[Transcript] Monde Numérique - Actu Technologies / [EDITO] Cyberarnaque : pensez-y AVANT que ça arrive !

Peut-être avez-vous déjà reçu ce genre de coups de fil ? Quelqu'un qui vous dit « Allô, bonjour, vous êtes bien Monsieur Machin » et votre numéro de compte bancaire est bien le « tac, tac, tac, tac ». Ah désolé, vous avez été victime d'une fraude, heureusement je vais vous aider à régler le problème. Évidemment, cet appel est faux, c'est un escro, un cyber-escro, un appel ou bien des SMS pour, soit disons, une commande en cours, une amende, un payé, etc. Il y a vraiment de quoi être stupéfait en ce moment, face à la multiplication des cyber-arnaques et par l'imagination sans limite des cyber-escros. Des pirates qui sont désormais de véritables professionnels, ils achètent au marché noir sur le darknet des fichiers qui proviennent de divers piratages et qui contiennent souvent des informations très précises à votre sujet. C'est comme ça qu'ensuite ils peuvent cibler leurs attaques et faire croire qu'ils vous connaissent, se faire passer pour votre conseiller bancaire, etc. Dans la plupart des cas, cependant, ils ne possèdent pas votre mot de passe, vos mots de passe permettant de véritablement vous soutirer de l'argent ou d'aller plus loin et c'est pour cela qu'ils vous contactent, ils essayent par tous les moyens de vous soutirer des informations. Ce sont de véritables maîtres de la manipulation mentale et on risque tous, un jour, de tomber dans les mailles du filet. Parce qu'un jour on est fatigué, stressé, contrarié, parce qu'il y a quelque chose de réel qui vient de se passer. Par exemple on a changé de banque ou on a vraiment eu un PV de circulation. Alors face à tout ça, il faut vraiment être de plus en plus prudent. Mais c'est plus facile à dire qu'à faire. Ce mois-ci a lieu le cyber mois, le mois de la cyber sécurité organisée par différentes instances européennes. C'est très officiel, c'est pour sensibiliser tout le monde à ces questions là. Il y a quelques jours, j'ai animé l'événement de lancement de ce cyber mois. J'en ai retenu quelques trucs que je vais vous livrer tout de suite, des trucs pour essayer de survivre dans ce monde connecté de plus en plus dangereux. Règle numéro 1, ne divulguer jamais d'informations sensibles comme un code secret ou un mot de passe à quelqu'un qui vous le demande par téléphone, par mail, par sms ou via les réseaux sociaux. Même si vous avez l'impression que c'est quelqu'un qui est fiable, la plupart du temps c'est un escrore, même votre banque n'a pas à connaître votre code secret de carte bancaire. Deuxièmement, ne cliquer jamais sur un lien si vous recevez un message, mais allez vous-même sur le site vers lequel on veut vous emmener, par exemple votre banque ou bien la poste ou autre, s'il s'agit d'une livraison, la CAF, le site en taille pour le paiement des amendes, etc. Si c'est vous qui faites la démarche de vous connecter pour en savoir plus, vous avez beaucoup moins de chance de vous retrouver sur un faux site web qui va vous soutirer des données. Troisièmement, c'est vraiment la base, utiliser toujours des mots de passe forts, des mots de passe complexes avec des chiffres et des laters, oui je sais, c'est embêtant à retenir, c'est pour ça qu'il faut utiliser un gestionnaire de mots de passe, ou au pire un petit carnet soigneusement tenu à jour. On a l'impression que ça complique un peu les choses, c'est pas faux mais au moins ça vous sécurise. Sinon c'est un peu comme si vous laissiez la porte de votre domicile sans verrou ou sans clé, est-ce que vous feriez ça dans le monde réel ? Pas du tout, et bien c'est pareil en informatique. Quatrième point, utiliser toujours l'authentification en deux étapes, vous savez l'envoi d'une

notification sur mobile en plus du mot de passe dès lors qu'il s'agit d'un compte important comme par exemple un compte bancaire ou même pour votre compte mail, comme ça à chaque fois que vous allez essayer de vous connecter par exemple sur un autre ordinateur, on vous demandera de vous authentifier. C'est casse-pied mais c'est vraiment une sécurité indispensable. Cinquième point, faites des sauvegardes de vos données précieuses, mais attention des sauvegardes hors ligne que vous
allez conserver sur des disques durs déconnectés de votre réseau, de votre wifi, de votre ordinateur principal. Et oui parce que sinon si vous utilisez un disque dur ou une clé USB toujours connectée sur votre ordinateur, et bien en cas d'attaque, c'est un support qui se retrouvera corrompu comme l'ordinateur lui-même. Bon, impossible de lister tous les cas de figure et tous les scénarios de cyberattaque, il y en a de nouveau quasiment tous les jours. Ce qu'il faut retenir c'est qu'on n'est plus à l'époque où on courait simplement le risque de faire entrer un virus sur son ordinateur. Aujourd'hui les pirates viennent taper à votre porte, ils vous appellent au téléphone, ils vous font croire des tas de choses, il faut donc être prudent et faire preuve de bon sens, voire même de méfiance. Si malheureusement vous avez un problème, par exemple un rençongiciel qui bloque votre ordinateur, surtout n'éteignez pas votre ordi, car ça permettra de conserver des traces et peut-être un mince espoir de récupérer des données. Ce qu'il faut faire c'est couper la connexion internet, donc par exemple vous éteignez votre box wifi. Enfin informez-vous un minimum sur
tout ce qui touche à la cyber sécurité et à la cyber malveillance. Alors attention, informez-vous avec des vrais infos, pas des fake news transmises par vos amis via whatsapp. Et puis si vous avez un doute sur une sollicitation, un truc très simple, posez la question à votre moteur de recherche préféré, vous tapez par exemple SMS, amendes etc. Il a sûrement la réponse car d'autres personnes avant vous se sont fait piéger et vous découvrirez vite s'il s'agit d'une arnaque. Enfin en cas de problème faites à peine un expert mais un vrai pas l'épicier du coin qui n'y connaît probablement rien et qui risquera d'aggraver les choses. Et voilà malheureusement en informatique lorsque le mal est fait, il faut bien le dire, on n'a plus que ses yeux pour pleurer la plupart du temps. Il est très difficile de récupérer ces données sauf si on a fait des sauvegarde. Alors on le dit et on le redit, il faut penser à tout cela avant que cela vous arrive. Bon on ne peut que recommander d'aller faire un tour sur le site officiel cybermalveillance.gov.fr qui regorge de conseils qui peut éventuellement vous aider lorsqu'il vous avait un problème, c'est à la fois pour les particuliers et pour les professionnels. C'est vraiment l'essayant d'avoir une hygiène informatique parfaite que vous éviterez de vous retrouver un jour dans une situation très compliquée.