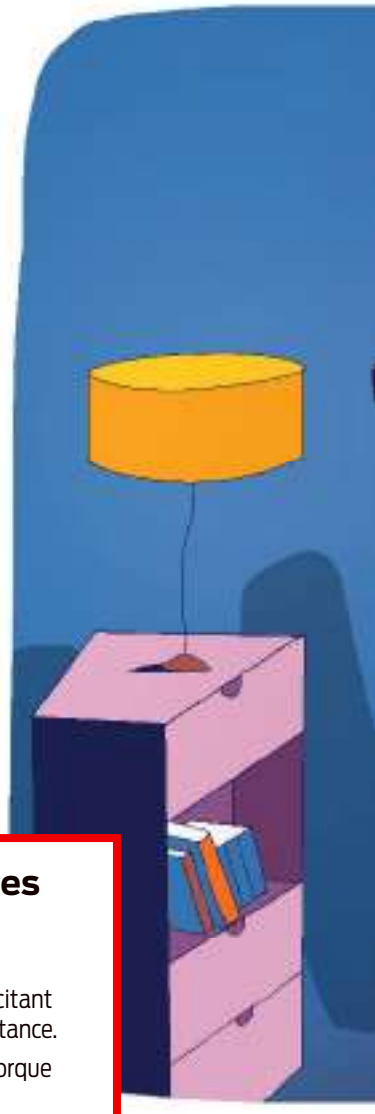
ARNAQUE AU FAUX SUPPORT TECHNIQUE

Ne payez pas !



Un message inquiétant s'affiche soudainement sur l'écran de votre ordinateur. Il vous demande d'appeler de toute urgence un numéro de téléphone. Pas de panique. La situation n'est pas aussi grave que l'on cherche à vous le faire croire.

— Par **CYRIL BROSSET**

Laurence travaillait sur son ordinateur quand, tout à coup, les pages qu'elle consultait se sont figées, plusieurs fenêtres se sont ouvertes intempestivement et un message inquiétant est apparu à l'écran. *« Il était écrit,* raconte-t-elle, *que mon PC avait été infecté par des programmes malveillants. Je devais composer de toute urgence un numéro de téléphone qui semblait correspondre à celui du service technique de Microsoft. Il était également précisé qu'il ne fallait surtout pas que j'éteigne la machine, faute de quoi toutes mes données seraient perdues. J'ai un peu paniqué, alors j'ai appelé. Au bout du fil, une personne m'a confirmé que l'appareil était vérolé, mais elle m'a dit qu'elle remettrait tout en ordre si je déboursais 240 €. Comme j'avais absolument besoin de mon ordinateur le jour même, j'ai payé. »* Une fois le virement effectué, le réparateur en a pris le contrôle à distance et a procédé à une série de manipulations. Le PC de Laurence s'est ensuite remis à fonctionner normalement.

Monique a vu la même annonce s'afficher sur son écran d'ordinateur alors qu'elle cherchait à se connecter au site de sa Caisse d'allocations familiales. Elle était accompagnée d'une sirène stridente qui n'a cessé de retentir qu'une fois le son des enceintes coupé. *« Comme je ne pouvais plus rien faire sur mon PC, j'ai téléphoné. Une personne charmante a pris la main sur mon ordinateur et, après avoir réalisé un diagnostic, m'a déclaré qu'il était infecté. Elle m'a proposé un dépannage à 90 €, auquel s'ajoutait un contrat de maintenance à vie de 400 €, que j'ai réglé par le biais d'un porte-monnaie électronique. »*

Les pirates font tout pour convaincre leurs victimes qu'elles ont affaire à de vrais services d'assistance en ligne

Les trois stades de l'arnaque

1. **L'ordinateur est bloqué** et un message apparaît incitant à composer un numéro d'assistance.
2. **Un faux réparateur** extorque de l'argent à sa victime sous prétexte de réparer le PC.
3. **Des données sensibles** sont volées et utilisées.

Laurence et Monique ont toutes les deux été victimes de l'arnaque dite « au faux support technique ». Le message qu'elles ont reçu n'était pas une véritable alerte et ne provenait nullement de Microsoft. Qui plus est, leur ordinateur n'a jamais été infecté ni bloqué. Il leur aurait suffi de le redémarrer pour résoudre le problème ! Quant au « professionnel » qu'elles ont eu en ligne, il ne s'agissait pas d'un réparateur mais d'un cybercriminel, dont l'unique objectif était de leur soutirer de l'argent.

