tous vos **logiciels** afin de corriger ces failles.

Rappel: *les logiciels les plus récents proposent tous une fonctionnalité de mise à jour automatique.*

Ne vous connectez pas sur un site bancaire depuis un ordinateur accessible par d'autres utilisateurs.

—

› Les ordinateurs en libre-service ou appartenant à des tiers n'apportent **aucune garantie** au niveau de la sécurité.
› Rien n'indique qu'ils ne sont pas infectés par un logiciel espion et un enregistreur de frappe qui peut servir à une personne **mal intentionnée** pour récupérer vos **mots de passe** et vos codes d'accès par exemple.

Rappel: *soyez vigilant lorsque vous utilisez un ordinateur en libre accès dans tout lieu public.*

Protection des données

Protégez vos données, comme vous protégez vos deniers.

> Ne laissez pas n'importe qui accéder à vos données.
> Prenez en soin, elles valent plus que de l'argent.
> Mettez-les en lieu sûr.

Au travail, respectez les règles de bonnes conduites dans l'utilisation du système d'information.

> Vous êtes **responsable** de toutes les opérations réalisées sous votre nom (login et mot de passe).
> Adoptez la bonne conduite face à des situations à risques.

Rappel: *afin d'éviter tout risque d'usurpation d'identité, verrouillez votre poste de travail, même pour quelques minutes.*

Tout ce qui est possible n'est pas forcément légal ou autorisé.

> Les **lois suisses**, notamment la loi cantonale sur la protection des données (**LPrD**), la loi fédérale sur la protection des données (**LPD**) ainsi que les **lois internationales** doivent être respectées.
> De plus, vous êtes soumis à des **règlements propres à votre organisation**, ainsi qu'à ceux des clients pour lesquels vous travaillez.

Respectez les règles en matière de propriété intellectuelle.

> Cela concerne aussi bien les logiciels que tout type de **création intellectuelle** disponible sur Internet.
> Au sein de votre organisation, seuls les logiciels pour lesquels des **licences** ont été acquises peuvent être utilisés.
> Une attention toute particulière doit être apportée au respect des **droits d'auteur** lorsque vous copiez des informations (textes, images, autres) sur Internet.

Ne stockez pas d'informations illicites sur les disques durs du système d'information de votre organisation ou sur d'autres supports de stockage.

—

Vous vous engagez à **ne pas consulter, diffuser** ou **stocker** de message, d'image ou d'information notamment:

- à caractère injurieux, calomnieux, diffamatoire, ou portant atteinte à l'honneur, à la réputation d'autrui ou à la condition humaine;
- incitant ou permettant à des tiers de violer des droits de propriété intellectuelle;
- en violation du caractère privé de la correspondance.

Rappel: *si vous constatez une anomalie ou si vous recevez une information à caractère illicite, vous devez en avertir votre supérieur hiérarchique ou la direction de votre organisation.*

Utilisez les ressources informatiques dans le cadre légitime de votre activité.

—

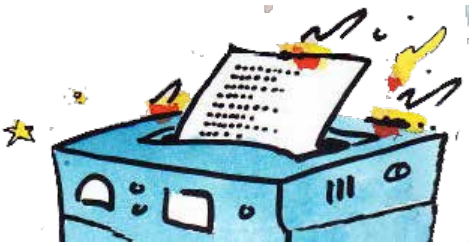
- Vous devez limiter l'utilisation des ressources informatiques de votre organisation conformément à vos **missions professionnelles**.
- L'utilisation des données de votre organisation est réservée aux seules **personnes autorisées**.

Rappel: *il est interdit de prendre connaissance* ***d'informations confidentielles*** *détenues par d'autres utilisateurs, même si ceux-ci ne les ont pas explicitement protégées.*

Ne laissez pas vos impressions sans surveillance.

—

- **N'oubliez pas vos documents confidentiels** sur les imprimantes et les photocopieuses qui ne se trouvent pas à proximité.
- Supprimez les documents en attente d'impression en cas de panne de l'imprimante.



Rappel: *méfiez-vous de* ***l'imprimante par défaut****. En effet, il ne s'agit pas toujours de celle sur laquelle vous imprimez des documents* ***confidentiels****.*

Vous êtes responsable de l'utilisation que vous faites de tout support numérique permettant la conservation des données.

—

› **L'autorisation préalable** de la direction est indispensable avant toute **utilisation** ou **introduction** de support numérique personnel sur le système d'information de votre organisation.
› L'utilisation des supports numériques est **strictement réglementée**.

Restez vigilant lorsque vous communiquez des informations.

—

› Avant toute communication, authentifiez votre **interlocuteur**.
› Dans un **lieu public**, faites attention à votre **entourage**.
› Au **téléphone** ou dans un **lieu public**, surveillez le **volume sonore** de votre voix.

Si vous devez envoyer des informations confidentielles par e-mail par exemple, utilisez un logiciel de chiffrement.

—

› Vous pouvez **chiffrer** vos **e-mails** avec un logiciel de **chiffrement**.
› Pour protéger les données sensibles, le Préposé fédéral à la protection des données recommande en particulier l'utilisation de la **cryptographie**.

