ANTENNE RÉGION VALAIS ROMAND

# O.3 : GARANTIE DE LA SÉCURITÉ DES DONNÉES (CYBERSÉCURITÉ)

*Les prestataires IT de la commune restent les interlocuteurs de référence pour cette thématique.*
*Cette fiche doit être considérée comme indicative et n'est en aucun cas exhaustive.*

*Pour des raisons de lisibilité, sauf mention spécifique, toute dénomination de personne, de statut ou de fonction se rapporte aux personnes des deux sexes.*

## CONTEXTE

L'actualité ne manque pas de nous rappeler que la cybercriminalité est en pleine recrudescence – le secteur public n'est pas en reste.

La sécurité des données est primordiale pour une administration communale, car elle est garante de la confidentialité des données notamment lors de la récolte, du traitement, du stockage ainsi que lors d'un éventuel transfert de données à une autorité administrative tierce ou à un sous-traitant.

Certaines mesures préventives et sécuritaires doivent être mises en place par un collaborateur attitré telles que définir un plan d'action en cas de cyberattaque ce qui vous permettra de ne pas céder à la panique et d'avoir les bons réflexes lors d'une situation de crise.

## QUI ?

### Exécutif communal

L'exécutif a la responsabilité juridique de la protection des données. Il doit mettre à disposition du responsable cybersécurité les moyens nécessaires pour assurer la protection des équipements, des données et du personnel de la commune.

### Opérationnel communal

La mission principale du responsable cybersécurité est de prévenir les risques en matière de sécurité informatique en définissant des stratégies et protocoles sécuritaires.

Le responsable cybersécurité est désigné en interne, selon les circonstances, toute ou partie de l'activité cybersécurité pourra être sous-traitée. **Une formation de niveau supérieur** convient pour le rôle qui exige rigueur, précision et discrétion. Le responsable cybersécurité doit être capable de décider, d'anticiper, d'agir, de planifier et d'organiser, et posséder d'excellentes compétences en matière de communication. L'activité peut représenter entre **10 et 80% d'un EPT** selon le nombre de collaborateurs, la sensibilité des données traitées et la part de l'activité sous-traitée.

## POINTS DE CONTRÔLE

- ☐ Un responsable cybersécurité est nommé au sein de la commune et son cahier des charges est clair.
- ☐ Nous avons une stratégie et des directives claires en matière de cybersécurité.
- ☐ Nous avons récemment procédé à des audits et des contrôles de conformité aux règles de sécurité internes et externes (<3 ans).
- ☐ Nous sensibilisons et formons les collaborateurs sur la cybersécurité.
- ☐ Nous avons un plan d'action en cas de cyberattaque.
- ☐ Nous sommes dotés d'un système de veille technologique.

**Une liste de contacts** est disponible sur l'extranet de l'Antenne Région Valais romand à l'adresse suivante: **https://www.regionvalaisromand.ch/fr/fiches-thematiques-provisoires-bonnes-pratiques-1813.html**

ou accessible grâce au QR code suivant:

## ACTIONS PROPOSÉES

### 1. Nommer un responsable cybersécurité

Une personne clairement définie au sein de l'administration doit être nommée en tant que responsable cybersécurité. Un cahier des charges complet se trouve en annexe O.3.I de la présente fiche.

### 2. Adopter une stratégie claire en matière de cybersécurité

Le responsable cybersécurité identifie les risques existants et doit s'assurer de l'établissement et du maintien des politiques internes essentielles en termes de sécurité informatique qui devront être adoptées par les employés communaux.

### 3. Identifier les risques existants grâce à des audits internes / externes

Selon les compétences métiers et les ressources internes, l'organisation d'un audit technique des infrastructures par le responsable cybersécurité ou une entreprise spécialisée est impérative en vue de corrections et d'améliorations de la stratégie de sécurité.

### 4. Former et sensibiliser les collaborateurs à la cybersécurité

Il s'agit de mettre en place un programme de sensibilisation des collaborateurs par le biais de formations, des sessions de e-learning et/ou des tests de phishing.

