Nos conseils pour affronter la recrudescence des « cyber-escroqueries »

Une augmentation de la vigilance s'impose pour faire face aux multiples attaques conduites par les cybercriminels qui, comme chaque année, redoubleront d'efforts durant la période des soldes.

Cette année la période des soldes d'hiver s'étalera du **9 janvier au 19 février** sur l'essentiel du territoire national avec quelques dérogations pour certains départements frontaliers et outre-mer.

Durant ces 4 semaines, les promotions battront leur plein en boutique et sur Internet.

Cet événement sera bien évidemment **l'occasion pour les cybercriminels de redoubler d'efforts** afin de profiter de la précipitation et de la crédulité des internautes imprudents en quête de la « bonne affaire à ne pas rater » en menant des escroqueries de toutes sortes.

Fausses annonces promotionnelles, faux sites de commerce en ligne officiels ou créés pour la circonstance, hameçonnage (*phishing*) par SMS, téléphone ou courriel (*email*), faux transporteur, faux support technique, faux service après vente, attaques par rançongiciels (*ransomware*)… Toutes les techniques frauduleuses seront 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, les rançonner…

Face à ce phénomène récurrent, **Cybermalveillance.gouv.fr appelle à la plus grande vigilance** et renouvelle ses recommandations pour faire face avec le plus de sécurité possible à cet événement :

1. ***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 vérification (*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. ***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. Retrouvez tous nos conseils pour faire face aux attaques par hameçonnage ici.

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. ***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. Retrouvez tous nos conseils pour bien gérer vos mots de passe ici.

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.

En cas de cyberarnaque ou de cyberattaque, 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.