Black Friday :
7 conseils pour éviter les cyber-arnaques

Lors des périodes promotionnelles, les cybercriminels multiplient les cyber-arnaques, profitant des nombreuses offres sur Internet pour tenter d'escroquer les consommateurs. Face à ce phénomène récurrent, Cybermalveillance.gouv.fr appelle ainsi à la plus grande vigilance et délivre 7 conseils pour éviter de se faire escroquer.

Fausses annonces promotionnelles, faux sites Internet marchands officiels, faux sites de commerce en ligne créés pour la circonstance, hameçonnage (*phishing*) par SMS, téléphone ou courriel (*email*), faux transporteur, faux support technique, fausses confirmations de commande, faux service après vente, attaques par rançongiciels (*ransomware* en anglais)… Toutes les techniques frauduleuses sont utilisées par les criminels pour essayer d'abuser leurs victimes afin de leur faire réaliser un achat qu'ils ne verront jamais arriver, les faire rappeler des numéros surtaxés, leur voler leurs données personnelles ou bancaires ou encore les rançonner.

1. Cyber-arnaques ? Méfiez-vous des offres trop généreuses

Si la promotion vous semble beaucoup plus intéressante que partout ailleurs, alors considérez la suspecte par principe et faites un minimum de vérification avant d'acheter (réalité de la promotion, notoriété du vendeur, risque de contrefaçon…) au risque de ne jamais voir arriver votre achat ou au mieux de vous faire livrer une contrefaçon.

2. Ne confondez pas vitesse et précipitation

Même pressé par un pseudo vendeur en ligne qui vous propose l'affaire du siècle ou par un compte à rebours de vente flash, ne donnez pas trop rapidement votre numéro de carte bancaire et prenez le temps d'un minimum de vérifications : existence réelle et notoriété du vendeur, réalité de la promotion, sécurité de la transaction…

3. Ne rappelez pas inconsidérément des numéros surtaxés

Si des messages énigmatiques reçus sur votre boîte vocale ou par SMS vous demandent de recontacter un pseudo transporteur « *pour votre livraison* » ou un service après-vente (SAV) « *suite à votre achat* » ou encore vous proposent une promotion « *immanquable »,* préférez rappeler le numéro officiel du commerçant, du transporteur ou du SAV concerné que vous trouverez sur son site officiel.

4. Cyber-arnaques : Attention à l'hameçonnage

Vérifiez scrupuleusement les adresses d'envoi dans les messages (un seul caractère peut parfois changer), ne cliquez pas sur les liens et n'ouvrez pas les pièces jointes d'expéditeurs inconnus ou douteux qui vous annoncent l'affaire du siècle : vous pourriez le regretter amèrement par le vol de vos codes d'accès, de vos données personnelles ou bancaires, la réception d'un virus, l'achat d'une contrefaçon…

Vérifiez la réalité de la promotion sur le site officiel du commerçant ou en contactant par téléphone son service commercial.

L'hameçonnage (phishing)

Apprenez à repérer et vous prémunir de l'hameçonnage grâce à notre fiche réflexe consacrée au sujet.

Publié le 08/04/2021PDF 123 KoTélécharger

5. Vérifiez la réalité et la notoriété des sites sur lesquels vous allez faire vos achats

Assurez-vous que vous n'êtes pas sur une copie frauduleuse d'un site officiel (*) ou sur un site créé pour la circonstance qui propose des affaires comme on n'en voit nulle part ailleurs, mais qui n'a en réalité que pour seul objet de vous escroquer.

(*) Vérifiez scrupuleusement l'adresse du site, un seul caractère peut parfois changer par rapport au nom du site officiel. Face à un site inconnu, rechercher son nom sur un moteur de recherche et consulter les avis vous évitera de nombreuses déconvenues.

6. Cyber-arnaques : Protégez vos données personnelles et bancaires

Quitte à rater une très bonne affaire, au moindre doute, ne fournissez pas trop vite vos données personnelles ou bancaires au risque de conséquences qui pourraient être dramatiques : usurpation d'identité, transactions bancaires frauduleuses…

7. Utilisez un mot de passe solide et différent pour chaque application ou site Internet

C'est le seul moyen de vous assurer que si votre mot de passe est compromis sur un site, cela ne compromettra pas l'ensemble de vos autres accès informatiques.

