Le « smishing » ou hameçonnage par SMS

Vous avez peut-être déjà reçu des SMS qui semblent être émis par une administration, une banque, un service de livraison ou tout autre organisme ou entreprise notoire, et qui vous inciteront à réaliser rapidement une action (se connecter, confirmer, mettre à jour, ou encore effectuer un paiement…), sous peine de vous voir appliquer des restrictions de service, une amende ou des frais. Attention, il s'agit probablement d'une tentative d'hameçonnage par SMS, également appelée « smishing ». Ce type de cyber-arnaque se multiplie depuis 2020, notamment parce qu'il est plus difficile d'identifier des SMS frauduleux que des mails d'hameçonnage.

Contacter l'entreprise en cas de doute

C'est pourquoi le site Cybermalveillance.gouv.fr vient de publier une fiche indiquant les ressorts et les spécificités de l'hameçonnage par SMS. Il rappelle comment se déroule ce type d'hameçonnage, donne plusieurs exemples concrets de messages frauduleux et explique quelles peuvent être les conséquences de ces arnaques. Enfin, la fiche indique comment réagir lorsque l'on reçoit un message d'hameçonnage par SMS et ce qu'il faut faire si on en est victime. Il est notamment conseillé au moindre doute, de contacter directement l'administration ou l'entreprise qui est censée avoir adressé

le SMS pour confirmer le message reçu. Sachant que l'administration n'adresse jamais à ses administrés de relance par SMS, ni de demande d'informations et encore moins d'amende.

Pour consulter la fiche : https://www.cybermalveillance.gouv.fr/tous-nos-contenus/actualites/smishing-hameconnage-sms