### 5. Etablir une procédure pour faire face à une cyberattaque

Il faut être prêt à une éventuelle situation de crise en élaborant une procédure détaillant un déploiement rapide des mesures en cas de cyberattaque (autorités à contacter, sauvegarde des données, liste de contacs, cellule de crise, etc.). Il est essentiel de se conformer aux documents et aux directives transmis par le Canton du Valais.

*Annexe A.3.V* : Liste de contacts en cas d'incident informatique ou de demande de service

ANTENNE RÉGION VALAIS ROMAND

# O.3 : GARANTIE DE LA SÉCURITÉ DES DONNÉES (CYBERSÉCURITÉ)

*Les prestataires IT de la commune restent les interlocuteurs de référence pour cette thématique.*
*Cette fiche doit être considérée comme indicative et n'est en aucun cas exhaustive.*

*Pour des raisons de lisibilité, sauf mention spécifique, toute dénomination de personne, de statut ou de fonction se rapporte aux personnes des deux sexes.*

## ACTIONS PROPOSÉES (SUITE)

Nul n'est à l'abri d'une cyberattaque ! Il est impossible de prédire quand cette dernière va se dérouler. Une stratégie en matière de cybersécurité permet non seulement de réduire la probabilité d'une attaque informatique, mais également de limiter les dégâts causés par une attaque. Avoir un plan d'action en cas de cyberattaque vous permettra de ne pas céder à la panique et d'avoir les bons réflexes. Cette procédure concerne non seulement le responsable de la sécurité informatique, mais également tous les employés communaux.

*Annexe O.3.V* : Fiche de survie à une cyberattaque

### 6. Mettre en place un système de veille technologique et se tenir informé des évolutions technologiques et réglementaires

L'innovation, le développement technologique et les réglementations en lien avec l'administration numérique sont en constante évolution. La veille technologique vous permettra d'être systématiquement à jour sur la thématique de la cybersécurité et sur les modifications des réglementations en matière de protection des données.

## ANNEXES / RÉFÉRENCES

O.3.I : Cahier des charges pour responsable cybersécurité
O.3.II : Fiche d'aide sur les mots de passe
O.3.III : Guide pour l'identification des courriels frauduleux
O.3.IV : Courrier de vérification pour le mot de passe
O.3.V : Fiche de survie à une cyberattaque
O.3.VI : Mémo : Sécurité numérique pour les administrations communales

ANTENNE RÉGION VALAIS ROMAND

ANNEXE 0.3 : GARANTIE DE LA SÉCURITÉ DES DONNÉES (CYBERSÉCURITÉ)

# I : CAHIER DES CHARGES POUR LE RESPONSABLE CYBERSÉCURITÉ

*Le prestataire IT de la commune reste l'interlocuteur de référence pour cette thématique.*
*Cette fiche doit être considérée comme indicative et n'est en aucun cas exhaustive.*

## PROFIL

**Le responsable de la cybersécurité** devrait être désigné en interne. Toutefois, selon les circonstances et en fonction des ressources disponibles, il se peut que l'intégralité ou une partie des activités de cybersécurité soient mutualisées avec d'autres administrations communales ou sous-traitées.

**Une formation de niveau supérieur** – idéalement dans le domaine de la cybersécurité - convient pour le rôle qui exige rigueur, précision et discrétion. Le responsable de la cybersécurité doit être capable de décider, d'agir, de planifier et d'organiser, et posséder d'excellentes compétences en matière de communication, car il devra sensibiliser, superviser et informer les employés communaux.

**L'activité peut représenter entre 10 et 80% d'un EPT** selon le nombre de collaborateurs, la sensibilité des données traitées et la part de l'activité sous-traitée.