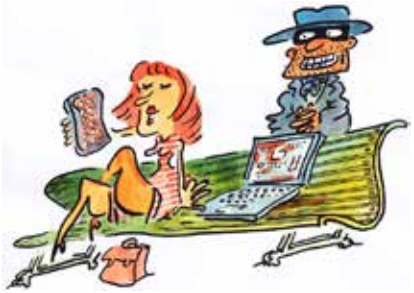
Quelques définitions:

—

› On entend par **données personnelles** (données), toutes les informations qui se rapportent à une personne identifiée ou identifiable.
› On entend par **données sensibles**, les données personnelles sur les opinions ou activités religieuses, philosophiques, politiques ou syndicales, la santé, la sphère intime ou l›appartenance à une race, des mesures d›aide sociale, des poursuites ou sanctions pénales et administratives.
› On entend par **traitement**, toute opération relative à des données personnelles - quels que soient les moyens et procédés utilisés - notamment la collecte, la conservation, l›exploitation, la modification, la communication, l›archivage ou la destruction de données.
› On entend par **fichier**, tout ensemble de données personnelles dont la structure permet de rechercher les données par personne concernée.
› On entend par **responsable de traitement**, la personne (ou l'organe public) responsable des données et de leur collecte, mais également celle qui décide du but et du contenu du fichier.
› On entend par **conseiller à la protection des données**, la personne de contact pour toutes les questions relatives à la protection des données.

Mobilité

Protégez vos équipements mobiles, comme vous protégez votre portefeuille.



- N'enregistrez pas de données trop importantes dessus.
- Ne les prêtez pas à n'importe qui.
- Ne les laissez pas trainer.

Vous êtes responsable des informations que vous emportez.

- Ne laissez **jamais** vos équipements portables **sans surveillance**. Dans la mesure du possible, cachez-les ou mettez-les **sous clé**.
- Protégez votre **écran** des **regards indiscrets** lorsque vous l'utilisez dans des **lieux publics** notamment.
- En cas de **perte ou de vol d'un appareil portable** professionnel ou privé avec accès à des informations professionnelles, annoncez immédiatement l'incident à votre supérieur hiérarchique.

Protégez l'accès aux informations qui se trouvent sur vos équipements mobiles par un mot de passe.

- Un bon mot de passe doit être **difficile à découvrir**, même par une personne qui vous connaît très bien.
- Un bon mot de passe doit être **facile à retenir**, sans que vous ayez besoin de le noter sur un **papier** pour vous en souvenir.

Ne stockez aucune donnée confidentielle sur vos équipements mobiles si elles ne sont pas chiffrées.

- Référez-vous à la **réglementation** de votre **organisation** en matière de chiffrement.

Protégez vos supports amovibles contre les logiciels malveillants.

—

› Utilisez un **logiciel antivirus** pour contrôler le contenu des supports amovibles que vous utilisez.
› Il existe des antivirus gratuits efficaces pour votre matériel personnel. Rappelez-vous de les maintenir à jour.

Ne branchez pas de clé USB sur un ordinateur ou une session avec des droits élevés (compte administrateur par exemple).

—

› Pour **limiter les actions** qu'une clé USB peut effectuer sur le système d'information, ne connectez des clés que sur des sessions avec des **droits limités**.
› Si vous disposez de droits élevés sur un ordinateur et sur le système d'information de votre organisation, soyez vigilant avec l'utilisation des supports USB. **Idéalement, utilisez une autre session (autre login) avec des droits limités**.

Nettoyez proprement le contenu de votre clé USB.

—

› Les clés peuvent contenir des **données sensibles**.
› Avant de les **prêter** ou de les **abandonner**, nettoyez leur espace de stockage, pour assurer la confidentialité de leur contenu.

Bloquez si possible l'accès à votre clé USB.

—

- Certaines clés présentent un **interrupteur physique**, qui permet de **bloquer** l'accès en écriture à la clé.
- Cet interrupteur ne **protège pas du vol** d'information, et donc des différentes problématiques de confidentialité, mais cela empêche des **éléments extérieurs** de **modifier** le contenu de la clé, ou de l'effacer **à votre insu.**

L'accès à Internet depuis un WiFi public ne garantit aucune sécurité sur la confidentialité des données téléchargées.

—

- Lors du téléchargement d'information via un WiFi public, les données sont transmises en clair.
- Rien n'indique que les données qui transitent ne sont pas surveillées par une personne **mal intentionnée** pour récupérer vos **mots de passe** ou encore des **documents confidentiels** par exemple.
- Soyez vigilant lorsque vous utilisez un **WiFi public** de ne pas télécharger de documents confidentiels. Si vous devez quand même le faire, utilisez une connexion chiffrée (**VPN**) ou système de **partage de connexion** depuis votre smartphone.

Le Bring Your Own Device (BYOD) est de plus en plus utilisé dans les milieux professionnels.

—

- Le BYOD, c'est le fait d'utiliser son appareil privé pour accéder à des informations professionnelles (e mail, agenda, applications métiers, etc.).
- Appliquez un **mot de passe** sûr sur votre smartphone privé utilisé à des fins professionnelles.

Autorité cantonale de la transparence et de la protection des données ATPrD
Rue des Chanoines 2, CH-1700 Fribourg
T +41 26 322 50 08
-
www.fr.ch/atprd
-
Avril 2019
-
Images
Pécub, Pier Paolo Pugnale
Expert en communication d'entreprise
http://www.pecub.ch/