GOUVERNEMENT

Liberté
Égalité
Fraternité

FFRandonnée

PRÉVENTION CONTRE LES ARNAQUES

A LA FÉDÉRATION FRANÇAISE DE LA RANDONNÉE PÉDESTRE, NOUS SOMMES TOUS CONCERNÉS PAR LA CYBERSÉCURITÉ

Systèmes d'Information et Transformation Digitale

Attention arnaques !

Le gouvernement lance un appel à la vigilance

La vulnérabilité des consommateurs et des entreprises face à des manoeuvres frauduleuses s'est accrue avec la crise sanitaire. La Fédération française de la Randonnée pédestre est aussi victime d'attaques venant d'internet. **Il est essentiel de maintenir une vigilance permanente en rappelant les attitudes réflexes qu'il convient d'adopter pour déjouer de potentielles arnaques.**

À cette fin, les services de l'État et les autorités de contrôle s'associent et proposent des fiches préventives d'identification des principales fraudes.
https://www.economie.gouv.fr/files/files/2022/Guide-TF-actualise-1907.pdf

L'équipe informatique de la Fédération française de la Randonnée pédestre vous accompagne avec une synthèse du guide du gouvernement de prévention contre les arnaques.

Systèmes d'Information
et Transformation Digitale

Vulnérabilité des consommateurs

- Arnaque aux achats en ligne
- Vol de coordonnées bancaires
- Arnaque au Compte Personnel de Formation (CPF)

Systèmes d'Information et Transformation Digitale

Vulnérabilité des consommateurs : Arnaque aux achats en ligne

Vérifier l'identité du vendeur

Avant toute commande, il est recommandé de contrôler que le site internet sur lequel vous naviguez n'est pas seulement une façade mais qu'il y a bien une entreprise réelle derrière celui-ci.

Choisir un site français ou européen

Il est préférable de choisir un site français ou européen. Les autres n'ont pas toujours une bonne connaissance de la réglementation applicable, présentent des prix qui n'incluent pas toujours les droits de douane et de TVA.

Vérifier la e-réputation

Si vous ne connaissez pas le site sur lequel vous naviguez, il est important de vérifier sa e-réputation. Par exemple, en **entrant le nom du site ou du produit sur un moteur de recherche**, éventuellement associé avec le terme « arnaque ».

Systèmes d'Information et Transformation Digitale

Messages de prévention

1 Vigilance

Soyez vigilants face à des annonces proposées sur les réseaux sociaux et que vous n'avez pas spécialement sollicitées.

2 Prenez le temps...

Prenez le temps de comparer ; si les mêmes produits sont vendus sur d'autres sites plus chers, méfiez-vous du site qui vous le propose à un prix trop faible.

3 Identité du vendeur

Vérifiez l'identité et les coordonnées du vendeur ; elles doivent toujours être présentes sur le site.

Vulnérabilité des consommateurs : Vol de coordonnées bancaires

Constater le vol

En consultant votre compte bancaire, vous découvrez des opérations réalisées à votre insu avec les références de votre carte bancaire que vous avez toujours en votre possession.

Je suis victime, que faire ?

Réagissez le plus vite possible !
Informations, conseils, assistance par du personnel de la police nationale et la gendarmerie nationale, **contacter INFO ESCROQUERIES au 0811 02 02 17** (prix d'un appel local depuis un poste fixe, ajouter 0,06€/minute depuis un téléphone mobile), du lundi au vendredi de 9h à 18h.

Systèmes d'Information et Transformation Digitale

Messages de prévention

1 Dans un magasin ou au restaurant

Ne jamais quitter sa carte bancaire des yeux.
Ne jamais confier sa carte bancaire à un inconnu.
Apprendre plutôt son code secret par coeur.

2 Sur internet

Réaliser les achats uniquement sur des sites de confiance dont l'adresse commence par « https » au moment de la transaction.
Ne pas enregistrer son numéro de carte bancaire sur le site commerçant, ni sur l'ordinateur.
Éviter le piratage de sa carte bancaire en protégeant son ordinateur avec un antivirus et un parefeu.
Favoriser les paiements avec un numéro de carte bancaire unique.

3 Au distributeur de billets :

Toujours cacher avec sa main le pavé numérique.
Ne pas se laisser distraire par des inconnus qui vous proposent leur aide ou qui vous demandent un renseignement.

.

Vulnérabilité des consommateurs : Démarchage relatif au compte CPF

Comment détecter une arnaque au CPF ?

Le mode opératoire des fraudeurs est toujours sensiblement le même : dans le cadre d'un démarchage, ils invitent de manière insistante, par email mais surtout par SMS, à transmettre des données personnelles.

Les crédits CPF n'expirent jamais !

Les fraudeurs prétendent généralement que les crédits de formation sont sur le point d'expirer et qu'il faut donc les mobiliser au plus vite. Certains messages comme « avant qu'il ne soit trop tard » ou « vous allez perdre vos droits au CPF » sont mensongers et doivent alerter.

