Check-list
Prévenir l'usurpation d'identité

GENERALI

Voici comment vous protéger des attaques

Il n'existe pas de protection absolue contre l'usurpation d'identité (vol/abus). Les experts le répètent constamment. Mais : Avec quelques précautions de sécurité vous compliquez la tâche des usurpateurs.

1. Les mots de passe devraient dépasser huit caractères et contenir, en plus des lettres, également des chiffres et des caractères spéciaux.
2. Attribuez des mots de passe et noms d'utilisateur différents selon les plateformes et renouvelez-les régulièrement. Vous empêchez ainsi qu'en associant vos profils un profil complet révélateur puisse être créé.
3. L'authentification à double facteur offre une sécurité supplémentaire. Celui qui veut se connecter sur l'ordinateur a alors besoin d'un code envoyé simultanément sur le smartphone.
4. Ayez toujours la dernière version de vos navigateurs Internet, systèmes d'exploitation et logiciels antivirus et téléchargez les mises à jour dès qu'elles apparaissent.
5. Lorsque vous naviguez sur des réseaux sans fil publics ou utilisez des appareils qui ne sont pas les vôtres, vous devriez toujours ouvrir des sites Internet tels que Facebook via un lien HTTPS.
6. Dans votre système d'e-mails, activez l'option «connexion sécurisée» (cryptage SSL).
7. Lorsque vous utilisez des services sur des réseaux publics, déconnectez-vous de ces services après utilisation.
8. Renoncez à utiliser vos comptes bancaires en ligne ainsi que d'autres comptes sensibles lorsque vous êtes sur un réseau public.
9. Jetez un œil à l'impressum ou aux conditions générales d'un site Internet pour vous assurer qu'il s'agit d'un prestataire sérieux.
10. Ne divulguez jamais plus d'informations que nécessaire (renoncez aux informations optionnelles).
11. Faites une recherche de votre nom sur Google. En mettant en place une alerte Google, vous pouvez contrôler quand et où votre nom est mentionné sur le net. La recherche occasionnelle de photos est également utile.
12. Ne réagissez pas aux e-mails dont vous ne connaissez pas l'expéditeur et n'ouvrez en aucun cas les annexes.
13. Soyez prudent lorsque vous partagez des données et informations personnelles sur les réseaux sociaux.
14. Choisissez des réponses aux questions de sécurité que vous êtes le seul à connaître.