Des méthodes de plus en plus efficaces

Les deux femmes sont loin d'être les seules à avoir été confrontées à ce genre d'escroquerie. *« Il ne s'écoule pas une semaine sans qu'un client me contacte parce qu'il a vu apparaître ce type de message sur son écran,* se désole Jordan Cartron, un réparateur indépendant installé à Compiègne, dans l'Oise. *Beaucoup d'entre eux ont composé le numéro indiqué et versé la somme demandée, qui oscille le plus souvent entre 150 et 500 €, mais qui peut atteindre*

RÉGIS FALLER

1 000 € dans certains cas.» « Depuis plusieurs années, cette arnaque constitue l'un des sujets les plus consultés sur Cybermalveillance.gouv.fr, la plateforme gouvernementale de lutte contre les fraudes en ligne, assure Jérôme Notin, son directeur général. *Les victimes sont nombreuses et les montants extorqués, très importants. Les escrocs, qui se sont professionnalisés et travaillent désormais par équipes à partir de plusieurs pays, se montrent de plus en plus efficaces.»*

Leur méthode ? Un premier groupe est chargé de diffuser les faux messages. Pour ce faire, il passe par des régies publicitaires, dont il contourne les systèmes de contrôle, afin que soient publiés des encarts vérolés intégrant un code informatique frauduleux sur leurs sites partenaires. Dès qu'un internaute se rend sur une page où figure l'une de ces pubs, le code s'active et l'annonce menaçante apparaît. Les plateformes les moins scrupuleuses, comme celles de streaming, de jeux ou encore de recettes de cuisine, sont les plus susceptibles d'être corrompues, mais aucune n'est exempte de risques. Une deuxième équipe répond aux victimes. *« Les aigrefins ont recours à des centres d'appels installés dans des pays francophones et demandent aux téléopérateurs de se faire passer pour de vrais techniciens,* explique Jérôme Notin. *Le discours est tellement bien rodé et les opérations si réalistes que la plupart des particuliers se font avoir et finissent par verser la somme réclamée. Certains ne se rendent même pas compte qu'ils ont été escroqués tant le subterfuge est redoutable.»* Jordan Cartron se souvient : *« J'ai déjà assisté à des interventions de ces pseudo-réparateurs. Ils passent leur temps à ouvrir des fenêtres, à modifier des paramètres et à fermer des boîtes de dialogue. Parfois, ils installent un antivirus gratuit ou une suite de sécurité payante qu'ils activent avec une licence piratée. En réalité, tout est faux. Ces manipulations ne servent absolument à rien, et pour cause, l'ordinateur n'a jamais eu le moindre problème.»*

Gare à vos données personnelles

Si les personnes âgées peu à l'aise avec l'informatique représentent les proies les plus faciles, n'importe qui peut, un jour ou l'autre, tomber dans le panneau, tant l'arnaque est bien ficelée. D'autant plus que les cybercriminels n'attendent pas que leurs cibles consultent un site infecté. Ils n'hésitent plus à envoyer massivement des courriels frauduleux (phishing) dans lesquels ils incitent les destinataires, sous un prétexte fallacieux (visionner une vidéo géniale ou réaliser une excellente affaire, par exemple), à cliquer sur un lien qui les redirige vers une page vérolée. Certains escrocs ont même expédié une fausse newsletter imitant celle d'une marque connue dans le but qu'un maximum >>>

>>> d'internautes cliquent sur le lien de désinscription, déclenchant l'affichage du fameux message. Le discours des prétendus réparateurs aussi ne cesse de s'affiner avec le temps. Désormais, il n'est pas rare que les téléopérateurs lancent sur les PC de leurs victimes un soi-disant outil de diagnostic qui repère des infections imaginaires, puis fassent parvenir à ces dernières une facture (fausse, évidemment !) à la fin de leur intervention.

