Table of contents

Les menaces en lignes

Avec l'essor du numérique, des réseaux sociaux, les arnaques en ligne se sont fortement développées et avec l'intelligence artificielle, elles deviennent de plus en plus sophistiquées.
Au travers de cette page, je vais essayer de vous aider à démystifier cela.

Les arnaques en ligne peuvent être de différents types. On parle entre-autre de

- Phishing ou hameçonnage (+ sms + appel)
- Piratage des comptes en ligne
- Arnaque au faux support technique
- Violation de données personnelles
- Rançongiciels ou ransomwares
- Spams
- Attaques en déni de service (DDoS)
- Faux ordres de virement
- Virus
- Arnaque aux sentiments
- Sextorsion
- ...

Mais avant d'aller plus loin, définissions un peu ces différents types d'arnaque

L’hameçonnage ou phishing

L’hameçonnage ou phishing constitue la principale cybermalveillance rencontrée, tous publics confondus. Cette technique d’attaque consiste à envoyer un courriel ou SMS à la victime en usurpant l’identité d’un tiers (une entreprise, une administration, etc.), pour l’inciter à réaliser une action comme communiquer des informations personnelles, professionnelles ou bancaires, ou encore ouvrir un lien ou une pièce jointe infectée par un virus. Assez simple, peu onéreuse et très rentable, cette technique d’attaque est devenue le principal vecteur à l’origine de tout un panel de cybermalveillances : piratage de compte, débits bancaires frauduleux, usurpation d’identité… Parmi les phishing les plus fréquents on peut citer : les faux messages d’infraction pédopornographique, les arnaques au faux support technique, les sollicitations concernant le compte personnel formation (CPF) ou encore les messages d’escroquerie à la livraison de colis.

À noter la tendance forte du développement de l’hameçonnage par SMS, ou smishing en anglais, les cybercriminels profitant de la plus grande difficulté à identifier un SMS frauduleux sur un téléphone.

Piratage des comptes en ligne

Le piratage de compte en ligne représente la seconde menace la plus rencontrée, tant par les particuliers que les professionnels. Si le piratage des comptes bancaires en ligne et des comptes de réseaux sociaux apparaît comme une cible de choix pour les cybercriminels, l'intérêt des attaquants s'oriente davantage vers les comptes de messagerie. Contenant une grande quantité d'informations, les messageries représentent une mine d'or pour les cybercriminels qui ont bien compris qu'en prenant le contrôle de la messagerie d'une victime, ils pouvaient prendre le contrôle de presque toute sa vie numérique. D'autant plus que dans le domaine de la cybersécurité, la messagerie est généralement le point central permettant la réinitialisation du mot de passe de tous les autres comptes en ligne de la victime. Les principales causes identifiées de ces piratages sont l'utilisation de mots de passe faciles à deviner, la réutilisation du même mot de passe sur de multiples comptes dont l'un a pu déjà être piraté, l'hameçonnage et l'absence d'authentification renforcée.

Arnaque au faux support technique

L'arnaque au faux support technique (ou fraude à la réparation informatique) arrive en troisième position. Cette forme de cybermalveillance consiste principalement à bloquer l'ordinateur de la victime par l'apparition d'un message évoquant un incident de cybersécurité pour l'effrayer afin de l'inciter à rappeler un prétendu support technique officiel et lui faire payer un pseudo-dépannage. Cette cybermenace cible essentiellement les seniors les moins aguerris au numérique ou les professionnels qui ne disposent pas de supports informatiques de proximité et qui sont donc plus facilement susceptibles de tomber dans ce piège.

L'arnaque au faux support technique voit ses modes opératoires évoluer sans cesse, aussi bien dans la diversification des méthodes d'approche que dans les conséquences pour les victimes : approches téléphoniques, notifications de réseaux sociaux contenant des liens malveillants qui déclenchent l'apparition du message d'alerte frauduleux, etc. Consécutivement à cette cybermalveillance, de nombreux cas de virements bancaires frauduleux ou de piratage de comptes en ligne des victimes d'arnaque au faux support technique sont, par ailleurs, rapportés. En effet, lors de la prise en main de l'appareil de la victime, le faux réparateur dérobe de plus en plus fréquemment des identifiants et mots de passe dont il fera par la suite un usage frauduleux.