RÉPUBLIQUE FRANÇAISE
Liberté
Égalité
Fraternité

CYBER MALVEILLANCE GOUV.FR
Assistance et prévention en sécurité numérique

LES MOTS DE PASSE

ADOPTER LES BONNES PRATIQUES

Messageries, réseaux sociaux, banques, administrations et commerces en ligne, réseaux et applications d'entreprise… la sécurité de l'accès à tous ces services du quotidien repose aujourd'hui essentiellement sur les mots de passe. Face à la profusion des mots de passe, la tentation est forte d'en avoir une gestion trop simple. Une telle pratique serait dangereuse, car elle augmenterait considérablement les risques de compromettre la sécurité de vos accès. **Voici 10 bonnes pratiques à adopter pour gérer efficacement vos mots de passe.**

1 UTILISEZ UN MOT DE PASSE DIFFÉRENT POUR CHAQUE SERVICE

Ainsi en cas de perte ou de vol d'un de vos mots de passe, seul le service concerné sera vulnérable. Dans le cas contraire, tous les services pour lesquels vous utilisez le même mot de passe compromis seraient piratables.

2 UTILISEZ UN MOT DE PASSE SUFFISAMMENT LONG ET COMPLEXE

Une technique d'attaque répandue, dite par « force brute », consiste à essayer toutes les combinaisons possibles de caractères jusqu'à trouver le bon mot de passe. Réalisées par des ordinateurs, ces attaques peuvent tester des dizaines de milliers de combinaisons par seconde. Pour empêcher ce type d'attaque, il est admis qu'un bon mot de passe doit comporter au minimum 12 signes mélangeant des majuscules, des minuscules, des chiffres et des caractères spéciaux.

3 UTILISEZ UN MOT DE PASSE IMPOSSIBLE À DEVINER

Une autre technique d'attaque utilisée par les pirates est d'essayer de « deviner » votre mot de passe. Évitez donc d'employer dans vos mots de passe des informations personnelles qui pourraient être faciles à retrouver (sur les réseaux sociaux par exemple), comme le prénom de votre enfant, une date anniversaire ou votre groupe de musique préféré. Évitez également les suites logiques simples comme 123456, azerty, abcdef… qui font parte des listes de mots de passe les plus courants et qui sont les premières combinaisons qu'essaieront les cybercriminels pour tenter de forcer vos comptes.

4 UTILISEZ UN GESTIONNAIRE DE MOTS DE PASSE

Il est humainement impossible de retenir les dizaines de mots de passe longs et complexes que chacun est amené à utiliser quotidiennement. Ne commettez pas pour autant l'erreur de les noter sur un pense-bête que vous laisseriez à proximité de votre équipement, ni de les inscrire dans votre messagerie ou dans un fichier non protégé de votre ordinateur, ou encore dans votre téléphone mobile auquel un cybercriminel pourrait avoir accès. Apprenez à utiliser un gestionnaire de mot de passe sécurisé qui s'en chargera à votre place, pour ne plus avoir à retenir que le seul mot de passe qui permet d'en ouvrir l'accès. *Voir notre encadré sur Keepass au dos de cette fiche.*

5 CHANGEZ VOTRE MOT DE PASSE AU MOINDRE SOUPÇON

Vous avez un doute sur la sécurité d'un de vos comptes ou vous entendez qu'une organisation ou société chez qui vous avez un compte s'est fait pirater. N'attendez pas de savoir si c'est vrai ou pas. Changez immédiatement le mot de passe concerné avant qu'il ne tombe dans de mauvaises mains.

CRÉER UN MOT DE PASSE SOLIDE

LA MÉTHODE DES PREMIÈRES LETTRES
Un tiens vaut mieux que deux tu l'auras
`1tvmQ2t'A`

LA MÉTHODE PHONÉTIQUE
J'ai acheté huit CD pour cent euros cet après-midi
`ght8CD%E7am`

Inventez votre propre méthode connue de vous seul!

MINISTÈRE DE L'INTÉRIEUR
AGENCE NATIONALE DE LA SÉCURITÉ DES SYSTÈMES D'INFORMATION

Les mots de passe

Retrouvez les 10 bonnes pratiques à adopter pour gérer efficacement vos mots de passe.

Publié le 08/04/2021PDF 311 KoTélécharger

Enfin, notez que si l'entreprise auprès de laquelle vous effectuez votre achat est localisée à l'étranger, vous pouvez rencontrer de réelles difficultés en cas de litige commercial car elle peut échapper au droit qui protège les consommateurs français.

Vous pensez avoir été victime d'une cyber-arnaque ? Rendez-vous sur Cybermalveillance.gouv.fr pour être conseillé et orienté vers les services appropriés, ou encore être mis en relation avec des prestataires spécialisés référencés sur la plateforme et susceptibles de pouvoir vous assister si besoin.