ARNAQUES ET SPOOFING

Categories: À la une !, Banques & organismes de crédit, Les autres arnaques, Quotidien
Tags: Actualités, Conseils

> *Le terme « spoofing » provient de l'anglais et plus particulièrement du verbe « to spoof » qui signifie usurper, le spoofing correspondant en effet à une usurpation d'identité de la part de l'escroc. Le spoofing est une technique qui s'est énormément développée ces dernières années, notamment du fait de la DSP2 et de la mise en place de l'authentification forte sécurisant les paiements en ligne. Comment cette technique est-elle utilisée pour mieux arnaquer les consommateurs?*

1) Le spoofing mode d'emploi

La nécessité pour les prestataires de services de paiement de demander une authentification forte du consommateur pour ses achats en ligne a permis de réduire les risques qu'un escroc effectue directement un paiement à la place du payeur. Mais la fraude ne disparait pas pour autant, ce sont simplement les procédés des escrocs qui évoluent.

Comme l'explique Julien Lasalle, responsable du service de surveillance des moyens scripturaux à la Banque de France, « *les fraudeurs, plutôt que d'essayer la technologie, vont s'attaquer au porteur de la carte lui-même* ». Plus particulièrement, c'est en manipulant ce dernier que les escrocs parviennent à lui faire valider lui-même et par le biais de l'authentification forte les opérations frauduleuses.

Pour y parvenir, le fraudeur usurpe l'identité d'une source fiable, le plus souvent un professionnel, et contacte sa potentielle victime par appel téléphonique, courrier électronique ou même SMS. L'escroc dispose alors de plusieurs moyens afin de gagner la confiance de son interlocuteur.

En cas d'appel par exemple, il est en général capable de personnaliser le numéro apparaissant pour le consommateur, de manière à afficher le numéro de la personne ou de l'établissement usurpé et non le sien. De la même façon, un e-mail frauduleux va reproduire à l'identique le type d'e-mails qu'envoie habituellement la personne ou l'établissement usurpé.

Notons que les escrocs ont tendance à préférer les appels aux e-mails ou SMS car une personne est plus facilement manipulable lorsqu'il est possible de lui parler directement. Celle-ci a en effet du mal à prendre du recul sur la situation et n'a pas ou très peu d'éléments lui permettant de détecter la fraude. C'est moins le cas dans l'hypothèse d'un e-mail ou d'un SMS dans lequel il est possible de rechercher des fautes d'orthographe ou de s'interroger sur la réelle provenance du message.

Une fois la conversation engagée, le fraudeur va tenter d'établir une relation de confiance avec son interlocuteur. Pour ce faire, il va rassurer la victime en lui exposant des informations la concernant et que seul le professionnel qu'il prétend être est censé connaître. Cela demande un travail en amont de l'escroc qui va devoir se procurer des données confidentielles sur les gens qu'il souhaite arnaquer. Pour y parvenir, il peut notamment faire du piratage informatique, parcourir les réseaux sociaux ou encore acheter des données sur le Dark Web, ce dernier étant un ensemble caché de sites internet permettant de préserver l'anonymat et la confidentialité de ses utilisateurs.

Lorsque la personne est rassurée sur l'identité de son interlocuteur, celui-ci va chercher à lui faire peur afin de la perturber et de l'amener à faire ce qu'il lui demande. En sa qualité de professionnel, il indique à sa victime avoir remarqué des mouvements frauduleux sur son compte bancaire. Celle-ci va alors paniquer et vouloir remédier à la situation au plus vite, et ce avec l'aide de l'escroc qu'elle pense professionnel et fiable.

Le fraudeur propose alors à sa victime de bloquer les opérations frauduleuses en cours. Il a pour cela besoin d'elle et lui demande soit de valider directement des opérations censées éviter la fraude, soit de lui transmettre les codes qu'elle reçoit afin qu'il les valide lui-même. Mais pendant que la victime pense permettre à un professionnel d'empêcher une tentative de fraude, en réalité l'escroc lui fait autoriser des opérations ne profitant qu'à ce dernier.

En général, la technique du spoofing nécessite du fraudeur un piratage du compte bancaire de sa victime afin qu'il puisse initier les opérations de son choix. Comme il ne peut aller au bout en raison de la nécessité d'une authentification forte pour les valider, il manipule alors sa victime car elle seule peut autoriser les opérations en question. Cela remet donc en cause l'efficacité de l'authentification forte qui certes complique quelque peu le travail des fraudeurs, mais n'empêche pas pour autant la fraude d'avoir lieu.