Violation de données personnelles

La violation de données personnelles est la cinquième cybermalveillance la plus fréquemment rencontrée, l'année 2021 ayant été marquée par de nombreux incidents de cybersécurité qui ont conduit à des fuites de données personnelles, et notamment de données médicales. Pour rappel, une donnée personnelle est une information permettant d'identifier directement ou indirectement une personne. Il peut s'agir d'un nom, d'une photo, d'une adresse postale ou de messagerie (mail), d'un numéro de téléphone, d'une adresse IP. La violation de données personnelles désigne ainsi la destruction, la perte, la modification ou la diffusion non autorisée de ces données. Qu'elle soit d'origine accidentelle ou malveillante, une violation de données personnelles peut avoir des conséquences de cybersécurité importantes pour le particulier ou l'organisation qui en est victime : atteinte à la réputation et/ou à la vie privée, préjudice financier, tentative d'usurpation d'identité, tentative d'hameçonnage, etc.

Rançongiciels ou ransomwares

L'attaque par rançongiciel ou ransomware en anglais, qui désigne une cyberattaque qui bloque l'accès à l'appareil ou à des fichiers en les chiffrant et qui réclame à la victime le paiement d'une rançon pour en obtenir de nouveau l'accès, demeure une des principales menaces à la cybersécurité traitées par la plateforme, avec toutefois de fortes variations en fonction des publics. Les chiffres démontrent en effet un intérêt décroissant des cybercriminels pour les particuliers, jugés sans doute moins solvables, tandis que les rançongiciels constituent la première cybermenace chez les professionnels, avec une hausse de plus de 95 % en 2021. Si les cybercriminels n'ont pas abandonné le ciblage des collectivités, les statistiques prouvent qu'ils visent en priorité les entreprises, sans doute parce qu'elles seraient plus enclines à payer les rançons demandées au regard des impacts économiques et réputationnels de ce type de cyberattaque pour leur activité. Cette tendance devrait malheureusement continuer à s'accentuer.

Spams

Le spam électronique ou spam téléphonique désigne une communication non sollicitée à des fins publicitaires, commerciales ou malveillantes. Il peut prendre différentes formes : SMS, MMS, email, messagerie instantanée, réseaux sociaux ou appel téléphonique. Dans bien des cas, il s'agit de prospection commerciale mais le spam peut également revêtir un caractère malveillant – incitation à rappeler un numéro surtaxé, envoyer un SMS à un numéro payant… – ou porter atteinte à la cybersécurité de la victime : tentatives d'hameçonnage ou phishing pour dérober des données personnelles et/ou confidentielles. À titre d'exemple, vous avez reçu un appel téléphonique d'une personne qui souhaite vous faire bénéficier d'une formation financée par votre Compte Personnel de Formation (CPF) ? Il peut s'agir de prospection commerciale, mais faites preuve de vigilance, car cela peut parfois déboucher sur une escroquerie ou le piratage de votre compte.

Attaques en déni de service [PRO]

Cinquième catégorie des demandes d'assistance la plus recherchée par les entreprises et associations, l'attaque en déni de service ou en déni de service distribué (DDoS pour Distributed Denial of Service en anglais) vise à rendre inaccessible un serveur par l'envoi de multiples requêtes jusqu'à le saturer, ou à exploiter une faille de cybersécurité afin de provoquer une panne ou un fonctionnement fortement dégradé du service. Durant l'attaque, le site ou service n'est plus utilisable, au moins temporairement, ou difficilement, ce qui peut entraîner des pertes directes de revenus pour les sites marchands et des pertes de productivité. Souvent visible, l'attaque porte directement atteinte à l'image et donc à la crédibilité et la réputation du propriétaire du site, car elle est perçue par les publics comme une défaillance de sécurité.

Faux ordres de virement [PRO]

Sixième demande d'assistance la plus recherchée par les entreprises et associations, le faux ordre de virement (FOVI) consiste à tromper la victime pour la pousser à réaliser un virement de fonds non planifié sur un compte détenu par le cybercriminel. Les FOVI peuvent présenter des modes opératoires différents : la demande est parfois présentée comme émanant d'un dirigeant avec un caractère « urgent et confidentiel ». On parle alors « d'arnaque au Président ». Une autre variante consiste à usurper l'identité d'un fournisseur pour communiquer de nouvelles coordonnées bancaires (changement de RIB) sur lesquelles il faut effectuer un règlement. Une autre version consiste à usurper l'identité d'un salarié de l'organisation pour demander le changement des coordonnées bancaires où virer son salaire. Dans la majorité des cas, cette fraude à la cybersécurité fait suite au piratage et à l'utilisation de la messagerie de la personne ou entité usurpée.

