ALERTE VIGILANCE

22 novembre 2017

Black Friday – Attention aux cyberarnaques !

Black Friday, Cyber Monday, Cyber Week soyez vigilants pour éviter que cette fête aux promotions ne se transforme pour vous en cauchemar.

Le BlackFriday se déroule le lendemain de la fête américaine du Thanksgiving, jour férié aux Etats-Unis, soit le 4e vendredi du mois de novembre. Il marque le coup d'envoi des achats pour les fêtes de fin d'année. Durant 24h la plupart des enseignes de distribution font des offres promotionnelles très alléchantes pour attirer les clients. Cet événement est suivi du Cyber Monday et de la Cyber Week, où les promotions continuent en particulier sur Internet.

Cette année, à compter du vendredi 24 novembre et sur toute la semaine qui suivra, ce sera donc l'euphorie autour des promotions de tout type.

Cet événement sera bien évidemment l'occasion pour les cybercriminels de redoubler d'efforts pour 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 Internet marchands officiels, faux sites créés pour la circonstance, hameçonnage (phishing en anglais) par SMS, téléphone ou courriel (email en anglais), faux transporteur, faux support technique, faux service après vente, attaques par rançongiciels (ransomware en anglais)… Toutes les techniques frauduleuses seront utilisées par les criminels pour tenter 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...

Au regard de cette période périlleuse qui s'annonce, **Cybermalveillance.gouv.fr appelle à la plus grande vigilance** et au respect des recommandations suivantes afin d'éviter que cet événement ne finisse pour vous en « vendredi noir » :

1. **Méfiez-vous des offres trop généreuses** : faites un minimum de vérification (*) au risque de ne jamais voir arriver votre achat ou au mieux vous faire livrer une contrefaçon.
(*) *Réalité de la promotion, notoriété du vendeur, risque de contrefaçon...*

2. **Ne confondez pas vitesse et précipitation** : même pressé par un pseudo vendeur en ligne qui vous propose l'affaire du siècle ne lui donnez pas immédiatement votre numéro de carte bancaire et prenez le temps d'un minimum de vérification (*Existence réelle du vendeur, réalité de la promotion, sécurité de la transaction...*).

3. **Ne rappelez pas inconsidérément des numéros surtaxés** : surtout si des messages énigmatiques vous demandent de recontacter un pseudo transporteur « pour votre livraison » ou un service après-vente « suite à votre achat », préférez rappeler le numéro officiel du transporteur ou du SAV concerné.

4. **Attention à l'hameçonnage** : vérifiez scrupuleusement les adresses d'envois (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…

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 pas pour autre objet que de vous escroquer. (*) vérifiez scrupuleusement l'adresse du site, un seul caractère peut parfois changer.

6. **Protégez vos données personnelles et bancaires** : quitte à rater une très bonne affaire, au moindre doute ne les fournissez pas au risque de conséquences qui pourraient être dramatiques (usurpation d'identité, transactions bancaires frauduleuses...).

7. **Utilisez un mot de passe différent et complexe 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 accès informatiques.

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.

Si vous êtes victime d'un hameçonnage ou d'un rançongiciel, vous pouvez vous référer aux fiches réflexe disponibles sur le site Cybermalveillance.gouv.fr :

https://www.cybermalveillance.gouv.fr/nos-articles/hameconnage-phishing/

https://www.cybermalveillance.gouv.fr/nos-articles/les-rancongiciels-ou-ransomware/

A propos de Cybermalveillance.gouv.fr

Cybermalveillance.gouv.fr est le dispositif national d'assistance aux victimes de cybermalveillance. Ce dispositif a été incubé par l'Agence nationale de sécurité des systèmes d'information (ANSSI) en copilotage avec le ministère de l'Intérieur et le soutien des ministères de l'Économie et des Finances, de la Justice et du secrétariat d'État chargé du Numérique. Il est désormais piloté par le Groupement d'Intérêt Public ACYMA.

Ses publics sont :
- les particuliers,
- les entreprises (hors opérateurs d'importance vitale – OIV – qui relèvent de l'ANSSI),
- les collectivités (hors opérateurs d'importance vitale – OIV – qui relèvent de l'ANSSI).

Ses missions sont :
- l'assistance des victimes d'actes de cybermalveillance,
- l'information et la sensibilisation au niveau national sur la sécurité numérique,
- l'observation du risque numérique pour pouvoir l'anticiper.

*Retrouvez toutes nos publications sur notre site Internet : **www.cybermalveillance.gouv.fr***

Suivez-nous sur nos réseaux sociaux *@cybervictimes*