Article de Bruno Godard du magazine Capital

Les fraudes à la carte bancaire ont touché 1,1 million de Français en 2015, selon un rapport de l'Observatoire national de la délinquance et des réponses pénales (ONDRP) et de l'Insee, publié mercredi 7 décembre.

La majorité des cas concerne les paiements en ligne.

Découvrez les 30 arnaques les plus courantes du e-commerce et les astuces pour ne pas vous faire piéger.

1. L'hameçonnage (ou phishing)

Le principe
Vous recevez un e-mail en provenance de votre opérateur téléphonique, d'EDF ou de votre banque. On vous demande en général de cliquer sur un lien qui vous redirige vers une page qui ressemble au site de l'entité qui vous a prétendument adressé ce message. Et l'on vous demande vos vrais mots de passe. Une fois que le pirate les a récupérés, il peut alors réaliser des opérations sur les sites réels.
La parade
Vous devez lire chaque mail et parcourir les pages avec attention. Dans tous les cas, lorsque vous donnez des informations personnelles, des codes ou des coordonnées bancaires, il faut que les pages soient sécurisées : l'adresse commence par «https », avec un petit cadenas dans la barre en haut à gauche de votre écran.

2. L'attrait du wi-fi gratuit

Le principe
Le Wi-Fi accessible sans avoir à rentrer un mot de passe est une porte grande ouverte vers vos appareils connectés. Des escrocs ont pu créer des hotspots pirates et peuvent siphonner toutes vos données, lorsque vous vous y connectez.
La parade
Evitez les réseaux publics ouverts ou utilisez des VPN (Virtual Private Network), qui sont des plates-formes sécurisées qui cryptent votre activité sur le Net.

3. La loterie bidon

Le principe
Un courriel vous annonce que vous avez gagné un iPhone dernier modèle, un voyage aux Maldives ou une forte somme d'argent. Bien sûr, on vous indique un numéro à appeler (qui sera toujours surtaxé) ou une somme à régler pour les frais de dossier. La ficelle semble énorme, mais de nombreux internautes se laissent pourtant berner.
La parade
Pour éviter cette arnaque, une règle simple : personne ne gagne jamais à une loterie à laquelle il n'a pas participé... Et quand on gagne un vrai concours, on ne verse jamais un seul centime pour récupérer son gain.

4. L'annonce d'emploi payante

Le principe
Sur des sites de petites annonces, des offres d'emploi très alléchantes avec salaires mirobolants sont postées. Mais pour y postuler, des escrocs vous demandent de téléphoner à un numéro surtaxé ou d'envoyer vos coordonnées bancaires et votre numéro de Sécurité sociale.
La parade
Pôle emploi recommande, avant de répondre à une annonce, de googliser le nom de l'employeur et de ne jamais envoyer de données personnelles par mail à un inconnu. Il faut se méfier des offres ne nécessitant aucune expérience, et surtout vérifier avant d'appeler si le numéro est surtaxé. Aucun employeur digne de ce nom ne fait payer des candidats avant de les recruter.

À lire aussi : Comment repérer une offre d'emploi bidon (et se protéger)

5. Le compte Facebook piraté

Le principe
En vous connectant sur votre compte Facebook, vous découvrez de nombreux messages de vos amis se demandant pourquoi vous avez posté sur leur mur une annonce commerciale. Ce sont en général des propositions pour des objets de contrefaçon.
La parade
Votre compte a été piraté et vous devez réagir très vite en changeant votre mot de passe. Puis, dans l'onglet «Historique personnel», retirez cette publication indésirable.

6. La boîte mail piratée

Le principe
C'est l'une des arnaques les plus courantes, et elle peut souvent vous piéger en passant inaperçue pendant quelques jours.
La parade
Si vous avez un doute au sujet de votre boîte mail, allez dans l'onglet «Activité récente» de votre messagerie pour voir si votre compte a envoyé des messages alors que vous étiez censé être déconnecté. Si c'est le cas, changez immédiatement votre mot de passe. Si ce n'est plus possible et que le pirate a pris possession de votre boîte, remplissez le formulaire de récupération de compte de votre fournisseur de messagerie. Changez tous vos autres mots de passe et prévenez votre banque que vous avez été piraté, car les escrocs ont pu lire tous vos mails et avoir accès à des données confidentielles.