## RESPONSABILITÉ ET CADRE LÉGAL

**Le responsable de la cybersécurité** élabore la politique de sécurité de l'information pour son organisation. Il n'est pas seulement garant de **sa mise en œuvre**, mais il en assure également **le suivi**. Il protège la commune des risques liés aux cyberattaques, tels que les ransomwares ou autres attaques informatiques. Il supervise la réalisation de projets tels que l'élaboration de règlements et la définition des exigences de sécurité interne, afin de garantir l'adhésion et la conformité de tous les employés (changement de mot de passe, etc.) ou le suivi de nouveaux systèmes d'information. Il doit être intégré dans les projets informatiques pour donner les prescriptions en lien avec la sécurité.

**L'exécutif a la responsabilité juridique de la protection des données**. Il doit mettre à disposition du responsable cybersécurité les moyens nécessaires pour assurer la protection des équipements, des données et du personnel de la commune.

## TÂCHES ET MISSIONS PRINCIPALES

### 1. Identifier les risques existants et définir une stratégie de sécurité informatique (prévention des risques)

Grâce à un ou des audits internes ou externes et selon les ressources disponibles, le responsable cybersécurité identifie les risques existants et les répertorie selon leur gravité. Il pourra ainsi implanter une stratégie et des protocoles de sécurité informatique (Système de sauvegarde, Firewall, directives de télétravail, méthode d'authentification à 2 facteurs (2FA) par exemple à l'envoi d'un code unique par SMS, etc.).

Il participera à la définition des procédures et la gestion des incidents de sécurité et de cybersécurité.

Il devra à minima :

1. Identifier les besoins d'audit de sécurité lors des analyses de solutions et préparer l'appel d'offres en coordination avec l'exécutif.
2. Assurer le suivi de la mise en place des recommandations résultants des audits de sécurité et effectuer les contrôles de validation y afférant.

Pour aller plus loin, selon le contexte et sa formation, il pourra :

3. Suivre et réaliser des projets d'amélioration des contrôles de sécurité ou informatiques.
4. Suivre et/ou planifier des audits du processus de gestion de la cybersécurité.

### 2. Mettre en place la stratégie de cybersécurité

Le responsable cybersécurité suit l'implémentation cohérente de la stratégie, la pérennité et la sécurité de l'ensemble des moyens informatiques dans le cadre de la stratégie numérique. Il accompagne la mise en œuvre opérationnelle de la cybersécurité dans les projets d'évolution de l'organisation.

Il devra à minima :

1. Définir en équipe la stratégie de sécurité de l'information de l'administration sous la coordination de l'exécutif.
2. Participer activement au pilotage de la cybersécurité et coordonner le suivi des risques de sécurité dans un souci constant d'efficacité par rapport aux coûts induits.

# I : CAHIER DES CHARGES POUR LE RESPONSABLE CYBERSÉCURITÉ

*Le prestataire IT de la commune reste l'interlocuteur de référence pour cette thématique.*
*Cette fiche doit être considérée comme indicative et n'est en aucun cas exhaustive.*

## TÂCHES ET MISSIONS PRINCIPALES (SUITE)

Pour aller plus loin, selon le contexte et sa formation, il pourra :

3. Contribuer activement à la définition du programme de cybersécurité et s'assurer de sa mise à jour continue pour couvrir adéquatement les risques IT et protéger les actifs de la commune.
4. Analyser et identifier les technologies clés dans le domaine de la cybersécurité.
5. Participer aux décisions stratégiques relatives à la sécurité de l'information de l'administration.

### 3. Former et sensibiliser les collaborateurs à la cybersécurité

Le responsable cybersécurité s'assure que toutes personnes ayant accès aux systèmes d'information de l'organisation soient formées et sensibilisées à la sécurité de l'information et aux bons comportements vis-à-vis des risques de sécurité et des cyberrisques – notamment dans le cadre du télétravail.

Il devra à minima :

1. S'assurer de la formation et de la sensibilisation de toutes personnes et populations de l'administration, y compris les spécialistes externes.

Pour aller plus loin, selon le contexte et sa formation, il pourra :

2. Participer proactivement à la sensibilisation et à la formation du personnel afin de réduire les comportements à risque pouvant impacter la sécurité des données personnelles ou sensibles de l'organisation et les former sur les réflexes à adopter en cas de cyberattaque.
3. Proposer des solutions et faciliter la compréhension des risques de sécurité en vulgarisant les concepts techniques sous-jacents.
4. En coordination avec l'exécutif communal, informer les collaborateurs et les populations de l'administration des nouvelles menaces ou des risques de sécurité importants pour les informations et données de l'organisation.

