**ADRER**
**Association pour un développement réfléchi et équilibré du Rayol-Canadel**
Rayol Park 83820 Rayol-Canadel sur Mer, www.adrer.fr

# Arnaques sur Internet

Dans ce 63ème numéro, qui sort de nos sentiers habituels, mais en tant qu'association d'usagers, avec l'augmentation sans précédent des tentatives d'arnaques et la sophistication de plus en plus grande des auteurs, il nous a semblé utile de partager avec nos adhérents, l'article ci-dessous paru dans ''UFC QUE CHOISIR'' de juin 2020, que nous reproduisons avec l'accord de la rédaction du magazine que nous remercions.

ZONE ROUGE — DOSSIER DU MOIS

## ARNAQUES SUR INTERNET
## Les repérer, bien réagir,

Achats, paiement des impôts... Internet s'est imposé dans notre quotidien et cela a favorisé le développement des escroqueries en ligne. *Que Choisir* décrypte les principales arnaques et vous donne des conseils pour vous en protéger ou réagir si vous en avez été victime.

— Par **MARIE BOURDELLÈS** et **CAMILLE GRUHIER** - Illustrations : **RÉGIS FALLER**

Faux diagnostic après l'incendie de l'usine Lubrizol à Rouen (76), investissement frauduleux lors de la privatisation de la Française des jeux… les arnaques du Web collent à l'actualité. L'épidémie de Covid-19 le démontre une nouvelle fois. Au cours de la crise sanitaire, de faux sites d'attestations de sortie dérogatoire se sont multipliés, et des e-commerçants ont vendu des masques inefficaces, voire de soi-disant produits miracles, ou bien n'ont pas honoré les commandes. Certains ont même commercialisé illicitement des médicaments. Sans compter les appels aux dons douteux. *« Le coronavirus crée un cocktail numérique explosif : les utilisateurs sont stressés, les apprentis télétravailleurs se multiplient et les cyberattaques augmentent »*, confirme Alain Bouillé, le délégué général du Club des experts de la sécurité de l'information et du numérique (Cesin). De la plateforme marchande vérolée au portail administratif détourné, ces escroqueries sur Internet sont bien connues et les modes opératoires, finalement, toujours identiques. Ce qui change, c'est leur habillage.

**Une cybercriminalité sous-évaluée**

Impossible, à notre époque, d'ignorer la cybercriminalité. Nous sommes tous connectés au Web en permanence, à la maison, dans la rue, depuis un ordinateur, une tablette ou un smartphone. Du virement bancaire à la réservation de voyages, notre quotidien est numérique, et les aigrefins s'adaptent. Piratage des appareils, escroqueries et faux moyens de paiement constituent les piliers d'une e-délinquance que l'on sait sous-évaluée. *« Policiers et gendarmes estiment, à la louche, les plaintes ayant une dimension cyber à environ 30 à 50 %, mais il s'agit d'un ressenti du terrain, pas de chiffres officiels »*, explique François-Xavier Masson, directeur de l'Office central de lutte contre la cybercriminalité liée aux technologies de l'information et de la communication (OCLCTIC). Ce qui est sûr? La croissance du nombre de cybercrimes s'avère exponentielle, et ceux-ci sont de plus en plus évolués. *« L'orthographe dans les e-mails constituait un indice. Or, les messages sont désormais parfaitement rédigés. Vos interlocuteurs au bout du fil n'ont plus d'accent et les numéros de téléphone sont locaux*, ajoute Pierre Penalba[1], qui dirige, entre autres, le groupe de lutte contre la cybercriminalité de la police judiciaire de Nice (06). *Du coup, les internautes, même prudents, se laissent piéger. »*