> Vidéo. Comment les pirates du web nous piègent :

7. La pétition détournée

Le principe
Vous signez une pétition en ligne qui vous paraît anodine mais, très vite, vous vous rendez compte que l'utilisation qui en est faite va finalement à l'encontre de vos idées.
La parade
Allez sur le site de la pétition et faites une demande de retrait de votre signature. Pour prévenir ce risque, il faut vous renseigner sur l'identité du lanceur de pétition avant de signer afin de ne pas participer à des campagnes qui ne vous correspondent pas.

8. Les impôts remboursés

Le principe
Un mail vous informe d'un remboursement d'impôt... Mais vous devez très rapidement renvoyer vos coordonnées bancaires par mail ou cliquer sur un lien, qui est une fausse page.
La parade
Ce mail est toujours une arnaque car le ministère des Finances a, dans la plupart des cas, vos coordonnées bancaires et ne vous les demandera jamais par mail !

9. La réexpédition de colis

Le principe
Un mail vous propose un travail ne demandant que quelques heures par semaine contre un joli complément de revenus. Selon l'annonce, vous devez simplement réexpédier des colis qui sont livrés chez vous. L'escroc vous envoie un contrat de travail et vous demande des documents officiels. Mais il achète les objets grâce à des cartes volées et, lorsque vous réclamez votre salaire, vous n'avez plus aucune nouvelle.
La parade
Aucune : vous avez simplement servi d'intermédiaire, et les sites escroqués vont se retourner contre vous pour obtenir réparation.

10. Chiens et chats : d'adorables bébés vous attendent

Le principe
Vous recevez un mail avec, en fichier joint, des photos de chiots ou de chatons, craquants. Le prix pour ces animaux est intéressant, mais le vendeur demande 2 000 euros de caution pour le transport. Vous payez et, bien sûr, le chien n'arrive jamais.
La parade
Il est toujours préférable d'acheter des animaux à des éleveurs ayant pignon sur rue ou de vous déplacer pour aller chercher votre compagnon à 4 pattes.

11. Le casino sans fonds

Le principe
Beaucoup de casinos en ligne arnaquent leurs clients en débitant des sommes non jouées et en ne payant jamais les gains. Comme ils sont basés à l'étranger et changent régulièrement de pays, vous n'avez aucune chance de récupérer votre argent perdu.
La parade
Pour éviter ce genre de désagrément, ne jouez que sur des sites qui disposent d'un service client ouvert 24 heures sur 24, et surtout qui ont été agréés par l'Arjel, l'Autorité de régulation des jeux en ligne.

12. Le piratage par rançongiciel

Le principe

Vous recevez un mail avec une pièce jointe. Vous l'ouvrez, un virus envahit votre ordinateur et un message vous demande de l'argent pour le débloquer. Vous venez d'être victime d'un rançongiciel.
La parade
Essayez de vous débrancher immédiatement du réseau, tentez de sauvegarder les dossiers qui ne sont pas encore bloqués et ne payez surtout pas la rançon. Pour s'en protéger, la seule solution est de faire des sauvegardes régulières de toutes vos données sur un disque externe et de ne jamais ouvrir une pièce jointe qui vous paraît suspecte.

13. Le faux mail de Yahoo!

Le principe
Un mail vous informe que votre boîte Yahoo! a été piratée et vous demande vos mots de passe pour récupérer vos données. Un hyperlien est glissé dans le mail et, si vous cliquez dessus, vous envoie sur une fausse page.
La parade
Pour **éviter** le risque, il convient de bien **vérifier** l'adresse de l'**expéditeur** du message et surtout que la page qui s'ouvre commence bien par «https://» et contient un cadenas en haut à gauche.

14. La menace terroriste

Le principe
Un courriel vous informe que vous êtes sur une liste de cibles potentielles d'organisations terroristes. Votre correspondant se fait passer pour un hacker ou un membre d'un service de renseignement et affirme qu'il peut agir pour faire sortir votre nom de cette liste, en échange d'une petite somme d'argent (en général 100 euros).
La parade
Ne **cédez** pas à la panique, ne **répondez** pas au mail et signalez-le sur *https://www.internet-signalement.gouv.fr*

15. Le chantage à l'adresse IP

Le principe
Un mail vous informe que des messages à caractère pédopornographique ou liés à une activité terroriste ont été émis à partir de l'adresse IP de votre ordinateur. On vous menace de vous dénoncer aux services concernés ou de bloquer votre machine à distance. Pour l'éviter, on vous intime d'envoyer une somme d'argent sur un compte PayPal.
La parade
Là aussi, il ne faut pas répondre et signaler au plus vite cette arnaque sur *https://www.internet-signalement.gouv.fr*

16. Les petites annonces de location falsifiées

Le principe
Des escrocs volent des photos sur les sites de location et les postent pour leurrer des internautes. Ils demandent des arrhes, les encaissent, mais vous ne pourrez jamais utiliser la maison.
La parade
Avant de louer, il convient de toujours faire quelques vérifications en googlisant le nom du loueur et l'adresse de sa maison pour vérifier que les deux coïncident. Il faut aussi appeler l'office du tourisme de votre lieu de vacances afin de vérifier que la personne qui a posté l'annonce est bien référencée.

