INTERNET en toute SÉCURITÉ

Quelques règles de base sur internet

1

MOTS DE PASSE : FAITES PREUVE D'IMAGINATION…

Aimez-les complexes, uniques, secrets et régulièrement renouvelés !

2

MISES A JOUR : ~~JE LE FERAI DEMAIN !~~

La mise à jour des logiciels et applications corrige les vulnérabilités appréciées des attaquants. N'attendez plus !

3

SAUVEGARDES : L'ATOUT SÉRÉNITÉ.

Pour préserver vos données, effectuez des sauvegardes régulières sur un support externe déconnecté.

4

WI-FI, CLÉ USB, ETC. : N'OUVREZ PAS LA PORTE A N'IMPORTE QUI !

Les services ou équipements qui vous sont offerts peuvent avoir été configurés à des fins malveillantes. Par prévoyance, évitez-les ou demandez l'avis d'un spécialiste.

5

ORDINATEUR, TÉLÉPHONE, TABLETTE : MÊME COMBAT !

Vos appareils mobiles aussi sont vulnérables ! Qu'attendez-vous pour les protéger ? Installez un logiciel anti-virus anti-espion (VPN) et un pare-feu régulièrement mis à jour.

6

MESSAGERIE : MÉFIEZ-VOUS DES APPARENCES…

Les courriels, les pièces jointes ou les liens qu'ils contiennent réservent parfois de mauvaises surprises… Les incohérences de fond ou de forme et les requêtes indiscrètes sont à prendre avec des pincettes !

7

TÉLÉCHARGEMENT : GARE AUX ARNAQUES !

Restez prudents lorsque vous téléchargez programmes et logiciels, préférez les sites officiels.

8

PAIEMENT EN LIGNE : ÉVITEZ LES FRAIS.

Soyez vigilants lors de vos achats sur Internet. Gardez en tête quelques bons réflexes : vérifiez que figure la mention « https:// » dans la barre d'adresse du site consulté et dans certain cas, un cadenas.

9

SÉPARATION DES USAGES : UN JEU D'ENFANT ?

Pour limiter l'effet boule de neige d'une action malveillante, séparez vos usages professionnels et personnels (messagerie, équipements…).

10

IDENTITÉ NUMÉRIQUE/ ATTENTION, DOSSIER !

Une fois sur Internet, vos données vous échappent et font le bonheur des adeptes de l'ingénierie sociale » (usurpation d'identité, espionnage…). Faites-vous discret…

⚠ Les principaux dangers sur internet ⚠

	L'HAMEÇONNAGE	LES RANÇONGICIELS	L'ARNAQUE AU FAUX SUPPORT TECHNIQUE
CYBERCRIMINEL 	 ***VOL DE DONNÉES*** Vous recevez un message ou un appel inattendu, voire alarmant, d'une organisation connue et d'apparence officielle qui vous demande des informations personnelles ou bancaires ? Vous êtes peut-être victime d'une attaque par hameçonnage (phishing en anglais) ! ***BUT*** Voler des informations personnelles ou professionnelles (identité, adresses, comptes, mots de passe, données bancaires...) pour en faire un usage frauduleux. ***TECHNIQUE*** Leurre envoyé via un faux message, SMS ou appel téléphonique d'administrations, de banques, d'opérateurs, de réseaux sociaux, de sites d'e-commerce...	 ***EXTORSION D'ARGENT*** Vous ne pouvez plus accéder à vos fichiers et on vous demande une rançon ? Vous êtes victime d'une attaque par rançongiciel (ransomware, en anglais) ! ***BUT*** Réclamer le paie-ment d'une rançon pour rendre l'accès aux fichiers verrouillés. ***TECHNIQUE*** Blocage de l'accès à des données par envoi d'un message contenant des liens ou pièces jointes malveillantes ou par intrusion sur le système.	 ***ESCROQUERIE FINANCIÈRE*** Votre ordinateur est bloqué et on vous demande de rappeler un support technique ? Vous êtes victime d'une arnaque au faux support ! ***BUT*** Inciter la victime à payer un pseudo-dépannage informatique et/ou la faire souscrire à des abonnements payants ***TECHNIQUE*** Faire croire à un problème technique grave impliquant un risque de perte de don-nées ou d'usage de l'équipe-ment (par écran bloqué, téléphone, SMS, courriel etc.).
COMMENT RÉAGIR ?			
VICTIME 	• Ne communiquez jamais d'information sensible suite à un message ou un appel téléphonique • Au moindre doute, contactez directement l'organisme concerné pour confirmer • Faites opposition immédiatement (en cas d'arnaque bancaire) • Changez vos mots de passe divulgués/compromis • Déposez plainte • Signalez-le sur les sites spécialisés	• Débranchez la machine d'Internet et du réseau local • En entreprise, alertez le support informatique • Ne payez pas la rançon • Déposez plainte • Identifiez et corrigez l'origine de l'infection • Essayez de désinfecter le système et de déchiffrer les fichiers • Réinstallez le système et restaurez les données • Faites-vous assister par des professionnels	• Ne répondez pas • Conservez toutes les preuves • Redémarrez votre appareil • Purgez le cache, supprimez les cookies et réinitialisez les paramètres de votre navigateur • Désinstallez tout nouveau programme suspect • Faites une analyse antivirus • Changez tous vos mots de passe • Faites opposition auprès de votre banque si vous avez payé • Déposez plainte

Pour aller plus loin ou obtenir de l'information :

- ► www.cybermalveillance.gouv.fr Assistance et prévention du risque numérique
- ► www.internet-signalement.gouv.fr Portail officiel de signalement des contenus illicites de l'Internet
- ► www.ssi.gouv.fr Agence nationale de la sécurité des systèmes d'information

Gendarmerie nationale
Une force humaine