**Gendarmes et policiers estiment que 30 à 50 % des plaintes ont une dimension cyber**

**La peur et la honte, des leviers efficaces**

Cybermalveillance.gouv.fr établit des statistiques. En 2019, la plateforme publique d'assistance et de prévention du risque numérique a vu le phishing et le piratage de compte d'utilisateur ou d'ordinateur (lire le lexique p. 16) se classer en tête des attaques avec, respectivement, 13 % et 14 % des cas recensés. Le chantage à la webcam prétendument hackée a affolé les compteurs et représente 38 % des demandes d'aide déposées sur le site. Vous en avez sans doute entendu parler : si vous ne lui versez pas une rançon, un malfaiteur vous menace par courriel de diffuser des vidéos compromettantes. Vous avez beau savoir que c'est impossible, vous paniquez. *« Ces maîtres chanteurs adorent jouer avec les sentiments comme la peur et la honte, parce que c'est efficace »*, analyse Pierre Penalba. Sans oublier les escroqueries à la romance. Les sites de rencontres ou les réseaux sociaux sont les terrains de chasse favoris de ces « arnacœurs », qui créent de faux profils d'hommes et de femmes pour harponner puis séduire leurs proies. L'objectif? Leur extorquer des fonds. *« Certains peuvent enfoncer leurs victimes dans la honte pour les maintenir sous pression : cela concerne souvent des personnes âgées ou des relations homosexuelles cachées. Ces victimes*, poursuit le policier, *n'osent en parler à personne. Et le vivent si mal qu'elles peuvent aller jusqu'au suicide. »*
Tablant davantage sur l'appât du gain que sur les émotions, le phishing, qui vise à collecter vos données personnelles dans le but d'usurper votre identité ou de vous voler de l'argent, grimpe cette année sur la première marche du podium. La nouveauté, c'est la montée en puissance des tentatives via les >:

14 — QUE CHOISIR 592 • JUIN 2020

**ADRER**
**Association pour un développement réfléchi et équilibré du Rayol-Canadel**
Rayol Park 83820 Rayol-Canadel sur Mer, www.adrer.fr

ADRER
Association pour un développement réfléchi et équilibré du Rayol-Canadel
Rayol Park 83820 Rayol-Canadel sur Mer, www.adrer.fr



ILS L'ONT VÉCU

**CHANTAGE À LA WEBCAM**

*J'ai reçu un e-mail qui menaçait de révéler des images de moi « en train de faire des choses devant un film porno » si je ne payais pas 1900 $ dans les 24 heures. J'ai été transie de peur. Je savais pourtant que c'était impossible : je n'ai jamais visité un site pornographique !* **Ève C., Bagnolet (93)**

>>> SMS et MMS envoyés en rafale sur les téléphones portables. *« Les consommateurs sont incités à visiter des sites frauduleux. À présent plus utilisé qu'un ordinateur pour surfer sur Internet, le smartphone représente une véritable opportunité pour les escrocs »*, certifie Jean-Jacques Latour, responsable de l'expertise en cybersécurité de Cybermalveillance.gouv.fr.

### Afrique et Europe de l'Est, les épicentres

Les autorités sont sur le pont. Aujourd'hui, 140 personnes sont regroupées au sein de la Sous-direction de lutte contre la cybercriminalité (SDLC), dont 70 policiers, gendarmes, ingénieurs, qui mènent l'enquête au quotidien à l'OCLCTIC. Au total, dans la police nationale, 600 agents ont reçu un enseignement spécial pour adopter les réflexes d'un bon cyberenquêteur, et 50 autres (policiers et gendarmes) sont formés chaque année avant de réintégrer leur service. *« La lutte contre la cybercriminalité est une priorité du gouvernement, qui déploie une politique forte pour renforcer ses moyens »*, assure François-Xavier Masson, le directeur de l'OCLCTIC. Pourtant, les résultats ne reflètent pas forcément cette détermination. Le commissaire précise : *« Sur les 200 000 signalements qui nous parviennent tous les ans via la plateforme Pharos* (lire encadré p. 21), *la majorité reste sans suite. Parce qu'ils ne relèvent pas du pénal, que l'arnaque a disparu ou que les escrocs sont installés à l'étranger. Seulement 300 cas donnent lieu à une procédure judiciaire. »*