Les margoulins ne se contentent plus d'obliger à payer une pseudo-prestation. Dès lors qu'ils ont pris la main sur les ordinateurs, ils peuvent en profiter pour subtiliser toutes sortes de données sensibles susceptibles de leur rapporter gros. Identifiants, mots de passe, justificatifs de domicile, scans de papiers d'identité… tout ce qu'il est possible de revendre sur le marché parallèle est bon à collecter. « *Nous avons déjà eu un cas où un faux réparateur avait recopié un fichier nommé Motsdepasse.txt qui se trouvait sur la machine d'un particulier. Ce dernier y avait imprudemment recensé tous ses codes secrets, dont ceux de sa banque. Résultat : à peine quelques heures plus tard, 16 000 € disparaissaient de ses comptes bancaires,* déplore Jérôme Notin. *Sans parler des escrocs qui souscrivent des emprunts en utilisant des codes bancaires volés ou créent de faux papiers d'identité grâce à des documents administratifs récupérés auprès de victimes d'arnaque au faux support technique.* » Il arrive également que des cybercriminels cachent dans les PC un logiciel « mouchard » leur permettant d'en reprendre le contrôle ultérieurement, voire recontactent leurs victimes plusieurs mois plus tard et leur réclament à nouveau de l'argent en alléguant une opération de maintenance.

Quand un escroc prend le contrôle d'un PC, il peut aussi y cacher un « mouchard »

Des aigrefins difficiles à appréhender

Si les services de police et de gendarmerie ne restent pas les bras croisés face à ces agissements, malheureusement leur bilan s'avère maigre. Le fait que les escrocs agissent de l'étranger et effacent de plus en plus souvent toute trace de leur intervention sur les ordinateurs de leurs proies ne facilite pas la tâche des forces de l'ordre. Sans compter que beaucoup de victimes ne portent pas plainte. Soit elles estiment que les chances de revoir leur argent sont quasiment inexistantes (ce qui n'est pas complètement faux !), soit elles n'ont pas conscience d'avoir été arnaquées, pensant avoir bénéficié d'une prestation réelle.

Quelques coups de filet ont toutefois été réalisés. En janvier 2019, trois chefs d'entreprise ont été arrêtés dans le département du Rhône. Ils étaient suspectés d'avoir extorqué quelque 2 millions d'euros à 8 000 personnes ! Actuellement mis en examen et placé sous contrôle judiciaire, le trio pourrait être présenté à la justice dans les mois qui viennent. Et, selon nos dernières informations, d'autres investigations seraient en cours. ◆

PRATIQUE
Savoir comment réagir

Voici quelques conseils pour déjouer les arnaques au faux support technique. Ils vous permettront d'avoir les bons réflexes en fonction de la situation dans laquelle vous vous trouverez peut-être un jour.

Un message alarmant apparaît à l'écran

 # Essayez de fermer la page. Si c'est impossible, appuyez simultanément sur les touches ctlr, alt et suppr de votre clavier. Cliquez ensuite sur « Gestionnaire de tâches », puis sur votre navigateur (Edge, Firefox, Chrome…) et sur « Fin de tâche ». Relancez le navigateur sans restaurer la session. **# Éteignez l'ordinateur** en appuyant longuement sur l'interrupteur si rien n'y fait. Vous ne perdrez pas vos données.

Vous avez appelé le numéro et versé la somme demandée

 # Portez plainte auprès de la police ou de la gendarmerie. **# Modifiez vos mots de passe,** notamment ceux de vos comptes bancaires et de votre messagerie, s'il existe un risque que des données personnelles aient été volées. **# Demandez à votre banque d'annuler la transaction** ou de vous rembourser les sommes versées en cas de paiement par carte. Mais sachez que cette démarche peut ne pas aboutir si l'établissement estime qu'il y a eu négligence de votre part. **# Faites examiner votre ordinateur** par un vrai réparateur (comptez une cinquantaine d'euros l'intervention), lorsque vous avez autorisé l'escroc à prendre la main dessus. Vous trouverez plus d'informations sur le site Cybermalveillance.gouv.fr, notamment une fiche récapitulative à présenter à l'agent qui prendra votre plainte.

Le reste du temps

 # N'enregistrez pas identifiants et mots de passe sensibles sur votre ordinateur ou sur les sites eux-mêmes. Notez-les plutôt sur papier. **# Indiquez votre numéro de téléphone** quand on vous le demande pour sécuriser vos connexions. **# Ne cliquez pas sur les liens** présents dans les e-mails douteux.