

## CAMBRIOLAGÈS

### Comment se protéger ?

#### Quelques conseils simples :

- ne pas laisser entrer les inconnus et démarcheurs non annoncés, demander une carte professionnelle aux agents se réclamant d'une agence (EDF, GDF, télécom...);
- en cas de cambriolage, ne toucher à rien et prévenir aussitôt la gendarmerie en composant le 17.



#### Portes et fenêtres...

- fermer portes et fenêtres, même pour une courte période ;
  - > ne pas hésiter à renforcer les ouvrants les plus accessibles et les accès annexes (cave, garage...);
  - > équiper les baies vitrées (très vulnérables aux intrusions) de verrous simples ou à clés.



#### Clés...

- ne pas laisser les clés sous un paillasson, dans la boîte à lettres, dans un pot de fleurs...
  - > remettre ses clés à une personne de confiance ;
  - > ne ranger pas vos clés de voiture à des endroits évidents des voleurs (porte-clés derrière la porte ou dans l'entrée) pour éviter les « home-jacking ».

#### En cas d'absence...

- ne pas laisser la porte du garage ouverte sans voiture ;
- ne pas laisser le courrier s'accumuler (le faire relever ou conserver à la poste) ;
  - > éviter que le domicile soit plongé dans le noir dès le crépuscule (programmateurs d'éclairage ou d'appareils électriques) ;
  - > demander à un voisin ou une personne de confiance de porter une attention vigilante à votre domicile (absence de plusieurs jours).

#### Les abords de la maison...

##### - Faire

- entretenir la végétation de façon à ce que l'habitation et notamment les accès restent visibles depuis la rue ;

équiper les abords de l'habitation d'un éclairage s'activant à la détection de mouvement.

##### - Ne pas faire

- ne pas laisser d'outils à l'extérieur qui pourraient aider les malfaiteurs à entrer (tournevis, échelle, outils de jardinage...);
- > éviter de signaler les absences sur les réseaux sociaux ou répondeurs téléphoniques.



### Vos biens...

- ne pas les « cacher » dans des endroits ciblés par les cambrioleurs (chambre, salle de bain, lingerie);

> placer vos biens les plus précieux dans un coffre scellé au sol ou dans un mur.

### Pour aller plus loin, vous pouvez :



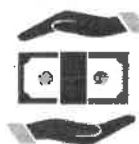
#### vous protéger :

- équiper votre habitation d'une alarme afin de détecter au plus tôt une intrusion et alerter;
- en cas d'absence prolongée, dans le cadre de l'opération tranquillité vacances, signaler vos absences à la gendarmerie;

> installer une clôture efficace sur le périmètre de votre habitation :

un modèle en treillis soudé de 2 m de hauteur permet de limiter les intrusions, haies végétales défensives (Berberis, cognassier du japon, rosier rugueux, pyracantha... qui s'intègrent parfaitement à tout type d'environnement et protègent les accès à votre propriété – attention toutefois aux jeunes enfants en raison de la présence d'épines proéminentes);

> solliciter des conseils (gratuits et sans engagement) auprès du référent-sûreté de la gendarmerie pour mieux protéger votre habitation : adressez-vous à votre brigade de gendarmerie.



#### Anticiper et limiter les désagréments d'un cambriolage :

- lister vos objets, notamment multimédia (n° de série), à conserver en lieu sûr ([www.liste-objets-voles.fr](http://www.liste-objets-voles.fr));
- photographier les objets de valeurs (bijoux...);

> marquer vos objets les plus précieux : il existe dans le commerce des kits de marquage (dit ADN synthétique, chimique ou forensique) permettant d'identifier de manière unique les objets marqués et de pouvoir les rendre à leur propriétaire en cas de vol.

### Contribuer à la sécurité de votre quartier :



- signaler les véhicules ou individus pouvant faire du repérage au « 17 » en donnant les éléments d'identification (marque, type, couleur, immatriculation, tenue vestimentaire...).

Votre brigade de gendarmerie est joignable aux coordonnées suivantes :

Brigade d'Eygurande  
07 rue Saint Loup 19340 EYGURANDE  
Tel : 05.55.94.30.05

**GENDARMERIE D'EYGURANDE**  
7 Rue Saint-Loup  
19340 - EYGURANDE  
Tél. : 05 55 94 30 05



# 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 indiscrettes 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...*

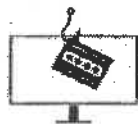


# ! Les principaux dangers sur internet !

## CYBERCRIMINEL



### L'HAMEÇONNAGE



#### **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...

### LES RANÇONGIERS



#### **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 paiement 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.

### L'ARNAQUE AU FAUX SUPPORT TECHNIQUE



#### **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 données ou d'usage de l'équipement (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](http://www.cybermalveillance.gouv.fr) Assistance et prévention du risque numérique
- ▶ [www.internet-signalement.gouv.fr](http://www.internet-signalement.gouv.fr) Portail officiel de signalement des contenus illicites de l'Internet
- ▶ [www.ssi.gouv.fr](http://www.ssi.gouv.fr) Agence nationale de la sécurité des systèmes d'information