En effet, toute la difficulté consiste à mettre la main sur les auteurs. Les pirates sont des as de l'informatique. Ils changent d'identité, se cachent derrière des Virtual Private Network (VPN, des « tunnels » sécurisés) pour dissimuler leur adresse IP (celle qui permet de localiser un ordinateur). Et surtout, ils se trouvent en Afrique et en Europe de l'Est, ce qui coupe court aux investigations françaises, malgré l'existence d'instances internationales de coopération comme Europol et Interpol. *« Il faut aussi une volonté politique,* insiste Pierre Penalba. *Au Nigeria, au Bénin, en Côte d'Ivoire, les "brouteurs" ont pignon sur rue et personne ne les ennuie. Avec les 100 000 € mensuels qu'ils gagnent, quand le salaire moyen s'élève entre 55 € et 110 € environ, ils ont largement de quoi arroser tout le monde. »* Peur, chantage, menaces… et corruption, donc. Les arnaques sur Internet collent à l'actu, mais elles piquent aussi les codes du polar. Un mauvais polar sans fin, hélas. ◆

*(1) Pierre Penalba est aussi l'auteur de* Cyber crimes *(Albin Michel, 19,90 €), un recueil d'arnaques croustillantes et drôles (ou pas).*

## LEXIQUE

**# Arnaque, escroquerie** Vous êtes victime d'une escroquerie lorsque vous avez volontairement remis un bien ou de l'argent, ou encore que vous avez rendu un service à quelqu'un, à la suite d'une tromperie. L'auteur de ce délit risque cinq ans d'emprisonnement et 375 000 € d'amende. L'arnaque est un mot du langage courant, sans portée pénale.

**# Botnet** Réseau d'ordinateurs reliés entre eux après leur infection par un logiciel malveillant et contrôlés à distance par des pirates.

**# Courrier indésirable *(spam ou pourriel)*** Courrier électronique, souvent publicitaire, envoyé à un grand nombre d'internautes sans leur consentement. Certains messages cachent des liens suspects ou des pièces jointes vérolées.

**# Cybercriminalité** Toute infraction commise à l'encontre ou par le biais d'un appareil numérique.

**# Dark Web** La face sombre d'Internet, dont le contenu s'avère le plus souvent illégal. Notez qu'il sert également dans certains pays pour éviter la censure.

**# Données personnelles** Celles-ci permettent d'identifier directement (nom, prénom) ou indirectement une personne (numéro de Sécurité sociale, adresse, photo, etc.).

**# Malware *(logiciel malveillant ou maliciel)*** Terme générique désignant les logiciels hostiles ou intrusifs (spyware pour espionner, adware destiné à imposer de la publicité, etc.).

**# Piratage *(hacking)*** Activité qui s'attache à compromettre les ordinateurs, les smartphones ou les tablettes (ou des réseaux). Virus, botnets et malwares sont des techniques parmi d'autres.

**# Phishing *(hameçonnage)*** Ce procédé consiste à vous faire croire que vous vous adressez à votre banque, au Trésor public ou à un autre interlocuteur connu pour obtenir vos renseignements personnels.

**# Scam** Il s'agit d'un pourriel, qu'on appelle aussi « arnaque nigériane », visant à abuser de la confiance du destinataire pour obtenir de l'argent.

**# Usurpation d'identité** Des données personnelles qui servent à vous identifier sont volées afin de nuire à votre réputation, de « pourrir » vos réseaux sociaux ou de réaliser des transactions et des infractions en votre nom.

**# Virus informatique** On appelle ainsi un programme malveillant logé dans un fichier (pièce jointe à un e-mail, par exemple) et conçu pour se propager d'un appareil à un autre.

ADRER
Association pour un développement réfléchi et équilibré du Rayol-Canadel
Rayol Park 83820 Rayol-Canadel sur Mer, www.adrer.fr



# LES MODES OPÉRATOIRES
# Toute la journée, de multiples pièges

**Lorsque vous lisez vos e-mails, naviguez sur Internet ou bien parcourez les réseaux sociaux, vous êtes exposé à des arnaques ! Voici les principales.**

