# LETTRE INFORMATION CYBER - SEPTEMBRE 2024

## Les Français face aux cybermenaces

Selon l'étude réalisée par Ipsos.Digital* pour Cybermalveillance.gouv.fr, 63% des sondés considèrent être suffisamment sensibilisés et informés sur les risques d'internet. 8 Français sur 10 déclarent ainsi savoir ce qu'est un spam et 6 Français sur 10 sont familiers avec les termes d'hameçonnage et de phishing. D'autres termes plus récents tels que deepfake (27%), rançongiciels (26%) ou smishing (7%) semblent moins bien connus.

De la même manière, les bonnes pratiques semblent être connues et les règles de sécurité « basiques » appliquées par une majorité, avec 85% des sondés déclarant faire des vérifications avant d'acheter ou de payer sur internet et 8 Français sur 10 qui indiquent faire régulièrement des mises à jour des appareils et applications sur leur PC.

Face à la menace, le sondage montre que les Français semblent là aussi savoir comment réagir : 50% des sondés ayant reçu un message d'hameçonnage n'y ont pas donné suite et ne sont donc pas tombés dans le piège, 25% expliquent s'être débrouillés seuls pour régler le problème potentiel.

Ainsi, malgré une perception optimiste de leur niveau de connaissance et de pratiques, 61% des personnes interrogées déclarent avoir été victimes d'au moins une cybermalveillance durant l'année écoulée.

Si 73% des Français reconnaissent avoir été confrontés à une tentative d'hameçonnage, menace principale et porte d'entrée vers d'autres cybermalveillances, 24% ont déclaré avoir été touchés par un piratage de compte en ligne (messagerie, réseaux sociaux, banque…), 20% à avoir été contactés par un faux conseiller bancaire et 11% à avoir subi un cyberharcèlement.

Loin d'être neutres, ces incidents peuvent entraîner de vrais impacts auprès de leurs victimes. 22% des victimes de cyberattaques déclarent avoir endossé une perte financière à la suite d'une attaque au cours de la dernière année ; 26% des victimes ont perdu leur accès à leurs comptes en ligne suite à un piratage et 20 % de ceux ayant eu un virus sur leurs appareils en ont perdu l'accès.

Enfin, parmi les conséquences des cybermenaces, l'impact psychologique (perte de confiance, anxiété, dépression) est non négligeable (9%). Une tendance particulièrement marquée chez les victimes de cyberharcèlement (24%).

* *Étude Ipsos.Digital réalisée pour Cybermalveillance.gouv.fr du 2 juillet au 12 août sur un échantillon de 3100 français de 18 à 75 ans*.

## Vol de données : une cyberattaque mondiale est en cours sur Windows et macOS

Une vaste campagne de vol de données a été repérée par les chercheurs d'*Insikt* de Recorded Future. L'opération, qui vise les détenteurs de cryptomonnaies et les gamers du monde entier, a été orchestrée par un gang de cybercriminels qui se fait appeler *Marko Polo*. Il s'agit d'une *« menace criminelle persistante »*, qui a été décelée lors d'une enquête entamée il y a six mois.

La campagne se distingue surtout par la diversité de ses cibles, des tactiques et de ses canaux de distribution. Les enquêteurs estiment que l'opération malveillante a **affecté des milliers d'internautes**. Selon toute vraisemblance, *« des dizaines de milliers d'appareils ont probablement été compromis à l'échelle mondiale »* et des *« données personnelles et d'entreprise sensibles »* ont été exposées. Les victimes ont par ailleurs perdu plusieurs millions de dollars au profit des hackers, probablement basés dans des pays comme la Russie, l'Ukraine, la Biélorussie ou encore la Moldavie.

Les cybercriminels choisissent apparemment leurs cibles avec soin. Pour maximiser leurs revenus, ils s'attardent sur les influenceurs du monde des cryptomonnaies, les joueurs, les développeurs de logiciels, ainsi que d'autres personnes ayant accès à des données sensibles ou à des actifs numériques. Ensuite, ils vont entrer en contact avec leurs cibles sur les réseaux sociaux.

Après avoir dupé les cibles, les pirates vont leur demander d'ouvrir un document, sous prétexte d'un emploi ou d'une collaboration alléchante. C'est évidemment là que le piège se referme. Le document contient un logiciel malveillant qui va s'immiscer sur l'ordinateur de la victime. Dans d'autres cas, les pirates relaient leur interlocuteur vers un site web factice, qui héberge le virus.

Là encore, la campagne orchestrée par *Marko Polo* se distingue par la grande diversité de son arsenal. Parmi les malwares utilisés, on trouve de redoutables infostealers, des logiciels taillés pour le vol de données. Grâce à cette panoplie de virus, le gang peut s'attaquer aux ordinateurs sous Windows et aux machines qui tournent sous macOS. Le malware Atomic Stealer est d'ailleurs capable de siphonner les mots de passe du trousseau Apple, et de s'emparer des fichiers associés aux extensions pour navigateurs, aux applications de portefeuilles crypto, et aux données des navigateurs.

Pour se protéger contre ce type d'attaque, il est recommandé de ne jamais télécharger de logiciels ou de fichiers à partir de liens partagés par des inconnus. Il est essentiel de se limiter aux sites officiels pour tous vos téléchargements. Par ailleurs, on vous recommande d'installer un antivirus sur votre ordinateur. Les virus employés par *Marko Polo* sont d'ailleurs détectés par la plupart des logiciels antivirus.

## Cyber Quiz Famille, 3ème édition : participez au jeu-concours cyber avec à la clef, de nombreux lots à gagner !

Cybermalveillance.gouv.fr organise pour la troisième année consécutive le Cyber Quiz Famille : un jeu-concours pour tester vos réflexes et apprendre les gestes essentiels en cybersécurité.

Le Cyber Quiz Famille est un **jeu-concours** destiné à faciliter le dialogue autour de la **cybersécurité**.

Grâce à des illustrations mettant en scène les membres d'une famille dans différentes situations du quotidien, parents et enfants vont pouvoir échanger sur ce sujet et ainsi apprendre à **connaître ou reconnaître les principales menaces cyber et les bonnes pratiques à retenir**.

Mots de passe, sauvegardes, mises à jour, piratage de compte… Testez vos réflexes et apprenez les gestes essentiels en cybersécurité, avec à la clef de **nombreux lots à gagner** (billets pour parcs d'attraction, spectacles et cinéma, etc.).

Le Cyber Quiz Famille sera disponible ici à partir du 1er octobre 2024. En attendant, n'hésitez pas à réviser vos connaissances grâce au Cyber Guide Famille.

**JOUER**

Pour mettre toutes les chances de votre côté, Cybermalveillance.gouv.fr vous propose de **réviser vos connaissances** en cybersécurité grâce au **Cyber Guide Famille**, un guide pédagogique spécialement dédié aux parents et aux enfants.

**LA SECURITE EST L'AFFAIRE DE TOUS.**