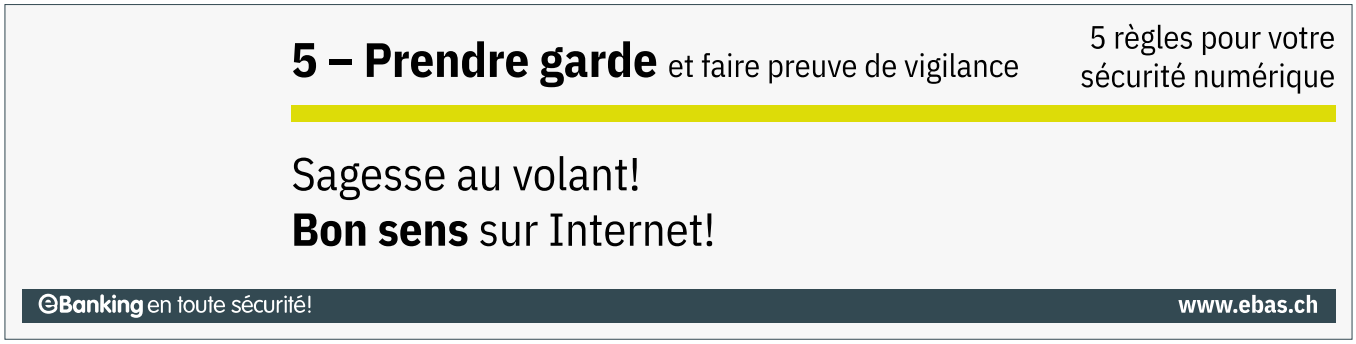
5 – Faire attention et être vigilant

Croyez-vous vraiment à tout ce que l'on vous raconte ? Exercez votre sens des responsabilités et restez toujours méfiant lorsque vous surfez sur Internet.

Principaux conseils à suivre :

- Soyez toujours prudent lorsque vous surfez sur Internet et réfléchissez bien avant de communiquer vos données personnelles.
- Les instituts financiers, les opérateurs téléphoniques ou autres fournisseurs de service ne vous demanderont jamais (ni par email, ni par téléphone) de leur communiquer votre mot de passe, ni de le modifier.
- Lorsque vous utilisez vos dispositifs mobiles, vous devez appliquer les mêmes mesures de précaution que celles que vous observez normalement sur votre ordinateur fixe à la maison.
- En cas d'incertitude ou si vous craignez avoir été victime d'une attaque, n'hésitez pas à demander de l'aide.



Les 4 premières règles vous ont permis de très bien sécuriser vos dispositifs et vos accès en ligne d'un point de vue technique. Or le comportement des utilisateur·ice·s continue de représenter le principal risque, au point de constituer la cible des attaques. À vous donc d'agir en conséquence en vous armant de bon sens.

Se protéger contre le phishing (hameçonnage) et les attaques d'ingénierie sociale

Dans le cas du phishing (https://www.ebas.ch/fr/le-phishing/), les escrocs tentent de gagner la confiance des utilisateurs à travers des messages envoyés par courriel ou par SMS, mais aussi par téléphone, en se faisant passer par exemple pour leur institut financier, dans le but de les attirer sur un site web (via un lien hypertexte) ressemblant comme deux gouttes d'eau à celui de leur banque. Si vous tombez dans le piège et que vous communiquez vos identifiants et codes d'accès, vous leur donnez la possibilité de dévaliser votre compte en toute tranquillité.

Dans le cadre d'une arnaque par téléphone (https://www.ebas.ch/fr/arnaques-par-telephone-les-faux-services-dassistance/), vous pouvez en revanche être contacté par de faux collaborateurs de Microsoft ou d'une société d'assistance informatique qui tenteront par tous les moyens d'accéder à votre dispositif.

N'oubliez jamais qu'un institut bancaire sérieux ne vous demandera, ni par mail ni par téléphone, de lui communiquer vos données d'accès à son service de banque en ligne.

Pour porter de telles attaques, les cyberpirates utilisent souvent les informations glanées dans les réseaux sociaux (https://www.ebas.ch/fr/les-reseaux-sociaux/). Faites donc preuve de prudence et réfléchissez bien (https://www.ebas.ch/fr/respect-de-la-vie-privee-et-protection-des-donnees-personnelles-sur-internet/) avant de publier des informations vous concernant.

Des risques accrus pour les dispositifs mobiles

Les droits d'accès pour les applications mobiles

De nombreuses applis accordent sans raison apparente des droits d'accès illimités. Or, les applications ne nécessitent pas toutes d'accéder par exemple à la position géographique, au répertoire des contacts ou au statut du téléphone. Lorsque vous accordez tel ou tel droit d'accès, réfléchissez s'il est vraiment nécessaire au fonctionnement de l'application et désactivez tous les droits superflus.

En règle générale, il convient d'être très prudent quand il s'agit de communiquer votre position géographique. Évitez les services de localisation et ne stockez pas la position géographique des photos que vous transmettez sur Internet. Voleurs et hackers pourraient utiliser ces informations à vos dépens.

Verrouiller immédiatement en cas de perte

Différentes applications permettent de verrouiller à distance les dispositifs perdus ou volés et de supprimer les données qui y sont stockées pour qu'elles ne soient plus accessibles. Mais attention : ces commandes peuvent également être utilisées par des personnes malintentionnées. À vous donc de vérifier la fiabilité de l'application. Une fois votre dispositif verrouillé, il convient de prendre contact avec votre opérateur de téléphonie mobile pour désactiver votre carte SIM.

Demander de l'aide

En cas d'incertitude ou si vous avez été –ou pensez avoir été – la victime d'une attaque, n'hésitez pas à demander de l'aide. En particulier :

- Contactez votre institut financier (https://www.ebas.ch/fr/partenaires/) en cas de doute ou d'incertitude lors de vos opérations d'e-banking.
- En cas de problème technique ou si vous suspectez la présence d'un logiciel malveillant, demandez conseil et assistance à un informaticien.
- Si vous avez été la victime d'une attaque, contactez votre institut financier (https://www.ebas.ch/fr/partenaires/) et la police (https://polizei.ch).

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 (https://www.ebas.ch/fr/2-surveiller-avec-lantivirus-et-le-pare-feu/)
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