*Annexe O.3.VI :* Mémo : Sécurité numérique pour les employés communaux

### 4. Maintien de l'infrastructure / stratégie de cybersécurité et veille technologique

Le responsable cybersécurité suit l'implémentation cohérente de la stratégie. Un rôle de veille technologique et en sécurité est inhérent à sa fonction. Il doit non seulement suivre les évolutions technologiques et réglementaires en termes de cybersécurité, mais également rester informé du cadre légal demandé par le canton et la confédération. Il identifie les risques de sécurité de l'information et préconise les contrôles à implémenter. Il participera à la définition des procédures et la gestion des incidents de cybersécurité.

Il devra à minima :

1. Collaborer aux projets informatiques critiques pour s'assurer que les problèmes de sécurité sont abordés tout au long du cycle de vie du projet.
2. Valider contractuellement les responsabilités et les exigences envers les prestataires informatiques et des sous-traitants.
3. Assurer la veille en sécurité permettant à l'administration d'anticiper les évolutions technologiques nécessaires et de couvrir de nouvelles failles de sécurité.
4. Fournir périodiquement et à la demande des tableaux de bord de pilotage de la sécurité aux membres de l'exécutif communal.

Pour aller plus loin, selon le contexte et sa formation, il pourra :

5. Assurer un rôle d'expert dans le développement d'applications ou les projets d'acquisition pour évaluer les exigences et les contrôles de sécurité et coopérer à leur mise en œuvre.
6. Contribuer activement à la définition de l'architecture sécurité du système d'information afin d'offrir à l'organisation une protection périphérique et interne optimale face à l'évolution des cybermenaces et autres risques pouvant compromettre la sécurité des systèmes d'information.
7. Définir et accompagner l'implémentation des contrôles sécurité critiques dans le système d'information.
8. Participer à la définition de procédures de gestion d'incidents dans le domaine de la cybersécurité en adéquation avec les processus de détection et de réaction de l'organisation.

ANTENNE RÉGION VALAIS ROMAND

# II: FICHE D'AIDE SUR LES MOTS DE PASSE

*Le prestataire IT de la commune reste l'interlocuteur de référence pour cette thématique.*
*Cette fiche doit être considérée comme indicative et n'est en aucun cas exhaustive.*

## CONTEXTE

Une grande majorité des violations concernent des mots de passe faibles ou des informations d'identification compromises.

Une bonne gestion des mots de passe et favoriser l'identification à deux facteurs (A2F) sont les clés essentielles pour se protéger.

Ce guide présente les règles de base et les bonnes pratiques pour construire, gérer et « conserver » vos mots de passe.

## QUI ?

### Commune

L'identification de l'utilisateur est nécessaire pour la bonne gestion des données et des responsabilités. Chaque collaborateur doit être en mesure de s'identifier de façon unique. Habituellement, la responsabilité de créer et conserver (en mémoire) un mot de passe unique est confié au collaborateur.

### Prestataire IT

Il peut arriver que le prestataire soit responsable de la création des mots de passe. Il doit dans ce cas s'assurer que les mots passe soient forts et que le collaborateur ait la possibilité de le retenir (sans post-it et sans fichier Excel). Le prestataire peut aussi configurer le système pour que, lors de la création du mot de passe, sa complexité soit garantie.

## UN MOT DE PASSE SÉCURISÉ ?

### Un mot de passe fort en 6 points :

1. Un mot de passe doit être composé de 12 caractères au minimum.
2. Il doit contenir des lettres, des chiffres ainsi que des caractères spéciaux ($,[,,°,§,¬,…).
3. Aucun lien avec votre vie de famille ainsi qu'aucune suite logique (12,3, 4,…/QWERTZ,…) ne doivent être utilisés. (L'ingénierie sociale permet de deviner le nom du chien).
4. Ne pas utiliser de mots du dictionnaire.
5. Ne partagez pas vos mots de passe en aucun cas avec autrui !
6. Utilisez un mot de passe différent pour chaque compte d'accès.