## 1 Je regarde mes e-mails

Difficile de garder une boîte e-mail « propre », sans spams (pourriels). Signal Spam, une association qui lutte contre ces messages indésirables, reçoit plus de deux millions de signalements par mois. *« Parmi eux, 90 % comportent du contenu marketing et 10 % sont issus de la cybercriminalité »*, précise Thomas Fontvielle, son secrétaire général. Le phishing (hameçonnage) constitue la première menace. Cette technique utilisée par les e-délinquants consiste à vous envoyer des courriels censés émaner d'administrations (impôts, Caf, Ameli...), d'opérateurs (Orange, EDF...) ou de grandes enseignes (Fnac, Cdiscount...). Sous le prétexte fallacieux d'une mise à jour de vos informations, d'une compromission de votre compte ou d'une commande que vous avez soi-disant effectuée, un lien vous mène vers un faux site, qui usurpe l'identité visuelle du tiers de confiance. Vous êtes alors invité à entrer des informations personnelles, ensuite dérobées à des fins illégales. *« Entre cinq et six plateformes frauduleuses sur les impôts sont signalées, chaque semaine, à la Direction générale des finances publiques »*, se désole Jean-Jacques Latour, de Cybermalveillance.gouv.fr, le site gouvernemental d'assistance et de prévention du risque numérique.

### Scams et virus à foison

Deuxième attaque fréquente : le scam, ce courriel supposé avoir été écrit par une de vos connaissances, bloquée à l'étranger sans moyen de paiement, qui implore une aide financière. En réalité, elle s'est fait pirater sa messagerie électronique. Un escroc a volé ses identifiants de connexion puis transmis l'e-mail désespéré à son répertoire, dont vous faites partie. En tel cas, prévenez votre contact ! Enfin, n'ouvrez pas n'importe quelle pièce jointe et ne cliquez pas sur un lien suspect : des virus informatiques pourraient infecter votre équipement. Une fois installés, ces programmes malveillants, désormais invisibles, sont capables soit d'aspirer vos données pour un usage frauduleux, soit de se servir de votre adresse IP pour constituer un réseau de machines (ou botnet, lire le lexique p. 16) et envoyer des campagnes de phishing à votre insu.

**ILS L'ONT VÉCU**

**SCAM**

*Le père de ma belle-fille m'a appelée parce qu'il avait reçu un e-mail douteux de moi. J'ai compris que ma boîte avait été piratée. Les escrocs ont envoyé un message à tous mes contacts. J'ai paniqué. J'ai appelé Orange, qui m'a aidée à changer mon mot de passe.*

**Thérèse L., Dainville (62)**

>>>

**ADRER**
**Association pour un développement réfléchi et équilibré du Rayol-Canadel**
**Rayol Park 83820 Rayol-Canadel sur Mer, www.adrer.fr**



# LES MODES OPÉRATOIRES

## 2 Je navigue sur Internet

Sans Internet, pas d'e-mails, pas de conversations virtuelles ni d'achats en ligne... mais pas d'escroqueries numériques non plus ! Quand vous consultez un site d'information ou d'e-commerce, vous n'êtes pas à l'abri de tomber dans un piège. Les bannières publicitaires qui s'affichent peuvent parfois être corrompues par des pirates informatiques, au même titre que les réclames apparaissant sur les réseaux sociaux ou dans votre messagerie électronique. Certaines de ces publicités vous redirigeront vers de fausses plateformes d'investissement, qui promettent des rendements rapides et élevés. Bitcoins, vaches laitières, placements financiers... la liste est longue, les bandits s'adaptant à l'actualité pour diversifier leurs « offres ». Vous pensez faire fructifier votre épargne, alors que vous enrichissez des brigands situés à l'étranger. Et comme vous avez effectué vous-même le virement, votre banquier refusera de vous rembourser.