Bien souvent, les victimes réalisent qu'elles se sont fait avoir trop tard. Il ne leur reste plus qu'à contacter l'établissement de paiement afin de leur signaler la situation et faire opposition. On retrouve ici l'obligation de notification prévue par la DSP2 et le code monétaire financier. Elles doivent également porter plainte, bien que qu'un dépôt de plainte ne soit pas nécessaire pour demander le remboursement des opérations non autorisées. Notons que ce type de fraude ne touche pas que des personnes naïves mais bien tout type de gens ; les fraudeurs étant doués pour amener leurs interlocuteurs à leur faire confiance.

Les opérations frauduleuses correspondent à des ajouts de bénéficiaires sur le compte bancaire, à des virements et/ou à des achats en ligne. Les sommes prélevées peuvent être très importantes et les effets dévastateurs pour les victimes. Il arrive qu'elles parviennent à récupérer leur argent mais la tâche n'est pas toujours simple, notamment du fait que les opérations ont été validées par le biais de l'authentification forte.

Afin de contrer ce phénomène, les banques font de la prévention et rappellent sur leurs sites ou applications mobiles qu'elles ne contacteraient jamais leurs clients pour leur faire valider une opération et qu'elles ne leurs demanderaient jamais des données de connexion ou d'informations bancaires. Elles appellent également leurs utilisateurs à ne jamais répondre aux communications qui n'auraient pas été sollicitées et à contacter leurs banques par leurs propres moyens.

Mais le spoofing est malgré tout très utilisé dans la pratique et l'ADC France reçoit énormément de dossiers de victimes de cette technique. Nous avons sélectionné quelques-uns de ces dossiers afin d'illustrer les propos ci-dessus.

2) Quelques exemples

Le premier exemple concerne une adhérente de l'association qui reçoit un appel téléphonique d'une personne prétendant être un policier. Celui-ci aurait constaté des opérations suspectes sur le compte bancaire de son interlocutrice, qui n'en est bien sûr pas à l'origine. L'escroc lui indique qu'en tant que policier, il peut remédier à la fraude en cours et la met en confiance en lui donnant des informations personnelles telles que sa date de naissance et sa banque.

Elle reçoit alors deux messages lui demandant de confirmer les opérations censées bloquer les paiements. Suivant les instructions de l'escroc, elle valide ces dernières. L'escroc raccroche, et lorsque la victime vérifie l'état de son compte, elle réalise que deux paiements de 308,32 euros et 751,24 euros ont été réalisés.

Le second exemple est semblable au premier sauf que cette fois, l'escroc se fait passer pour un salarié de Boursorama Banque et explique à sa victime que des paiements frauduleux sont en cours sur le compte commun du couple. Il contacte d'abord la femme et lui demande de transmettre les codes qu'elle reçoit afin qu'il puisse bloquer les paiements. Puis il l'informe qu'il va devoir contacter son mari. Ce dernier, mis au courant par sa femme de la situation, répond à l'appel et transmet également à l'escroc les codes qu'il reçoit. Il finit par se rendre compte de l'arnaque mais raccroche trop tard, deux virements de 6 500 euros et 10 000 euros ainsi que des achats pour un total de 15 629,84 euros ayant déjà été effectués.

Ce dernier cas est d'autant plus intéressant que la femme devient sans le vouloir la complice de l'escroc. Comme elle prévient son mari qu'il va recevoir un appel de sa banque, ce dernier est moins méfiant que s'il n'avait pas été averti par sa femme et le travail du fraudeur en est facilité. Nous remarquons également l'énorme montant des sommes prélevées et l'importance du préjudice subi par les victimes. Une telle fraude est d'autant plus étonnante qu'elle a abouti en raison de l'absence de réaction de la banque sur des opérations aussi importantes. Qu'en est-il du devoir de vigilance auquel sont pourtant soumis les prestataires de services de paiement ?

Un récent cas de spoofing a également attiré notre attention : en plus des étapes habituelles, l'escroc se faisant passer pour un conseiller bancaire a informé sa victime qu'il devait récupérer sa carte bancaire compromise dans le but de lui en envoyer une nouvelle. Pour ce faire, il a prévenu son interlocuteur qu'un taxi allait venir à son domicile chercher sa carte. Cela a réellement eu lieu, une voiture se faisant passer pour un taxi s'étant effectivement rendue chez la victime afin que celle-ci lui donne son instrument de paiement. Des retraits d'espèces frauduleux ont par la suite été effectués à l'aide de la carte bancaire en question.

Si vous pensez avoir été victime d'une arnaque, contactez-nous à contact@adcfrance.fr ou au 03.62.02.11.15.

(*Texte tiré du mémoire de Madame BELLAIRE : https://adcfrance.fr/banque-organisme-de-credit/fraude-a-la-carte-bancaire-le-memoire-de-troisieme-cycle-de-madame-tara-bellaire/*)