

Microsoft, Cybermalveillance.gouv.fr et la section de lutte contre la cybercriminalité du Parquet de Paris appellent à se mobiliser contre les arnaques au faux support technique

L'arnaque au faux support technique est la 3^e menace cyber pour les particuliers, selon le dernier rapport d'activité de [Cybermalveillance.gouv.fr](https://cybermalveillance.gouv.fr). Microsoft figure parmi les marques les plus usurpées par les escrocs. Cette tendance s'installe au fil des ans - avec des modes opératoires plus agressifs apparus en 2022, comme le fait de s'attaquer aux comptes bancaires des victimes. Si le préjudice financier pour les victimes était de quelques centaines d'euros auparavant, il peut s'élever aujourd'hui à plusieurs milliers, voire dizaines de milliers d'euros, toujours selon Cybermalveillance.gouv.fr.

Qu'est-ce que l'arnaque au faux support technique et qui est concerné ?

L'arnaque au faux support technique consiste à effrayer les victimes en indiquant un problème technique grave (virus) afin de les pousser à payer pour un dépannage informatique fictif. La technique utilisée par les cybercriminels est l'apparition d'un message d'alerte anxiogène qui semble bloquer l'ordinateur. Les escrocs peuvent également débiter un contact en affichant de faux messages d'erreur sur les sites web que la victime visite, indiquant des numéros de support technique et invitant à les appeler.

Lorsqu'une victime échange avec un escroc, ce dernier propose des solutions fictives de dépannage en demandant un règlement unique ou en proposant un abonnement à un faux service.

L'arnaque au faux support s'est considérablement répandue ces dernières années et occupe la 3^e place du classement des menaces cyber les plus fréquentes pour les particuliers, selon le dernier rapport d'activité de Cybermalveillance.gouv.fr.

« Nous voyons l'arnaque au faux support technique se répandre au fil des ans et les techniques deviennent de plus en plus agressives et lucratives. Les cybercriminels peuvent aller jusqu'à prendre le contrôle des comptes bancaires en ligne d'une victime. Alors que le préjudice financier pour les victimes s'élevait auparavant à plusieurs centaines d'euros, il peut atteindre jusqu'à plusieurs milliers, voire dizaines de milliers d'euros aujourd'hui. », explique Jérôme Notin, Directeur Général de Cybermalveillance.gouv.fr

En 2024, Cybermalveillance.gouv.fr a recensé 136 500 consultations d'articles et 13 500 recherches d'assistance en lien avec l'arnaque au faux support technique.

Face à ce fléau, **Cybermalveillance.gouv.fr, Microsoft et la section de lutte contre la cybercriminalité du Parquet de Paris partagent leurs recommandations avec le plus grand nombre.**

En 2023, 585 plaintes ont été transmises à la section de lutte contre la cybercriminalité, portant parfois sur des faits plus anciens car elles ont transité par les tribunaux d'autres ressorts. Le préjudice total des faits commis en 2023 est évalué à 374 000 euros, sans compter les montants bien plus importants qui ont fait l'objet de tentatives mais ont été bloqués par les banques.

Le Parquet de Paris encourage les victimes à lui adresser directement des lettres-plaintes, afin qu'elles soient prises en compte plus rapidement et donc avec de plus grandes chances de succès. Cybermalveillance.gouv.fr a mis en ligne des recommandations afin que ces lettres-plaintes contiennent toutes les informations utiles à un traitement immédiatement efficace.

« Ce qu'on constate, c'est moins d'attaques portant sur de petits préjudices, mais une sophistication des processus, qui amènent les escrocs à augmenter le montant prélevé à chaque victime individuellement. Paradoxalement, ils jouent sur la peur de perdre ses données personnelles et de se faire pirater. On peut tous devenir victime. C'est pourquoi il est absolument nécessaire de mettre en garde contre ce mode opératoire spécifique. » souligne Johanna Brousse, cheffe de la section de lutte contre la cybercriminalité du Parquet de Paris

Les arnaques aux faux supports techniques ne discriminent personne, quels que soient l'âge ou le milieu social. Personne n'est à l'abri et certaines populations peuvent être plus vulnérables lorsqu'elles sont confrontées à ces arnaques.

En effet, selon une étude Microsoft réalisée par Ifop, seuls 16 % des seniors déclarent connaître précisément les démarches à suivre en cas d'arnaques en ligne. Microsoft, Cybermalveillance.gouv.fr et la section de lutte contre la cybercriminalité du Parquet de Paris, publient une fiche qui leur est dédié et dans laquelle ils peuvent retrouver toutes les bonnes pratiques et tous les conseils. Et parce que 39 % des seniors en France se tournent vers un membre de leur famille en cas de problème technique, une seconde fiche est publiée ce jour pour aider les proches à les accompagner.

Microsoft, l'une des marques les plus usurpées par les escrocs

« Appelez l'assistance Windows » : voici le genre de message qu'une victime peut recevoir dans une fenêtre qui s'ouvre sur son ordinateur. Les cyberattaquants peuvent également appeler directement les victimes ou leur envoyer un e-mail.

« Parce que nos technologies sont très utilisées à travers le monde, Microsoft et notre environnement Windows sont régulièrement utilisés par les cyberattaquants qui pratiquent l'arnaque au faux support technique. La première chose à savoir : Microsoft ne vous contactera jamais directement par téléphone sans que vous ne nous ayez sollicités. », déclare Philippe Limantour, Directeur technologique et cybersécurité de Microsoft France.

Depuis plusieurs années déjà, Microsoft alerte sur le phénomène et partage avec tous ses conseils et bonnes pratiques, qui sont les suivants :

- Microsoft ne vous enverra jamais d'e-mails ni ne vous appellera de manière non sollicitée pour vous demander des informations financières ou personnelles ou pour offrir un support technique afin de réparer votre ordinateur. Si vous ne nous l'avez pas demandé, nous ne vous appellerons pas pour offrir un support.
- Si un message d'erreur ou une fenêtre contextuelle s'affiche comportant un numéro de téléphone, ne l'appellez pas. Les messages d'erreur et d'avertissement de Microsoft n'incluent jamais de numéro de téléphone.
- Microsoft ne vous demandera jamais de payer le support sous la forme de cryptomonnaie comme Bitcoin, ou de cartes cadeaux.
- Téléchargez des logiciels uniquement à partir de sites web officiels de partenaires Microsoft ou du Microsoft Store. Méfiez-vous du téléchargement de logiciels à partir de sites tiers, car certains d'entre eux peuvent avoir été modifiés à l'insu de l'auteur pour regrouper des logiciels malveillants et d'autres menaces.