### Les malfaiteurs ont progressé

Certains portails marchands ont recours aux mêmes stratagèmes : une annonce alléchante associée à un site au design séduisant (les malfaiteurs ont beaucoup progressé en orthographe et en graphisme, méfiance). Les pratiques frauduleuses liées à la crise du coronavirus (vente illégale de médicaments, commercialisation de masques inefficaces...) illustrent parfaitement ce phénomène. Votre commande ne sera pas honorée ou, au pire, vous recevrez des produits défectueux, voire dangereux ! Et vos informations personnelles seront pillées : soit vous serez abonné à un service obscur vous coûtant 49 € par mois (arnaque à l'abonnement caché), soit votre compte sera soudainement débité, ou votre identité, usurpée. Les pirates installeront parfois un programme malveillant sur votre machine. Il s'agit de l'arnaque au faux support technique. D'un coup, votre écran s'éteint,

## 3 Je visite les réseaux sociaux

Twitter, Snapchat... les arnaques se multiplient sur les réseaux sociaux et prennent des formes diverses et variées. Y pullulent, par exemple, des annonces de comptes frauduleux vous promettant un gain comme un smartphone ou des bons d'achat. **La page sur laquelle vous serez dirigé cache un dispositif de phishing.** Sur Facebook et Instagram principalement, méfiez-vous des publicités vantant des produits miracles ou bon marché : lingerie anticancer, vêtements à des prix défiant toute concurrence, ventilateur par temps de canicule... Vous risquez d'atterrir sur un site illicite : votre argent sera empoché mais vous ne recevrez jamais le produit, ou alors il se révélera défectueux. Quant à se faire rembourser, c'est en général... mission impossible.

### Le smartphone augmente les risques

Utilisé par les trois quarts des Français, le smartphone permet d'accéder à tous les services en ligne. Or, moins sécurisé qu'un ordinateur, il présente certains dangers qui lui sont propres, entre les faux appels en absence *(ping calls)*, les messages indésirables et les campagnes de phishing. Pour ces dernières, les escrocs récupèrent des fichiers de numéros de téléphone sur le dark Web (la partie « cachée » et dangereuse d'Internet), envoient des SMS en masse, avec un lien vers un site frauduleux. Attention également aux virus dissimulés dans les applications que vous téléchargez. Invisibles, ils aspirent vos données (coordonnées bancaires, identité).

ADRER
Association pour un développement réfléchi et équilibré du Rayol-Canadel
Rayol Park 83820 Rayol-Canadel sur Mer, www.adrer.fr

et un message vous avertit qu'un virus infecte votre ordinateur. Un numéro de téléphone est indiqué. Les margoulins qui vous répondront vous demanderont de payer pour être dépanné. En aucun cas, ne versez de l'argent. Faites appel à un technicien en informatique (Microsoft, société de dépannage...).



ILS L'ONT VÉCU

**FAUX JEU-CONCOURS**

*J'ai reçu un message privé sur Messenger, m'annonçant que j'avais été tirée au sort pour remporter un Thermomix. Il fallait que j'appelle un numéro payant pour obtenir des codes de validation. J'ai téléphoné à huit reprises, cela m'a coûté 74 €. Je n'ai pas été remboursée et n'ai rien gagné !*

**Laëtitia F., Crest (26)**

**SUPPORT TECHNIQUE FRAUDULEUX**

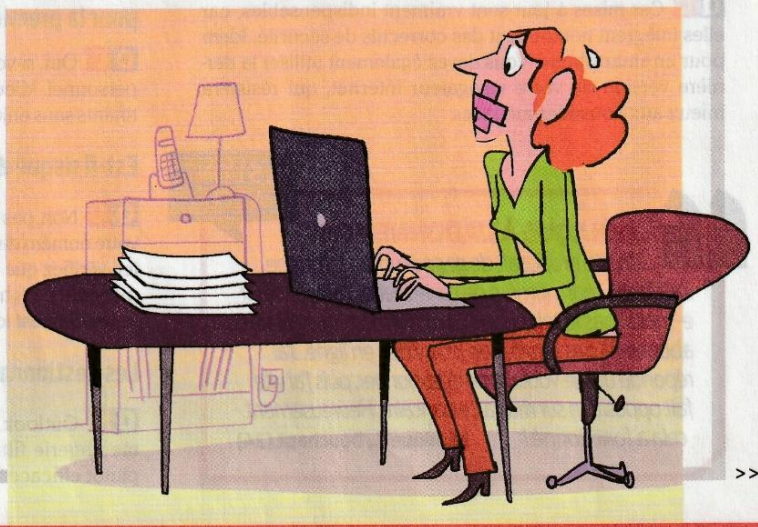
*Mon ordinateur s'est éteint et un message est apparu : je devais donner 300 € pour le désinfecter. Ça inquiète ! Donc, j'ai payé. La banque m'a dit :* « Vous avez fourni votre numéro de carte bleue, tant pis pour vous. »

