Club informatique menneçois
Le numérique pour tous

Newsletter

Septembre 2021 | 46

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

Denis GELIN

Les arnaques sur Internet

Les arnaques du Web se multiplient et collent désormais à l'actualité. L'épidémie de Covid-19 le démontre car, 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, de soi-disant produits miracles ou bien n'ont pas honoré les commandes. Le coronavirus crée un cocktail numérique explosif. 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. Cet article a été largement inspiré par le n° 592 du magazine Que Choisir de juin 2020.

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. 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. Du coup, les internautes, même prudents, se laissent piéger.

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 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. 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 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.

L'Afrique et l'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.

Pourtant, les résultats ne reflètent pas forcément cette détermination. Un commissaire précise : sur les 200 000 signalements qui nous parviennent tous les ans via la plateforme Pharos, 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 chan-

Les arnaques sur Internet *(suite)*

gent 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.

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 modes opératoires

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 70 % sont issus de la cybercriminalité.

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.

Lexique

 # Arnaque : escroquerie dont vous êtes victime à la suite d'une tromperie.

 # 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.

 # 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 a un autre interlocuteur connu pour obtenir vos renseignements personnels.

 # Scam : il s'agit d'un pourriel 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 : c'est 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.

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 et envoyer des campagnes de phishing à votre insu.

2 Je navigue sur internet

Quand vous consultez un site d'information ou d'e-commerce sur Internet, 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 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 di-

Les arnaques sur Internet *(suite et fin)*

versifier 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.

Utilisez les sites marchands qui affiche un numéro de téléphone où les joindre et un mode de paiement sécurisé : un petit cadenas s'affiche dans la barre de recherche au moment du paiement.

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 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.

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 anti-cancer, 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).

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.

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, 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 disparaitre dans la nature.

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, sil 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

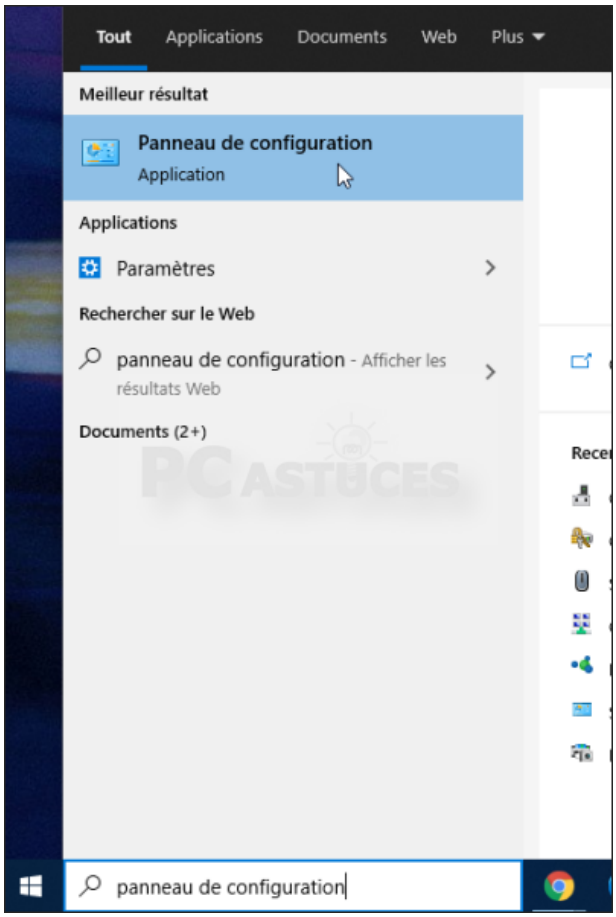
- Intemet-signalement.gouv.fr
  Pour dénoncer tout acte de cybercriminalité (escroquerie, mais aussi incitation à la haine. etc.). La plateforme d'harmonisation, d'analyse, de recoupement et d'orientation des signalements (Pharos) mènera l'enquête.
- Info Escroqueries : 0 805 805 817
  Gendarmes et policiers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

Conseils et astuces

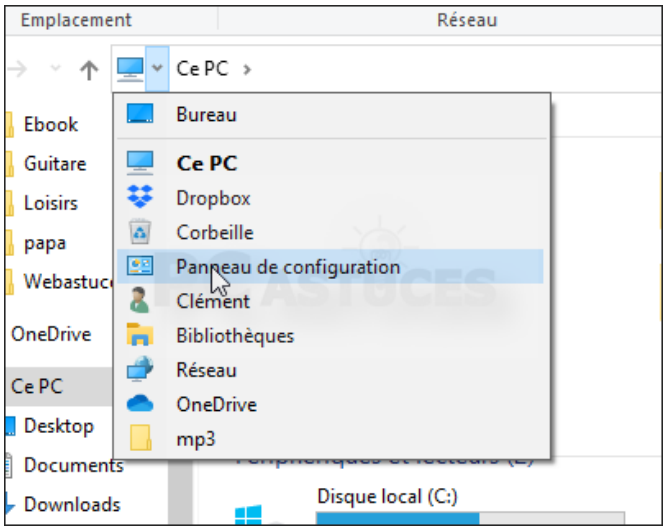
Windows 10 - Retrouver le panneau de configuration

Tous les réglages de Windows 10 ne se trouvent pas dans l'application Paramètres. Certains sont toujours dans l'ancien Panneau de configuration. Voici comment le retrouver facilement.

