CYBERSÉCURITÉ
Les bons gestes à adopter

**Arnaques numériques ? Pas de panique !
Dans cette infographie, VOé vous donne
les clés pour mieux vous protéger.**

DOUBLE AUTHENTIFICATION :

Processus qui permet de renforcer la sécurité de votre compte (en plus de votre mot de passe, vous devez saisir un code fourni par SMS, e-mails ou via une application pour valider votre connexion).

KÉASACO

INGÉNIERIE SOCIALE

Technique de manipulation psychologique utilisée par les cybercriminels pour vous inciter à partager vos informations confidentielles.

GESTIONNAIRE DE MOTS DE PASSE

Logiciel sécurisé qui regroupe tous vos mots de passe derrière un mot de passe unique.

CATFISHING

Ruse qui consiste à créer une identité fictive sur un réseau social pour vous extorquer de l'argent.

PHISHING (OU HAMEÇONNAGE)

Pratique qui a pour but de récupérer vos informations personnelles en vous connectant à un site qui usurpe l'identité d'un site de confiance (banque, institution publique, etc.).

Comment protéger mes données personnelles ?

L'ingénierie sociale vise à vous faire réagir émotionnellement ("Regarde, tu étais dans cette vidéo !" par exemple) pour vous pousser à cliquer sur le lien.
Le risque ? Atterrir sur un site de phishing et télécharger un logiciel malveillant ou vous faire voler vos données personnelles par un cybercriminel.

Nos conseils :

Activez la double authentification :

En cas de mot de passe volé, vous recevrez un code de double authentification qui empêchera le pirate informatique de se connecter à votre compte.

Définissez un mot de passe unique et complexe :

Privilégiez un mot de passe difficile pour chacun de vos comptes (+ de 12 caractères avec des majuscules, minuscules, chiffres et symboles).

Suivez l'actualité liée au numérique :

Les piratages se multiplient ? C'est le bon moment pour changer de mot de passe et en définir un plus sûr !

Soyez vigilant(e) :

Ne cédez pas aux propositions trop alléchantes, ne cliquez pas sur les liens qui vous semblent suspects et ne partagez pas vos données sensibles.

Vous avez fait une rencontre sur le net ?

Si vous pensez avoir rencontré l'âme sœur, restez attentif : il s'agit peut-être d'un catfisher qui tentera de vous extorquer de l'argent sous divers prétextes (payer des frais médicaux, quitter son pays pour vous rejoindre, etc.).

Nos conseils :

Faites une recherche inversée par image (via des applications comme Reversee ou Search by image): cela vous permettra de voir si la photo de profil ne correspond pas à quelqu'un d'autre

Assurez-vous d'avoir un **échange physique ou vidéo** pour constater de la véracité de son identité.

Comment réagir face aux SMS et e-mails frauduleux ?

Vous avez un colis en attente et vous devez cliquer sur le lien pour le récupérer ? Attention : arnaque ! Les cybercriminels privilégient de plus en plus les e-mails et les SMS, car ce sont les canaux de communication sur lesquels nous sommes le moins vigilants.

Nos conseils :

Ne cliquez pas sur le lien :

Tapez l'adresse dans votre navigateur et vérifiez que les résultats qui apparaissent soient dignes de confiance.

Appelez les institutions concernées :

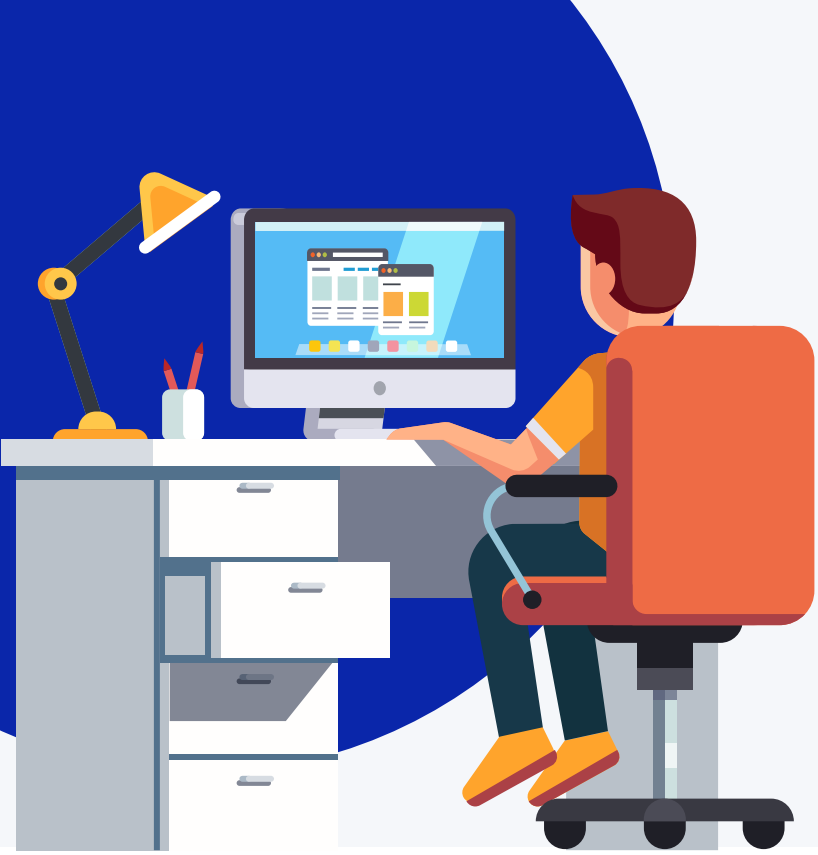
Vérifiez auprès de votre banque s'il y a eu une transaction, auprès de la Poste si vous attendez un colis,etc...

Encore une fois :

Soyez vigilant(e) et méfiez-vous des messages qui vous semblent suspects.

Faut-il porter plainte ?

Vous avez été victime ou témoin d'une arnaque ? Signalez-le au Centre National pour la Cybersécurité (NCSC) en déposant une plainte via le formulaire.



Comment protéger ses enfants ?

Internet, c'est génial : applications ludiques, séries éducatives, ... De quoi ravir petits et grands ! Mais accéder sans contraintes à des milliers d'informations et d'images de toutes sortes peut porter à conséquence.

Nos conseils :

Instaurez un contrôle parental : cette méthode vous permettra de bloquer l'accès à certains sites, de définir des horaires d'utilisation et de garder un œil sur les recherches effectuées.

Les outils pour renforcer sa sécurité et celle de ses proches

Si votre mémoire vous fait défaut, optez pour un gestionnaire de mots de passe : lastPass, KeePass, iCloud ou même la fonctionnalité de votre navigateur sont autant de solutions efficaces.

Installez le contrôle parental BLI BLA BLO sur les appareils électroniques de vos enfants.

En savoir plus

Utilisez des outils de vérification pour vous assurer que votre email n'ait pas fait l'objet d'une violation de données.

Pour les fraudes par téléphone, contactez l'ombudscom via leur formulaire de demande de conciliation.

vOé

énergies | installations | renouvelable | multimédia

TÉLÉPHONE 058 234 20 00
ADRESSE Rue de la Poste 2, 1350 Orbe
Rue des Eterpaz 26, 1337 Vallorbe
E-MAIL info@voe.ch
SITE voe.ch

bli bla blo
Le multimédia d'ici.

NOUS SUIVRE