**Monique D., Benquet (40)**

## 4 Je discute sur des messageries instantanées

Autre vecteur de pratiques trompeuses : les messageries instantanées, telles que Messenger, WhatsApp ou Telegram. Les mêmes « bons plans » rencontrés sur les réseaux sociaux sont parfois relayés par vos contacts, ignorant qu'il s'agit de pièges. Mais également par des personnes que vous ne connaissez pas, qui vous ont d'abord invité sur les réseaux sociaux et se servent de ces messageries pour lancer, entre autres, des arnaques à l'offre d'emploi. Des bandits se font en effet passer pour de potentiels recruteurs et abusent de la détresse de certains chômeurs. Par exemple, un petit boulot bien payé vous est proposé. Votre interlocuteur échange par écrit avec vous. Il vous envoie un chèque sous un prétexte fallacieux, comme l'achat de matériel ou le paiement d'un loyer. D'abord crédité sur votre compte, il est ensuite débité, car volé ou sans provision. Fanny C., victime de ce procédé, a perdu plus de 3 000 €.

Gare aussi à l'arnaque au sentiment ! **Des escrocs créent de faux profils pour harponner leurs proies.** Ils les contactent sur Skype ou WhatsApp, par exemple, et au fil des messages, feignent le grand amour. Pendant des semaines, voire des mois, une soi-disant relation de couple se construit et des plans d'avenir sont échafaudés jusqu'à ce qu'un rendez-vous soit fixé. Mais juste avant la rencontre, alléguant un accident, une maladie ou une agression, ces aigrefins prient leurs victimes d'effectuer un transfert de fonds. Et continueront à leur extorquer de l'argent avant de disparaître dans la nature.



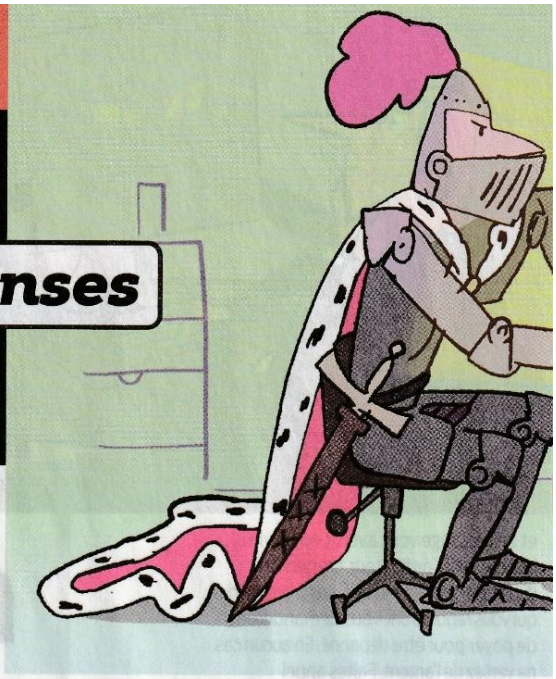
>>>

ADRER
Association pour un développement réfléchi et équilibré du Rayol-Canadel
Rayol Park 83820 Rayol-Canadel sur Mer, www.adrer.fr



# VOS QUESTIONS Nos réponses

Mises à jour logicielles, sécurisation du réseau wifi, publication sur les réseaux sociaux... Nos recommandations pour limiter les risques de se faire avoir !



## Quel est le risque de me faire arnaquer sur Internet ?

QC Le danger est réel : 90 % des Français déclarent avoir déjà été confrontés à la cybermalveillance. Qui n'a jamais hésité à cliquer sur un lien ou une pièce jointe ? Les comptes Facebook sont souvent piratés. Sur Internet, la vigilance s'impose. Soyez prudent par principe.

