

## Sécurité sur tous les plans avec la Bienfaisance !



Sécurité sur tous les plans avec la Bienfaisance !

Après la sécurité routière en octobre dernier, la Bienfaisance avait choisi d'aborder le problème de la sécurité.

En ce samedi 8 avril, Christiane Georgen, présidente de la Bienfaisance, recevait les représentants des deux institutions qui oeuvrent quotidiennement à la protection des personnes, des biens et de l'environnement, la gendarmerie représentée par le commandant de la communauté de la brigade de Vic-Fezensac et les pompiers représentés par le chef de centre Pierre Pontier.



Devant un public nombreux et attentif, le commandant de gendarmerie a ouvert la séance par un **exposé didactique sur les principales cybermenaces**, des menaces répertoriées en 8 catégories au nom parfois un peu barbare comme l'hameçonnage ou le rançongiciel.

Outre l'hameçonnage ou le rançongiciel, ont été évoqués le faux assistant, le chantage webcam, la fraude à la carte bancaire, le faux investissement, l'escroquerie sentimentale et les fausses annonces.

Par le biais de vidéos et avec des exemples concrets, ces techniques d'arnaque sur internet sont devenues tout de suite beaucoup plus claires et dans l'assistance, plusieurs personnes ont témoigné avoir été victimes de l'une ou l'autre.

Après avoir explicité chacune des menaces, le commandant a proposé des solutions pour détourner ces pièges.

**L'hameçonnage ou phishing** est un SMS ou mail frauduleux destinés à tromper la victime pour l'inciter à communiquer des données personnelles et/ou bancaires en se faisant passer pour un tiers de confiance.

Pour détecter un mail frauduleux, il faut bien observer l'adresse très souvent fantaisiste et surtout ne pas cliquer sur les liens ou pièces jointes contenus dans le mail

**L'arnaque au faux assistant** consiste à vous effrayer en vous indiquant un problème technique grave afin de vous pousser à payer un pseudo-dépannage informatique.

Dans ce cas, il ne faut surtout pas appeler le numéro indiqué et simplement éteindre et redémarrer l'appareil.

Une victime dans la salle a expliqué être tombée dans le piège et avoir été débitée à deux reprises pour un pseudo dépannage. Comme elle avait elle-même donné l'autorisation à la banque pour le prélèvement, elle n'a pu être remboursée.

En cas de **fraude à la carte bancaire** très courante, il faut surveiller régulièrement ses comptes, faire opposition si l'on constate des prélèvements inhabituels et signaler la fraude sur le site [Perceval](https://www.perceval.fr).

Quant aux **fausses annonces**, il faut se méfier de tout ce qui est trop beau pour être vrai !

Plus d'informations ici : <https://www.cybermalveillance.gouv.fr/cybermenaces>



**Après avoir passé en revue les différentes menaces, le commandant a proposé une liste de « bonnes pratiques » pour éviter d'être victimes de ces pièges.**

Il faut protéger vos accès avec des mots de passe solides, sauvegarder vos données régulièrement, utiliser un antivirus, télécharger vos applications uniquement sur les sites officiels, vérifier les sites sur lesquels vous faites des achats, éviter les réseaux WiFi publics ou inconnus...

Plus d'informations ici : <https://www.cybermalveillance.gouv.fr/bonnes-pratiques>

Dans un deuxième temps, a été abordé **le thème des cambriolages**.

Il a été question de l'opération « tranquillité vacances » : pendant toute absence prolongée de votre domicile, vous pouvez vous inscrire à l'opération tranquillité vacances. Les services de police ou de gendarmerie se chargent alors de surveiller votre logement. Des patrouilles sont organisées pour passer aux abords de votre domicile. Vous serez prévenu en cas d'anomalies (dégradations, cambriolage ...).

Ont été également évoqués **les démarchages à domicile** et les moyens de distinguer le vrai du faux.

En effet, les "faux" démarcheurs utilisent le prétexte du porte-à-porte pour s'introduire chez vous afin d'effectuer un repérage en vue d'un cambriolage ou de voler de petits objets de valeur. Ils agissent en général par deux.

Les "vrais" démarcheurs sont des travailleurs indépendants ou rattachés à une entreprise (des VRP : voyageur représentant et placier), qui doivent pouvoir justifier de leur identité et de leur profession. Le contrat signé doit aussi respecter plusieurs conditions (délai de rétractation, devis, conditions de paiement) pour être considéré comme valide.

Mais les représentants de la gendarmerie se sont montrés rassurants : notre secteur est en effet relativement préservé des cambriolages.

En 2022, on n'en relève que 17 pour 29 communes.

Les représentants de la gendarmerie ont ensuite laissé la place **aux pompiers qui ont abordé plusieurs situations à risque : l'incendie, l'intoxication domestique, les chutes et les gestes qui sauvent**.

Béregère Labit a procédé à des démonstrations pour illustrer les propos de Pierre Pontier.



Gestes à adopter en cas d'étouffement



Pose d'un garrot pour lutter contre l'hémorragie sanguine



Mise en PLS d'une victime inconsciente



Massage cardiaque



#### Utilisation du défibrillateur

En matière de gestes qui sauvent, Pierre Pontier a insisté sur **la nécessité de créer le premier maillon de la chaîne des secours** ; toute minute qui passe accroît le risque de ne pas ramener des gens à la vie.

En cas d'accident (ou arrêt) cardiaque, il recommande aux proches, à la famille de procéder tout de suite au massage cardiaque.

Ces 1eres minutes de massage sont primordiales et déterminantes dans le sauvetage d'une vie avant que les pompiers ne prennent le relai. Les pompiers apprécient énormément que cet exercice soit entamé à leur arrivée, cela les aide et les encourage.

Il faut tenir compte de notre zone rurale où parfois les déplacement des pompiers prennent un peu de temps et les minutes comptent !

Il a donc été question de l'alerte, qui on alerte, comment on alerte, par quels moyens et pour cela il existe **l'application Staying Alive** – dont le SDIS est partenaire- téléchargeable sur son téléphone.

**L'application mobile Staying Alive** cartographie les défibrillateurs cardiaques recensés en France et propose des tutoriels sur le comportement et les gestes de premiers secours à adopter en cas d'arrêt cardiaque. Par ailleurs, elle permet de s'inscrire en tant que **Bon Samaritain**.

Ces citoyens sauveteurs et volontaires gardent la géolocalisation de leur smartphone activée, et peuvent être sollicités pour intervenir sur un arrêt cardiaque à proximité en attendant l'arrivée des secours, que ce soit en allant chercher un défibrillateur ou en commençant à prodiguer un massage cardiaque s'ils sont formés aux gestes qui sauvent.

Les pouvoirs publics ont mis à disposition dans toutes les villes dans les bâtiments publics des défibrillateurs automatiques, 8 sur Vic ( face à l'église, à la mairie, aux arènes, au gymnase, au stade de foot, au stade de rugby, à la salle polyvalente, à l'école maternelle, à Lagraulais)

On a beau avoir le matériel et la compétence, il faut connecter les deux grâce à un outil d'alerte semblable au bip des pompiers, c'est cette application gratuite téléchargeable sur smartphone, a expliqué Pierre Pontier.

Plus d'infos : <https://www.stayingalive.org/index?lang=fr>



L'après-midi s'est achevé autour du verre de l'amitié qui permis aux participants de continuer à échanger sur des sujets qui nous concernent tous.

**Bravo à la Bienfaisance pour cette initiative à renouveler !**

Merci à Caroline Cueillens pour les photos des pompiers