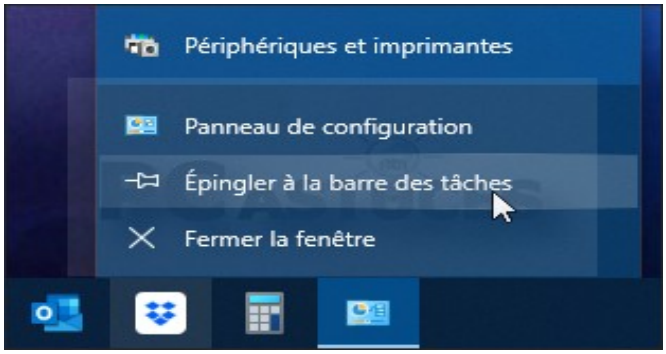
1. Tout d'abord, vous pouvez simplement saisir **Panneau de configuration** dans le champ de recherche du menu Démarrer.



2. Vous le trouverez aussi dans l'explorateur Windows. Cliquez sur la page flèche avant **Ce PC** : un menu s'affiche avec un lien vers le Panneau de configuration.



3. Une fois qu'il est ouvert, vous pouvez l'épingler à la barre des tâches. Cliquez pour cela avec le bouton droit de la souris sur son icône dans la barre des tâches puis cliquez sur **Epingler à la barre des tâches**. Désormais il vous suffit de cliquer sur cette icône pour ouvrir le Panneau de configuration.



Samedi 4 septembre
de 10 à 18 H 00

FORUM DES ASSOCIATIONS

Mennecy - Parc de Villeroy
Entre les deux orangeries

Venez nombreux sur le stand du CIM

Le club rouvre !

Votre Conseil d'Administration s'est réuni le 20 août et a décidé de rouvrir partiellement le club sous conditions sanitaires.

Malgré la 4ème vague de COVID, il a estimé que la majorité des adhérents devaient probablement être vaccinés mais qu'il convenait néanmoins de rester prudent en appliquant le protocole sanitaire que vous trouverez ci-dessous.

Le club rouvrira donc tous les mardis après-midi à partir du 7 septembre par créneaux horaires : 14 H 00 - 16 H 00, 16 H 00 - 18 H 00, sur inscription préalable auprès de Michel en indiquant le motif de la venue au club.

Des formations pourront reprendre au gré des animateurs à condition de n'accueillir que 4 personnes en plus de l'animateur.

Pour l'instant, les ateliers et les réunions thématiques continueront en visioconférence dans l'attente de jours meilleurs.

Nous espérons le plaisir de vous retrouver bientôt.

Club informatique menneçois
Le numérique pour tous

PROTOCOLE SANITAIRE
pour l'accès aux locaux du CIM
à compter du 7 septembre 2021

Le présent protocole sanitaire a été établi par le Conseil d'Administration du Club lors de sa réunion du 20 août 2021.

Les consignes qu'il contient sont applicables pour l'accès et l'utilisation des locaux du CIM. Elles sont à respecter scrupuleusement.

- port du masque obligatoire dès l'entrée dans le bâtiment des locaux du CIM,
- présentation du pass sanitaire à l'accueil du CIM lors de la première venue au club,
- feuille de présence à signer à chaque visite au club,
- respect des gestes barrières de base : pas de contacts physiques, distanciation physique de 1,5 mètre minimum entre les adhérents,
- cloisonnement des 3 salles et ouverture uniquement des portes donnant sur le couloir,
- présence de gel hydro-alcoolique à l'entrée de chaque salle et lavage des mains obligatoire à l'entrée et à la sortie des salles,
- 4 personnes + 1 animateur maximum par salle,
- nettoyage et désinfection par les utilisateurs avant et après chaque utilisation des plans de travail, claviers (recouverts de film cellophane), souris, avec les lingettes mises à disposition,
- alerter rapidement le Conseil d'Administration lorsqu'un test Covid est positif après que les locaux du Club aient été fréquentés dans les 7 jours qui précèdent le test.

Recommandation : installer l'application « TousAntiCovid » sur les Smartphones.

Lien vers le téléchargement de TousAntiCovid et son mode d'emploi

Le contenu du présent protocole évoluera en fonction de la situation sanitaire et des consignes données par la Mairie.