## Faut-il verrouiller l'accès à son smartphone avec un code ?

QC Oui ! Cela vaut aussi pour l'ordinateur portable. Une combinaison à quatre chiffres ralentira déjà le voleur (si ce n'est pas 0000 !), mais si elle est composée de six chiffres, cela lui compliquera davantage la tâche. Méfiez-vous de la fonction de reconnaissance faciale des smartphones. Lors de nos tests en laboratoire, nous la dupons régulièrement avec une simple photo imprimée sur une feuille A4. Les systèmes perfectionnés sont réservés aux appareils haut de gamme.

## Mon ordinateur me propose souvent d'installer des mises à jour. Suis-je obligé de le faire ?

QC Ces mises à jour sont vraiment indispensables, car elles intègrent notamment des correctifs de sécurité. Idem pour un smartphone. Vous devez également utiliser la dernière version de votre navigateur Internet, qui résistera mieux aux nouvelles menaces.

ILS L'ONT VÉCU

### ARNAQUE À L'ABONNEMENT

*Un site proposait de gagner un smartphone. J'ai donné mon numéro de carte bleue. J'ai reçu deux e-mails (pas le téléphone !) m'informant que j'étais abonnée à des services de jeux vidéo en ligne. J'ai répondu que je voulais me désabonner, puis j'ai vite fait opposition sur ma carte bancaire. Heureusement, cela a fonctionné !* **Monique T., Douchapt (24)**

## Trop de mots de passe à gérer ! Je me sers du même pour tous mes comptes. Ça pose un problème ?

QC Oui ! C'est une grave erreur, car si un pirate le découvre, il accédera à tous vos comptes. Certains logiciels sont dédiés à la gestion des mots de passe. *Que Choisir* les a testés, ils sont efficaces et sûrs. Sinon, adoptez une méthode mémorisable et déclinable (par exemple, le Lundi, je Joue au Squash dans le 94 devient « lLjJSq*94 », le Mardi je Joue au Tennis dans le 75 devient « lMjJTe*75 », etc.). Soignez le mot de passe de votre boîte e-mail principale et changez-le régulièrement. Enfin, si possible, activez la double authentification (en plus du mot de passe, un code envoyé par SMS valide la connexion).

## Mon navigateur Internet me propose d'enregistrer mes identifiants quand je les renseigne pour la première fois sur un site. Est-ce sûr ?

QC Oui, si vous vous connectez depuis votre ordinateur personnel. Mieux vaut toutefois n'y consigner que les identifiants sans enjeu (ni carte bancaire, ni données sensibles).

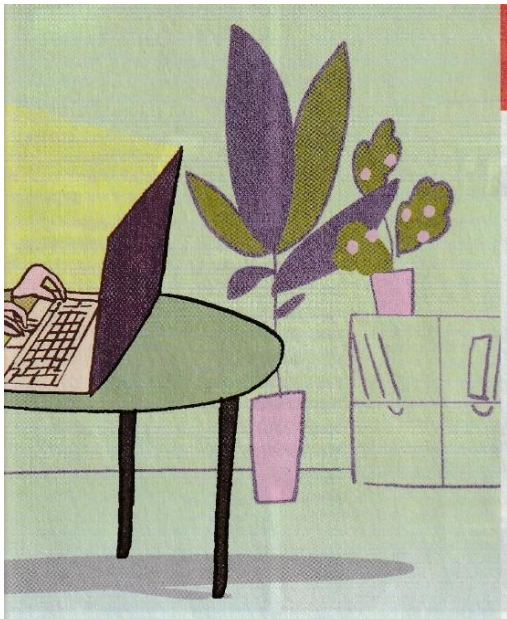
## Est-il risqué de payer avec ma carte bancaire ?

QC Non, pas plus qu'en magasin. Mais ne fournissez jamais votre numéro de carte dans un autre contexte. Et avant d'acheter, vérifiez que le site est sécurisé (adresse de la page commençant par « https » et précédée d'un petit cadenas) et que le vendeur est identifiable (adresse, numéro de téléphone).