Perte des droits du compte CPF

Les fraudeurs incitent la victime à s'inscrire à des formations factices auprès de sociétés « coquilles vides » dont le financement sera réglé par le CPF, **engendrant de facto une perte de droits du compte personnel** de la victime.

Systèmes d'Information et Transformation Digitale

Messages de prévention

1 Rester attentif

- Ne jamais répondre à un démarchage téléphonique.
- Ne rappeler aucun numéro.
- Ne jamais communiquer les identifiants et mot de passe de son compte personnel de formation.
- Ne jamais donner son numéro de sécurité sociale.
- Ne jamais cliquer directement sur un lien reçu par mail ou SMS.
- Ne pas répondre à des formulaires d'inscription en ligne.

2 Le site officiel du CPF

Utiliser uniquement le seul site officiel **www.Mon-CompteFormation.gouv.fr**

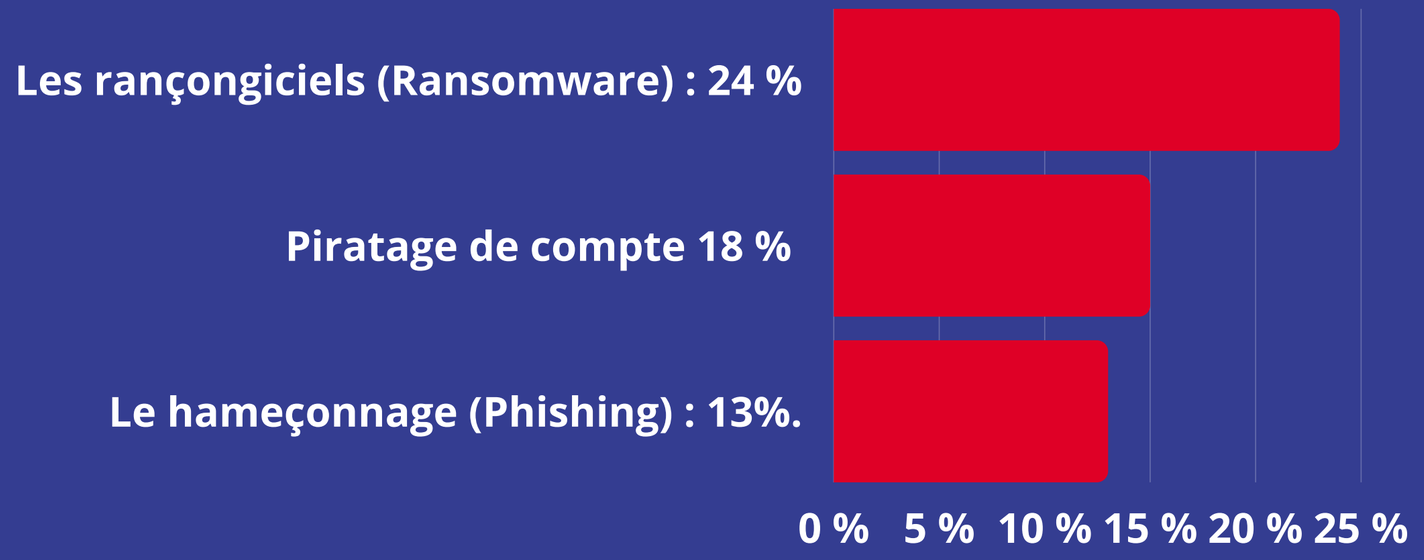
Vulnérabilité des entreprises et associations

55 % des demandes d'assistance à l'agence de cyber malvaillance de l'état sont regroupées sur 3 sujets.

Voyons comment nous prémunir de ces menaces qui peuvent provoquer des arrêts de production de plusieurs jours.

Systèmes d'Information et Transformation Digitale

Cybersécurité



Source : https://www.cybermalveillance.gouv.fr

RANÇONGICIELS (RANSOMWARES)

Logiciels malveillants qui bloquent l'accès aux fichiers et qui réclament à la victime le paiement d’une rançon pour en obtenir de nouveau l’accès.

Comment protéger ses données ?

Vigilance

N’ouvrez **jamais** les courriels ou les pièces jointes d’expéditeurs inconnus ou d’un expéditeur connu, mais dont la structure du message est inhabituelle ou qui comporte des fautes d'orthographes

.

Ne cliquez **jamais** sur les liens provenant de chaînes de messages, ou vide.

Mises à jour

Appliquez de manière régulière et systématique les mises à jour de sécurité du système et des logiciels installés sur votre machine.
Tenez à jour l’antivirus.

Mot de passe

Utilisez des mots de passe suffisamment complexes et changez-les régulièrement.

Rançongiciels = arrêt de production de plusieurs jours !!

Si vous cliquez sur un lien qui va lancer le Rançongiciel et encrypter les fichiers de votre ordinateur ou du serveur de l'entreprise, **le temps de retour à la normale peut être de plusieurs jours**. Le temps que le service informatique restaure les fichiers qui ne sont pas encryptés depuis les sauvegardes. De plus, les restaurations seront forcément des fichiers anciens, donc **toute la production de la journée sera perdue** !

