Smishing – un SMS qui risque de vous coûter cher

2 mars 2021 | Beatrice Kübli

La communication numérique se faisant de plus en plus à l'aide des smartphones et des services de messagerie, les escrocs tentent désormais d'attirer leurs victimes dans un piège par le biais de messages courts (SMS, WhatsApp, etc.). Ce nouveau mode opératoire porte le nom de smishing, une contraction des mots « SMS » et « phishing », ou hameçonnage.

Le smishing : comment cela fonctionne

Un message vous est envoyé par SMS ou par un autre service de messages courts, exigeant une réponse. Et, souvent, il vous donne à entendre que le temps presse, ou que vous risquez de subir des conséquences déplaisantes si vous n'obtempérez pas. Le texto a un contenu crédible, par exemple :

- un avis d'envoi par la poste ;
- un colis bloqué parce que les frais de port n'ont pas été réglés ;
- un code envoyé par erreur par l'un de vos contacts ;
- un message que vous n'auriez pas vu ;
- un concours qui propose des prix alléchants.

Vous êtes invité·e à cliquer sur un lien pour envoyer un texto à un numéro donné ou répondre à un texto.

Les conséquences d'une attaque de smishing

Voici ce qui risque de se passer si l'on cède à la demande :

- vous aurez conclu un abonnement, par exemple en répondant par « oui » à un texto ;
- vos données de paiement risquent d'être utilisées abusivement, par exemple parce que vous avez été amené·e à saisir votre identifiant Apple pour télécharger une application prétendument urgente, ou à cliquer sur un lien qui ouvre une page de paiement falsifiée ;

- un compte est piraté, par exemple, lorsque vous transmettez un code à quelqu'un qui se fait passer pour un ami. En réalité, il s'agit du code de confirmation pour réinitialiser un compte (par exemple WhatsApp). Les arnaqueurs saisissent un nouveau mot de passe et prennent le contrôle.
- Un logiciel malveillant sera installé, par exemple après avoir cliqué sur un lien.

Excès de confiance, manque de contrôle : les arnaqueurs se frottent les mains

Les gens sont plus enclins à faire confiance à un texto qu'à un courriel, et sont plus susceptibles d'y répondre – les arnaqueurs comptent là-dessus. Si le danger que représentent les liens dans les courriels est connu de la plupart des gens qui se montrent donc circonspects, un texto est souvent perçu comme un message personnel et digne de confiance. À cela s'ajoute le fait qu'actuellement, le contenu des SMS ne peut pas être vérifié ; alors que les fournisseurs de courrier électronique et les programmes de messagerie filtrent les courriels d'hameçonnage, les fournisseurs de services de télécommunication n'ont pas les bases légales pour le faire. Ainsi, analyser les contenus des textos reviendrait à violer le secret des télécommunications. En outre, rares sont ceux qui ont un antivirus ou un antispam installé sur leur smartphone, ce qui est particulièrement important pour les appareils Android, les iPhones étant mieux protégés par l'architecture fermée du système Apple.

Comment me protéger contre le smishing ?

- En cas de doute, **renseignez-vous ailleurs,** sur des canaux officiels ! Appelez la Poste, l'ami ou la collègue, etc. ou envoyez un courriel à une adresse officielle ! Ne PAS utiliser les informations données dans le SMS à cette fin !
- **N'ouvrez aucun document** et ne cliquez sur aucun lien si vous n'êtes pas sûr·e à 100% de l'expéditeur !
- **Méfiez-vous de toute anomalie !** Est-ce bien le style qu'adopterait normalement votre contact pour vous écrire ? La demande formulée est-elle conforme à ce qui se fait habituellement dans ce cas ? Par exemple, qu'un versement soit requis pour la remise d'un prix est plutôt inhabituel.
- **Vérifiez sur Google** si la demande a déjà été identifiée comme une arnaque.
- **Supprimez le message !**
- **Installez un logiciel antivirus** et antispam sur votre smartphone Android !
- **Veillez à mettre régulièrement à jour le logiciel** de votre smartphone !