17. Les faux amis Facebook

Le principe
Une inconnue, souvent charmante, veut faire partie de vos amis ou contacts sur les réseaux sociaux. Souvent parce qu'elle trouve votre photo de profil «très jolie»... Bien sûr, ces profils sont des faux, créés par des escrocs, la plupart du temps basés au Sénégal et baptisés «brouteurs». Leur but : nouer une fausse relation amicale ou sentimentale avec vous, pour finalement vous demander de l'argent (pour payer un voyage, financer une opération ou un traitement médical pour eux ou un proche, payer des études, ou juste leur venir en aide...).
La parade
Là encore, une règle simple : ne jamais envoyer d'argent à des inconnu(e)s.

18. Les numéros surtaxés

Le principe
Vous recevez par mail un mot de votre banque, par exemple, vous demandant de l'appeler de toute urgence ou un message vous suggérant d'écouter très rapidement votre boîte vocale. Dans les deux cas, on vous propose d'appeler un numéro qui, à chaque fois, est surtaxé.
La parade
Si un mail ou un SMS vous indiquent d'écouter un message vocal ailleurs que sur votre propre répondeur, fuyez ! L'arnaque est garantie à 100 %. Et même si des entreprises honnêtes utilisent parfois des numéros surtaxés, elles ont l'obligation légale de préciser le prix de l'appel.

À lire aussi : Arnaques aux appels surtaxés, enfin de grosses amendes !

19. Les appels au secours

Le principe

Un de vos contacts vous informe par mail qu'il est bloqué dans un pays étranger où il s'est fait dérober tous ses papiers et son argent. Il précise parfois être injoignable et vous demande d'opérer un transfert d'argent afin de le sortir de cette mauvaise passe.
La parade
La plupart du temps, la boîte mail de votre contact a été piratée et c'est un escroc qui l'utilise pour réclamer de l'argent. N'oubliez jamais que lorsqu'on est en difficulté à l'étranger, on trouve toujours un téléphone pour donner l'alerte à la famille ou aux amis. Personne n'envoie de mail dans ce genre de situation !

20. Les pièges des sites de charme

Le principe
Multiplication des pop-up, pages ouvertes restant dans le cache de votre machine, numéros surtaxés, les sites érotiques peuvent également être infestés de virus qui se chargent lorsque l'on clique sur un lien proposant des vidéos gratuites. Certains sites peuvent vous réclamer un numéro de carte bancaire pour prouver que vous êtes majeur. Et vous débitent de petites sommes qui peuvent passer inaperçues.
La parade
Dans tous les cas, il est formellement déconseillé de donner des informations bancaires sur ces sites. Surtout, ne cliquez jamais sur les liens qui s'affichent dans les pop-up... Et limitez votre surf aux géants du secteur qui ont pignon sur rue.

21. ... et ceux des sites de rencontre

Le principe
Sur ces sites, comme dans la vraie vie, des escrocs peuvent se cacher derrière un sourire avenant. Et même sur des plates-formes réputées pour leur sérieux, comme Meetic, on peut tomber sur des malfaisants.
La parade
La règle de base est de ne jamais fournir de données personnelles (adresse précise, numéro de téléphone, coordonnées bancaires...) avant la première rencontre qui, de préférence, doit avoir lieu dans un endroit public, et plutôt dans la journée.

22. Le crédit providentiel

Le principe
Par mail, mais aussi sur des forums, de «généreux internautes» proposent des crédits entre particuliers. Et, bien entendu, ils demandent une avance de quelques centaines d'euros pour débloquer ces sommes qui bien sûr n'arrivent jamais.
La parade
Même si certains, en proie à de graves difficultés financières, peuvent se faire prendre, le bon sens doit être en éveil : on ne doit jamais verser un seul centime pour obtenir un prêt ! Et ne pas oublier que personne ne prête gratuitement de l'argent à quelqu'un qu'il ne connaît pas.