Règles optionnelles permettant d'éviter de modifier ses mots de passe à intervalle régulier :

1. Favorisez l'**authentification à 2 facteurs (2FA)** car elle permet de renforcer la sécurité lors d'une connexion à internet. Cette méthode consiste vérifier deux fois l'identité de l'utilisateur :

   I. Mot de passe;

   II. Code reçu par SMS ou sur une application mobile lors de chaque connexion.

2. L'utilisation d'un gestionnaire de mots de passe est une solution sûre (KeePass, SecureSafe, Password Safe, etc.) :
   - Les données sont chiffrées et bien protégées.
   - Certains mots de passe peuvent être partagés (par exemple pour accéder au site Internet d'un journal local, etc.).
   - Elle nécessite **un seul mot de passe** (très) fort.

### Liens :

Choisissez une phrase facile à mémoriser et élaborez votre mot de passe en prenant la première lettre de chaque mot et en incluant la ponctuation et les chiffres :

« Ma fille Tamara Meier fête son anniversaire le 19 janvier ! »

Vous obtenez alors une chaîne de caractères apparemment arbitraire, mais facile à mémoriser :

« MfTMfsal19j ! »

Testez votre mot de passe ici ! **https://www.passwortcheck.ch/fr**
Vérifiez si votre courriel est compromis ! **https://haveibeenpwned.com**

ANTENNE RÉGION VALAIS ROMAND

ANNEXE 0.3 : GARANTIE DE LA SÉCURITÉ DES DONNÉES (CYBERSÉCURITÉ)

# III : GUIDE POUR L'INDENTIFICATION DES COURRIELS FRAUDULEUX

*Le prestataire IT de la commune reste l'interlocuteur de référence pour cette thématique.*
*Cette fiche doit être considérée comme indicative et n'est en aucun cas exhaustive.*

## COURRIELS SUSPECTS

Les arnaques sur internet se multiplient et les administrations publiques ne sont pas épargnées.

Les malfrats récoltent des informations en amont afin d'usurper l'identité d'une personne de votre entourage ou de récolter des informations vous concernant dans le but de faire du chantage – notamment en menaçant de divulguer ou d'effacer des données en créant une situation d'urgence. Souvent, ils vous inciteront à cliquer sur une pièce jointe ou à obtenir votre identifiant et votre mot de passe. Ces arnaques peuvent se présenter sous forme de concours, tests en tout genre, programmes gratuits, jeux gratuits…

### Comportements à adopter en cas de doute

Avant d'ouvrir **un courriel suspect** :

1. Demandez-vous si vous connaissez l'émetteur du courriel et si vous attendez un courriel de sa part.
2. Vérifiez le courriel de l'émetteur, car lors d'une tentative d'escroquerie l'adresse utilisée ressemble, mais ne correspond pas à l'adresse courriel originale (par exemple : contact@**g**gmail.com).
3. Méfiez-vous des courriels avec des salutations impersonnelles (Monsieur, Cher partenaire, etc.).
4. Soyez prudent aux courriels qui vous demandent d'effectuer une action urgente ou qui vous profèrent des menaces.
5. Une administration publique ou un prestataire informatique ne vous demandera jamais votre mot de passe. Ne répondez pas à ce genre de demande. En cas de doute, contactez directement la personne par téléphone afin de vérifier l'identité de l'auteur de la demande.
6. Ne cliquez pas sur les liens d'un courriel suspect et surtout ne téléchargez pas **les pièces jointes**, car ces dernières peuvent contenir des logiciels malveillants tels que des chevaux de Troie.