Systèmes d’Information et Transformation Digitale

Piratage de compte

Le piratage de compte désigne la prise de contrôle voire l'utilisation frauduleuse d'un compte au détriment de son propriétaire légitime. Le pirate va usurper le compte et trouver votre mot de passe.

Comment éviter de se faire pirater un compte ?

Mot de passe

Utilisez **des mots de passe différents et complexes** pour chaque site et application utilisés pour éviter que, si un compte est piraté, les cybercriminels puissent accéder aux autres comptes utilisant ce même mot de passe.

Données sensibles

Ne communiquez jamais d'informations sensibles (mots de passe) par messagerie, par téléphone ou sur Internet.

Sécurité

Lorsque le site ou le service le permettent, activez la double authentification pour augmenter le niveau de sécurité.

La double authentification, appelée aussi validation en 2 étapes, est un procédé qui permet de renforcer la sécurité de ses comptes en agissant comme une protection supplémentaire en cas de vol de votre mot de passe.

Systèmes d'Information et Transformation Digitale

Hameçonnage / Phishing

Le hameçonnage ou phishing est le principal mode opératoire utilisé par les cybercriminels pour dérober des informations personnelles et/ou bancaires. Par message électronique (e-mail), SMS ou encore par téléphone, il consiste à usurper l'identité d'un tiers de confiance (banque, administration, réseau social, entreprise de livraison, commerce en ligne...) pour tromper la victime et l'inciter à communiquer ses données d'identité, ses mots de passe ou ses numéros de carte bancaire

Comment éviter le phishing ?

Vigilance

Méfiez-vous des demandes étranges : posez-vous la question de la légitimité des demandes éventuelles exprimées. **Aucun organisme n'a le droit de vous demander votre code carte bleue, vos codes d'accès et mots de passe.** Ne transmettez rien de confidentiel même sur demande d'une personne qui annonce faire partie de votre entourage.

Restez attentif !

Ne faites pas confiance aux noms de domaine dont l'adresse peut être fausse, c'est très simple à vérifier, **il suffit de regarder !**

Par exemple :

- www.impots.gouvv.fr au lieu de www.impots.gouv.fr
- www.impots.gouvfr.biz au lieu de www.impots.gouv.fr
- www.infocaf.org au lieu de www.caf.fr

L'origine du message

L'adresse de messagerie source n'est pas un critère fiable : **une adresse de messagerie provenant d'un ami, de votre entreprise, d'un collaborateur peut facilement être usurpée**. Si vous avez un doute, contactez la personne pour vérifier l'origine du message.

Systèmes d'Information et Transformation Digitale

Les 3 axes de la cybersécurité

Prévention

Rester informé (e) des recommandations mises à votre disposition pour prévenir des dangers d'internet. En lisant ce document et en appliquant ces quelques règles vous avez déjà accompli la première étape.

Sécurité

Avoir un ordinateur avec des mises à jour régulières et les appliquer lorsque le système vous les proposent.
Avoir un antivirus à jour.

Vigilance

C'est la partie la plus importante : votre vigilance et vos actions !
Vous êtes le premier acteur de la sécurité de votre infrastructure.
Réfléchissez toujours avant d'agir et sans précipitation.

Systèmes d'Information et Transformation Digitale

Se protéger de la cybersécurité est finalement assez simple ...

Nous avons vu qu'il y a quelques règles simples à appliquer :
- ne jamais communiquer d'informations sensibles, à personne !
- rester attentif et concentré (e), ne jamais agir dans la précipitation et regarder avant d'agir va permettre d'éviter les soucis et autres pertes de données.
- avoir toujours sa machine à jour !

Tous concernés

A la Fédération Française de la Randonnée Pédestre, nous sommes tous concernés par la cybersécurité.

Systèmes d'Information et Transformation Digitale

FFRandonnée

Présentation des administrations impliquées dans le document source

- Le Ministère de l'Intérieur :
• la direction générale de la police nationale (DGPN)
• la direction centrale de la police judiciaire (DCPJ)
• la direction générale de la gendarmerie nationale (DGGN)
• le pôle judiciaire de la gendarmerie nationale (PJGN)

- Le Ministère de l'Économie et des Finances :
• la direction générale de la concurrence, de la consommation et de la répression des fraudes (DGCCRF), chargée de la protection des consommateurs

- Le Ministère de l'action et des comptes publics :
• la direction générale des finances publiques (DGFIP)
• la direction générale des douanes et des droits indirects (DGDDI)

- Le Ministère de la Justice :
• la direction des affaires criminelles et des grâces (DACG)

- Le Ministère de l'Agriculture :
• la direction générale de l'alimentation (DGAL)

- L'Autorité des marchés financiers (AMF), l'Autorité de contrôle prudentiel et de résolution (ACPR), et la Banque de France, les autorités de contrôle du secteur financier

- La Commission Nationale de l'Informatique et des Libertés (CNIL) :
• pour les atteintes aux données personnelles

- L'Agence Nationale de la Sécurité des Systèmes d'Information (ANSSI)

Source https://www.economie.gouv.fr/fraudes-escroqueries-guide-prevention-grand-public-entreprises
https://www.cybermalveillance.gouv.fr/