## Les gestionnaires de spams sont-ils fiables ?

QC Outlook, Gmail, Yahoo ! et les autres services de messagerie filtrent les e-mails qu'ils jugent indésirables plutôt efficacement. Malheureusement, leur système n'est

ADRER
Association pour un développement réfléchi et équilibré du Rayol-Canadel
Rayol Park 83820 Rayol-Canadel sur Mer, www.adrer.fr



pas fiable à 100 %. Ainsi, il arrive de trouver un « bon » courriel dans les spams, et inversement. Du coup, restez très prudent, surtout lorsque vous ne connaissez pas l'expéditeur d'un message. Un simple clic un peu trop rapide sur un lien ou une pièce jointe suffit pour installer un logiciel malveillant sur votre ordinateur.

### Peut-on être infecté par une appli mobile téléchargée dans l'App Store ou le Google Play Store ?

**Q C** C'est hélas possible ! Les smartphones, désormais plus utilisés que les ordinateurs pour se connecter à Internet, représentent évidemment des cibles de choix pour les pirates. Le nombre d'applications vérolées, principalement dans le Google Play Store (Apple se montre plus vigilant), est donc devenu élevé. D'un aspect normal (jeux, utilitaires, etc.), elles dissimulent des logiciels malveillants pour, par exemple, pirater des comptes Facebook et y poster de faux commentaires.

### On m'a conseillé d'utiliser des adresses e-mail différentes selon les sites, est-ce utile ?

**Q C** Vous pouvez recourir à une adresse e-mail pour les échanges nécessitant votre vrai nom (administrations, banques, etc.) et à une autre pour les sites de vente en ligne, les réseaux sociaux, etc.

### Doit-on accepter tout le monde comme ami sur Facebook ou autre ?

**Q C** Non, car quelle que soit l'identité affichée, vous ne savez pas qui se cache derrière un profil. Limitez plutôt vos contacts au strict minimum. Les réseaux sociaux constituent un puits d'arnaques.

ZONE ROUGE

## BIEN RÉAGIR

### EN CAS D'ESCROQUERIE

**# Alertez** rapidement votre banque pour annuler l'opération et faites opposition à votre carte bancaire si elle a été utilisée par l'escroc.
**# Consignez** toutes les preuves possibles : URL, capture d'écran, référence de la transaction...
**# Déposez plainte** contre l'auteur des faits ou, s'il n'est pas identifié, contre X. Les autorités développent une plateforme en ligne, baptisée Thésée, pour faciliter la démarche. Elle sera opérationnelle dans le courant de l'année.

### EN CAS DE CYBERATTAQUE

**# Déconnectez** votre ordinateur d'Internet et lancez immédiatement l'antivirus.
**# Modifiez** vos mots de passe. Conservez les preuves, signalez l'attaque et portez plainte.

### SITES ET NUMÉROS UTILES

**#Internet-signalement.gouv.fr**
Pour dénoncer tout acte de cybercriminalité (escroquerie, mais aussi incitation à la haine, etc.). La plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (Pharos) mènera l'enquête.
**# Info Escroqueries : 0 805 805 817**
Gendarmes et policiers pourront vous conseiller et vous orienter.
**# Cybermalveillance.gouv.fr**
C'est la plateforme d'assistance et de prévention du risque numérique du gouvernement.

### Sur les réseaux sociaux, faut-il éviter de poster du contenu personnel ?

**Q C** Oui, car toute donnée déposée sur Internet nous échappe instantanément. N'importe qui peut enregistrer une photo publiée et s'en servir. Pensez d'ailleurs à verrouiller la confidentialité de vos comptes Facebook, Instagram, Snapchat ou Twitter en passant en revue les paramètres.

### Sauvegarder ses données, c'est comme nettoyer les volets : on a toujours mieux à faire, non ?

**Q C** Mais c'est essentiel ! Copiez régulièrement vos photos et documents divers sur un disque dur externe. Vous serez content de les retrouver si un pirate bloque votre ordinateur.

### Pourquoi faut-il sécuriser son réseau wifi ?

**Q C** Un réseau facile d'accès permet à un escroc d'intercepter les données qui y transitent. Rendez-vous dans l'interface de gestion de votre box (ou de votre routeur) pour modifier le mot de passe et activer le protocole de chiffrement WPA2 (ou, à défaut, WPA-AES). ◆