Veuillez trouver des informations complémentaires et les références sur les pages internet suivantes :

- Escroquerie sur internet : **https://www.skppsc.ch/fr/sujets/escroquerie/escroquerie/**
- Hameçonnage (phishing) : **https://www.ibarry.ch/fr/risques-sur-internet/phishing/**
- Centre national pour la cybersécurité (NCSC) : **https://www.ncsc.admin.ch/ncsc/fr/home.html**

Contrôler un lien ou un site internet !
Plateforme de sécurité Internet :
**https://checkawebsite.ibarry.ch/fr/home/Home**

ANTENNE RÉGION VALAIS ROMAND

ANNEXE 0.3 : GARANTIE DE LA SÉCURITÉ DES DONNÉES (CYBERSÉCURITÉ)

# IV : COURRIER DE VERIFICATION POUR LE MOT DE PASSE

*Le prestataire IT de la commune reste l'interlocuteur de référence pour cette thématique.*
*Cette fiche doit être considérée comme indicative et n'est en aucun cas exhaustive.*

## MOTS DE PASSE

### Courriers types pour votre prestataire IT

Exemple :

**Objet : Vérification de la configuration de création des mots de passe**

Cher Monsieur Prestataire IT,

Dans le cadre de la revue de nos exigences sur la cybersécurité nous souhaitons nous assurer que tous nos mots de passe ont une longueur de 12 caractères au minimum dont des caractères spéciaux, des majuscules, minuscules et chiffres.

Pouvez-vous nous confirmer que la configuration de notre connexion lors de la création de comptes impose cette complexité lors de la création des mots de passe.

Je vous remercie pour votre retour et votre confirmation écrite. Je reste à disposition pour toute question supplémentaire.

Meilleures salutations,

Dans le cas d'un hébergement de l'application chez le prestataire, exigez la mise en place de l'**authentification à 2 facteurs (2FA)!**

ANTENNE RÉGION VALAIS ROMAND

ANNEXE 0.3 : GARANTIE DE LA SÉCURITÉ DES DONNÉES (CYBERSÉCURITÉ)

# V : FICHE DE SURVIE À UNE CYBERATTAQUE

*Le prestataire IT de la commune reste l'interlocuteur de référence pour cette thématique.*
*Cette fiche doit être considérée comme indicative et n'est en aucun cas exhaustive.*

## PROCÉDURE EN CAS DE CYBERATTAQUE

### Les mesures urgentes à prendre en cas d'incident ou de suspicion de cyberattaque

Une cyberattaque peut se manifester par une perte de données, par une prise de contact suspicieuse (demande de rançon ou de mot de passe …) ou par un comportement inhabituel de vos ressources informatiques (applications, serveurs, etc).

**Les bons réflexes :**

1. Déconnectez votre informatique du réseau extérieur. Il est nécessaire d'isoler votre ordinateur du réseau en coupant toutes les connexions internet et VPN afin de stopper l'intrusion et ainsi d'éviter la propagation de l'attaque. En revanche, n'éteignez pas votre ordinateur. Cela permettra de faire une analyse détaillée de l'attaque.
2. Contactez immédiatement (de préférence par téléphone) le responsable de la sécurité de votre commune ou votre supérieur hiérarchique ainsi que le prestataire informatique qui pourra vous guider dans les premières mesures techniques à prendre.

*Annexe A.3.V* : Liste de contacts en cas d'incident informatique ou de demande de service

3. Prévenez immédiatement la Police cantonale (117). Elle vous redirigera vers des spécialistes et vous guidera dans les premières démarches administratives.
4. Constituez une cellule de gestion de crise afin de piloter les actions des différentes composantes concernées (technique, RH, financière, communication, juridique…). Il est conseillé de définir préalablement les acteurs qui seront partie prenante à la cellule de crise.
5. Dans la mesure du possible, procédez à une copie physique (sauvegarde hors-ligne) du disque de votre ordinateur. Cette sauvegarde doit être séparée du réseau.
6. Annoncez l'incident auprès des autorités compétentes :
   a. Au Centre national pour la cybersécurité (NCSC) : **https://www.report.ncsc.admin.ch/fr/**
   b. À la cellule de cybersécurité de l'administration cantonale : **cybersecurity@admin.vs.ch**
   c. Au Préposé à la protection des données en cas de vol avéré ou potentiel de données personnelles.