Virus

Dernier acte de cybermalveillance le plus rencontré par les publics, le virus est un programme informatique malveillant dont l'objectif est de s'implanter sur un système informatique (ordinateur, appareil mobile, serveur, etc) pour perturber son fonctionnement normal et entraver la cybersécurité de son propriétaire à son insu. Il existe différents types de virus comme le rançongiciel, le cheval de Troie, le logiciel espion… Touchant aussi bien les particuliers que les professionnels, ils peuvent s'infiltrer dans un système informatique par l'ouverture d'un message (mail, MMS, chat), d'une pièce jointe ou d'un clic sur un lien frauduleux. Il peut également s'introduire en naviguant sur un site malveillant, en s'installant dans un appareil ou un logiciel non mis à jour, par l'absence d'utilisation d'un antivirus, l'installation d'une application piratée, etc. Les symptômes d'une infection par un virus peuvent se manifester par une alerte de l'antivirus, un ralentissement ou un blocage anormal de l'appareil, des fenêtres ou des messages d'erreur qui s'affichent sans raison, la modification de logiciels ou programmes, etc.

Arnaque aux sentiments

Les arnaques aux sentiments, aussi appelées escroqueries sentimentales, ciblent de plus en plus de victimes en ligne. En effet, avec la montée en puissance des réseaux sociaux et des sites de rencontres, les arnaques aux sentiments se multiplient, touchant des milliers de personnes chaque année. Ces escroqueries jouent sur les émotions et la vulnérabilité de la victime pour lui soutirer de l'argent ou des informations sensibles. En général, l'escroc évite tout contact physique afin de ne pas être identifié, trouvant toujours des excuses pour éviter la rencontre ou même être contacter par téléphone.

Mode opératoire

Mais comment font-ils ? Allez-vous demander ?

Les deux vidéos suivantes vont vous montrer comment tout cela peut se passer. Dans la première vidéo, vous allez vous glisser dans la peau d'un hacker, tandis que dans la deuxième vidéo vous serez dans la peau de la victime.

Comment se protéger ?

1. Sensibilisation et information

- Se tenir informé des types d’arnaques les plus courants (phishing, faux sites, offres trop alléchantes, etc.).
- Participer à des campagnes de sensibilisation et suivre des formations sur la sécurité numérique.

2. Créez des mots de passe complexes, comprenant des lettres majuscules et minuscules, des chiffres et des caractères spéciaux. Il est recommandé de ne pas utiliser le même mot de passe sur différents sites et de privilégier l’activation de l’authentification à deux facteurs lorsque cela est possible.
    1. J'a!Oubli3m0nM0td3p@ss3
    2. M0nCh!3n3stl3plusgent!l
3. Utilisez un gestionnaire de mot de passe. Celui-ci vous permettra de définir des mots de passe complexe de manière aléatoire et différents pour tous vos sites.
4. Vérifier l’authenticité des sites et des communications
5. Avant de saisir des informations personnelles ou bancaires, assurez-vous que le site est sécurisé (présence du cadenas et de « https » dans la barre d’adresse). Méfiez-vous également des courriels ou messages suspects demandant des informations sensibles et vérifiez toujours l’expéditeur.
6. Garder ses appareils et logiciels à jour. Installez régulièrement les mises à jour de sécurité de vos systèmes d’exploitation, navigateurs et applications. Cela permet de corriger d’éventuelles failles exploitées par les cybercriminels. Ayez un antivirus à jour.
7. Se méfier des offres trop belles pour être vraies. Une offre trop avantageuse ou un gain inattendu doit toujours éveiller la méfiance. Avant de cliquer ou de transmettre des informations, prenez le temps de vérifier la véracité de l’offre auprès de sources fiables.

En appliquant ces bonnes pratiques, chacun peut renforcer sa sécurité en ligne et contribuer à lutter contre la prolifération des arnaques sur Internet.