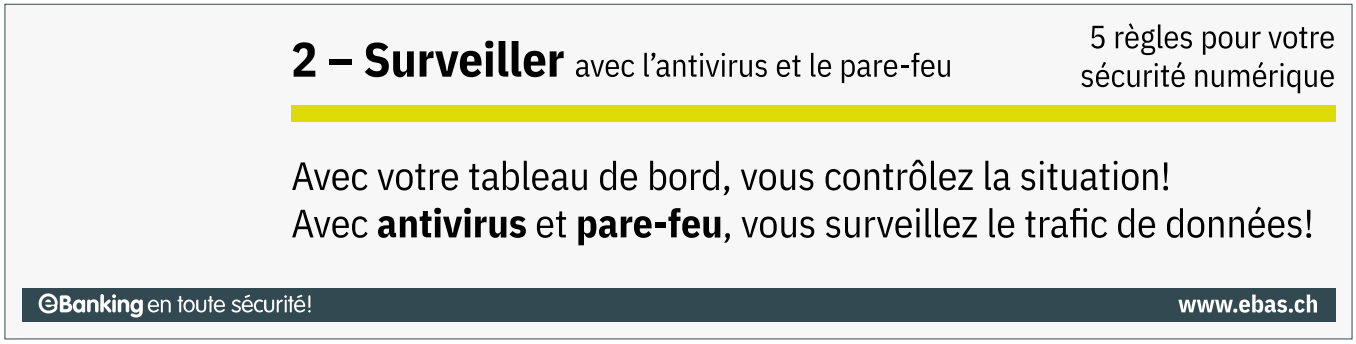
2 – Surveiller avec l'antivirus et le pare-feu

Quelles « portes » votre dispositif laisse-t-il ouvertes et quels virus viennent s'y présenter ? Dans la pratique aucune, si vous avez activé un pare-feu et installé un programme de protection antivirus.

Principaux conseils à suivre :

- Utilisez un programme antivirus et activez la fonction de mise à jour automatique.
- Vérifiez régulièrement que votre dispositif n'a pas été infecté en procédant à un scan complet du système.
- Activez le pare-feu embarqué de Windows ou mac OS avant de connecter votre dispositif à Internet ou à tout autre réseau.



Comment procéder

Utilisez un programme antivirus et un pare-feu, avec les mises à jour automatiques activées, pour rester toujours protégé contre les nouvelles menaces.

Windows

Windows 10 est livré avec un pare-feu et l'antivirus « Windows Defender » activés par défaut. Cette protection est optimale.

Si vous souhaitez ajouter d'autres fonctions, comme par exemple un contrôle parental etc., voici une liste (non exhaustive) de produits, dont certains gratuits :

- AVG Free Anti-Virus (https://free.avg.com)
- Avira Free Antivirus (https://www.avira.com)
- Bitdefender (https://www.bitdefender.de)
- F-Secure (https://www.f-secure.com)
- G Data (https://www.gdata.de)

- Kaspersky (https://www.kaspersky.de)
- Malwarebytes (https://www.malwarebytes.com)
- McAfee (https://www.mcafee.com)
- Norton (https://ch.norton.com)
- Panda (https://www.pandasecurity.com)
- Sophos (https://www.sophos.com)
- Trend Micro (https://www.trendmicro.com)

macOS

Sous macOS, vous devez absolument activer le pare-feu embarqué qui lui est désactivé par défaut. Pour cela, cliquer sur « Préférences Système » dans le menu « Apple ». Cliquer sur « Sécurité » puis sur le bouton « Coupe-feu » pour activer le pare-feu. Ce dernier restera activé lors des prochains redémarrages.

Mac OS X dispose aussi d'un système de protection intégré dont la mission est d'empêcher toute intrusion de malwares. Le programme activé par défaut « Gatekeeper » permet également d'éviter d'installer par erreur des logiciels malveillants.

Des antivirus spécialisés peuvent apporter une protection supplémentaire. Voici une liste (non exhaustive) de programmes de protection (dont certains gratuits), capables de détecter également les virus Windows :

- AVG (https://free.avg.com)
- Avira (https://www.avira.com)
- Bitdefender (https://www.bitdefender.de)
- F-Secure (https://www.f-secure.com)
- Kaspersky (https://www.kaspersky.de)
- Norton (https://ch.norton.com)
- Trend Micro (https://www.trendmicro.com)

Smartphone und Tablet

Un pare-feu est plus compliqué à installer sur un smartphone ou une tablette. Sur les dispositifs Android, l'utilisateur doit disposer de droits root, tandis que sur un iPhone, il est nécessaire de procéder à un « jail-break » (débridage) de l'appareil. Ce genre d'opération (l'obtention des droits root ou le jailbreak) risque d'endommager votre appareil et de désactiver différents mécanismes de sécurité du système d'exploitation. Cela risque également de vous faire perdre tous les droits de garantie. Nous vous conseillons donc de ne pas vous aventurer dans ce genre de manipulation.

Pour les utilisateurs d'**Android** en revanche, il est absolument indispensable d'installer un antivirus. Nous vous conseillons donc d'installer un des programmes antivirus suivants, certains étant disponibles gratuitement :

- AhnLab (https://www.ahnlab.com)
- AVG (https://free.avg.com)

- Avira (https://www.avira.com)
- Bitdefender (https://www.bitdefender.de)
- G Data (https://www.gdata.de)
- Kaspersky (https://www.kaspersky.de)
- McAfee (https://www.mcafee.com)
- Norton (https://ch.norton.com)
- Sophos (https://www.sophos.com)
- Trend Micro (https://www.trendmicro.com)

Il n'existe pour le moment aucun programme antivirus pour les **dispositifs iOS** (tels que iPhone ou iPad). Cela s'explique par la fermeture de leur système d'exploitation qui doit empêcher l'installation d'applications suspectes ou autres logiciels malveillants, et limite fortement les autorisations des applications installées.

Protégez vos données et tous vos dispositifs en suivant les « 5 règles pour votre sécurité numérique » :

Règle n°1 – Sauvegarder (https://www.ebas.ch/fr/1-sauvegarder-les-donnees/)

Règle n°2 – Surveiller

Règle n°3 – Prévenir (https://www.ebas.ch/fr/3-prevenir-avec-les-mises-a-jour-logicielles/)

Règle n°4 – Protéger (https://www.ebas.ch/fr/4-proteger-les-acces-internet/)

Règle n°5 – Faire attention (https://www.ebas.ch/fr/5-faire-attention-et-etre-vigilant/)

Pour aller plus loi

Que faire en cas d'infection par un logiciel malveillant ?

Vous trouverez ici (https://www.ebas.ch/fr/les-infections-par-malware/) des informations supplémentaires sur la procédure à suivre si vous redoutez que votre dispositif ait été infecté, ou si votre antivirus vous signale la présence d'un logiciel malveillant.

À quoi sert un pare-feu ?

Lorsque les internautes naviguent sur Internet depuis leur ordinateur, tablette ou smartphone, des « portes d'accès » invisibles (ports) s'ouvrent sur les différents dispositifs. L'ouverture de ces portes expose ainsi les dispositifs aux attaques des cybercriminels. Une fois installé, le pare-feu réduit autant que possible l'ouverture de ces portes et surveille le trafic de données entre les dispositifs et la toile. Le pare-feu tire la sonnette d'alarme dès qu'il détecte un trafic suspect.