**Protection des données et transparence (PPDT)**
Me Lauris Loat
Préposé cantonal à la protection des données et à la transparence
Tél. 027 288 29 00
**prepose@parl.vs.ch**

**Veuillez vous référer à la fiche proposée par le Canton du Valais.**

ANTENNE RÉGION VALAIS ROMAND

# VI : MÉMO : SÉCURITÉ NUMÉRIQUE POUR LES ADMINISTRATIONS COMMUNALES

*Le prestataire IT de la commune reste l'interlocuteur de référence pour cette thématique.*
*Cette fiche doit être considérée comme indicative et n'est en aucun cas exhaustive.*

## LA SÉCURITÉ NUMÉRIQUE AU QUOTIDIEN

### Les gestes barrières pour votre sécurité numérique

En prévention et afin d'optimiser votre sécurité numérique, voici 5 actions à appliquer quotidiennement :

#### 1. Sauvegarder les données → www.ebas.ch/step1

Pour prévenir une perte de données qui peut survenir lors d'une fausse manipulation, d'un problème technique ou d'une cyberattaque, il nécessaire de :

- Sauvegarder régulièrement ses données sur un disque dur externe ou une plateforme en ligne de stockage agrée (cloud) selon les directives transmises par le responsable cybersécurité.
- S'assurer que les données ont bien été copiées et qu'elles peuvent être restaurées aisément.
- Limiter dans le temps la connexion au disque dur externe ou à la plateforme de stockage en ligne afin d'éviter toute intrusion.

#### 2. Surveiller avec l'antivirus et le pare-feu (firewall) → www.ebas.ch/step2

L'utilisation accrue d'internet expose la commune à de nouveaux dangers. Une protection adaptée doit impérativement être mise en place.

- Installez un antivirus et s'assurer que la mise à jour automatique est active.
- Scannez régulièrement votre système informatique afin de s'assurer que votre poste de travail n'a pas été infecté.
- Le pare-feu de votre ordinateur doit toujours être actif lors d'une connexion à internet.

#### 3. Prévenir avec les mises à jour logicielles → www.ebas.ch/step3

Les logiciels, les applications ou un système d'exploitation obsolètes ne sont plus en mesure de garantir une cybersécurité optimale.

- Ne téléchargez que des programmes ou logiciels dont vous avez besoin et seulement depuis les sites officiels des prestataires.
- Assurez-vous que tous vos logiciels et que votre système d'exploitation soient à jour en activant la mise à jour automatique.

#### 4. Protéger les accès Internet → www.ebas.ch/step4

Des actions simples vous permettront de limiter les intrusions indésirables.

1. **Verrouillez** votre poste de travail lorsque vous vous absentez même pour une courte durée.
2. Utilisez **des mots de passe forts** (minimum 12 caractères incluant des minuscules, des majuscules, des caractères spéciaux et des chiffres).
3. Pensez à utiliser **un gestionnaire de mots de passe** qui vous garantira une centralisation de tous les mots de passe, un excellent chiffrement et une bonne protection des données. Il nécessite un seul mot de passe (KeePass, SecureSafe, Password Safe,...).
4. Ne réutilisez pas le même mot de passe pour différents comptes d'utilisateur.
5. Favorisez **l'authentification à 2 facteurs (2FA)** qui permet la double vérification de l'identité d'un utilisateur par un mot de passe et un code reçu par SMS ou via une application.
6. Utiliser **un VPN** lorsque vous vous connectez sur un WIFI externe cela permet de chiffrer et de sécuriser la connexion entre votre ordinateur et internet.

#### 5. Faire attention et être vigilant → www.ebas.ch/step5

Avant de communiquer vos données personnelles et financières, il est nécessaire de clarifier la nature de la demande, notamment en vérifiant le courriel de l'expéditeur avant d'ouvrir une pièce jointe. Une autorité ou une entreprise ne vous demandera jamais votre mot de passe. En cas de doute, n'hésitez pas à contacter la personne par téléphone.