23. La commande acceptée

Le principe
Un site vous affirme par mail que la commande que vous avez passée a été acceptée... alors que vous n'avez rien commandé du tout. Le montant de votre achat, assez important, est précisé dans le corps du mail, on vous affirme que la somme va être débitée. Pour annuler la commande, on vous propose d'appeler un numéro de téléphone, qui bien sûr est surtaxé.
La parade
Ne paniquez pas, vérifiez votre compte en banque. Et rappelez-vous qu'aucun site marchand n'utilise de numéros surtaxés pour ses livraisons.

À lire aussi : Acheter en ligne sans se faire arnaquer

24. Le chantage à la sextape

Le principe
Sur les sites de rencontre, ou sur les réseaux sociaux, des escrocs, après des jours de mise en confiance, proposent à leurs interlocuteurs de se montrer nus sur des photos ou via des webcams. Puis ils exercent un chantage en menaçant d'envoyer les images compromettantes aux proches de leurs victimes si ces dernières ne leur versent pas une somme d'argent.
La parade
N'envoyez jamais des photos dénudées à des inconnus. En cas de chantage, n'hésitez pas à porter plainte.

25. Un smartphone à 1 euro

Le principe
Sur les réseaux sociaux, des publicités alléchantes vous proposent des smartphones haut de gamme à 1 euro. On vous demande vos coordonnées bancaires, mais lorsque vous avez fini l'inscription, on vous prévient que vous participez simplement à une tombola. Vous pensez n'avoir perdu que 1 euro, mais, le mois suivant, votre compte sera débité de plusieurs dizaines d'euros car vous avez été inscrit sans le savoir à plusieurs sites payants.
La parade
Restez lucide ! On ne peut pas payer 1 euro un smartphone qui en coûte plus de 700...

26. Le colis inattendu

Le principe
Vous recevez un texto ou un mail vous précisant que vous avez reçu un colis et qu'il est disponible dans un relais colis. Pour le récupérer, on vous précise que vous devez d'abord appeler un numéro de téléphone. Sauf que vous n'aviez rien commandé.
La parade
Pour éviter d'appeler ce numéro surtaxé, il faut simplement vérifier plusieurs points : le marchand doit être clairement identifié dans le message, le numéro du colis doit correspondre au numéro de confirmation d'une commande que vous avez passée, et l'adresse du point relais doit être spécifiée.

27. Le vendeur fantôme

Le principe
Sur les sites de petites annonces entre particuliers, des escrocs font des offres alléchantes avec des produits à des prix modiques. Vous envoyez votre chèque, il est encaissé, l'objet acheté n'arrivera jamais.
La parade
Pour limiter les risques, il faut entrer en contact direct avec le vendeur, lui parler au téléphone si possible et surtout utiliser des modes de paiement comme PayPal, qui vous garantissent une traçabilité de la transaction.

28. Le faux antivirus

Le principe
Vous êtes en train de naviguer sur le Net quand, soudain, un pop-up s'affiche sur votre écran, expliquant que votre ordinateur contient un virus. Pour régler ce problème, le message vous propose un lien vers un antivirus contre le paiement de quelques euros. Si vous le faites, vous allez télécharger un antivirus bidon qui ne servira à rien, voire un virus qui bloquera votre ordinateur.
La parade
La règle est de fermer immédiatement ce pop-up car aucun éditeur de logiciels antivirus sérieux n'utilise cette méthode pour recruter de nouveaux clients.

29. Les cartes de paiement sans contact

Le principe
Grâce au système NFC (Near Field Communication), on peut régler certains achats sans avoir à taper son code. On passe simplement la carte sur le lecteur et le tour est joué. Mais, dans les transports en commun ou même dans les magasins, certains pirates peuvent, à l'aide d'un simple smartphone équipé d'une appli malveillante, récupérer les données de votre puce.
La parade
Dans les faits, le risque est limité car ce système de paiement ne vaut que pour les achats de moins de 20 euros. Mais on peut se munir d'un étui de protection isolant qui, pour moins de 1 euro, évitera tout risque de piratage.

30. L'intrusion de pirates dans votre cloud

Le principe
Coffre-fort numérique virtuel, le Cloud permet de stocker des documents, des photos ou des vidéos et d'alléger la mémoire de votre ordinateur. Mais attention, votre code peut être piraté et les malfrats peuvent mettre la main sur des données sensibles.
La parade
Pour un mot de passe sûr, il faut utiliser au moins 10 caractères, avec trois types différents (chiffres, caractères spéciaux et lettres). Si vous avez un doute (comportement anormal de l'ordinateur, antivirus qui se déclenche, mails étranges), changez-en immédiatement. Et surtout, utilisez- le uniquement pour ce service de stockage de données.