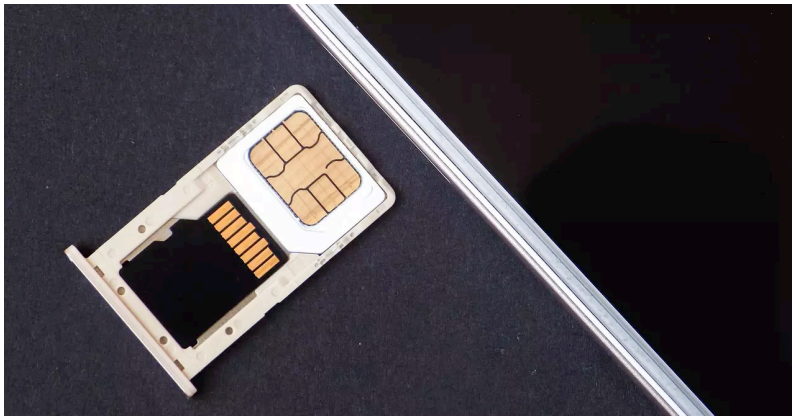
OVATION
AMERICAS

# Juin 2022 Infolettre

# Vérifiez si votre carte SIM a été clonée en procédant comme suit :

## Signes que votre carte SIM a été clonée



**Les pirates pourraient cloner votre carte SIM sans que vous vous en rendiez compte.**

Pour ce faire, ils peuvent utiliser l'ingénierie sociale et usurper l'identité de votre identité. C'est un problème sérieux, car ils pourraient agir en votre nom, recevoir des codes 2FA pour se connecter à vos comptes, passer des appels ou envoyer des SMS, etc. Il y a quelques drapeaux rouges qui peuvent indiquer que votre carte mobile a été clonée ou, au moins, qu'il y a quelque chose d'étrange.

Ce type d'attaque est connu sous le nom d'échange de carte SIM. Fondamentalement, il s'agit d'un cybercriminel capable de cloner votre carte mobile. Vous utiliserez toujours une stratégie pour y parvenir, soit en trompant la compagnie de téléphone, soit l'utilisateur lui-même. Heureusement, ce n'est pas un problème courant, car il existe des mesures de sécurité importantes. Cependant, il est pratique de savoir quels signes il pourrait y avoir et ainsi éviter les problèmes.

## Vous ne recevez pas d'appels

L'un de ces signes est que vous ne recevez pas d'appels. Vous essayez même de vous appeler depuis un autre mobile, de donner un signal mais vous ne recevez rien sur le mobile. Il y a quelque chose d'étrange et vous commencez à soupçonner que vous n'avez peut-être pas le contrôle de votre carte SIM et que quelqu'un a pu la cloner sans que vous vous en rendiez compte. Ce problème est sans aucun doute l'un des plus courants. Peut-être avez-vous reçu un appel étrange, vous alertant d'un problème supposé, et c'est en fait ce qui a déclenché le vol de votre carte. À partir de là, vous ne pourrez plus recevoir d’appels.

## Les SMS n'arrivent pas

Quelque chose de similaire se produit avec les SMS. Les pirates, en fait, visent à cloner des cartes mobiles précisément pour avoir le contrôle des messages texte. De cette façon, ils pourront recevoir des codes d'authentification à deux facteurs, par exemple, et accéder à des comptes bancaires, des réseaux sociaux, etc. Si vous voyez qu'un SMS ne vous parvient pas, si vous vérifiez qu'il doit bien arriver et que vous voyez aussi que vous ne recevez pas d'appels non plus, c'est sans aucun doute un signe que quelque chose se passe. Cela ne signifie pas toujours qu'il s'agit d'une attaque SIM Swapping, mais c'est une possibilité.

## Vous avez perdu la connexion

Un autre signe que vous allez avoir est si vous voyez que vous avez perdu la connexion. Vous essayez de vous connecter encore et encore, vous êtes dans une zone avec une couverture, mais néanmoins vous voyez que cela ne fonctionne pas. C'est comme si vous n'aviez pas de carte SIM insérée et que votre téléphone mobile ne recevrait aucun signal d'aucune sorte et que vous n'auriez pas d'appels, de SMS ou d'Internet. Bien que cela puisse se produire pour de nombreuses raisons, telles qu'une défaillance de la ligne, une mauvaise couverture ponctuelle ou même des problèmes avec la carte SIM endommagée, la vérité est que cela pourrait

également être dû à un clonage de carte mobile.

### Votre téléphone a un emplacement différent

Si vous vérifiez l'emplacement de votre téléphone et qu'il semble que vous étiez ailleurs, comme si votre ligne mobile se trouvait dans une autre ville ou un autre pays, c'est un signe clair que votre carte a été clonée sans que vous vous en rendiez compte. C'est quelque chose qui devrait vous alerter et prendre rapidement des mesures, comme appeler la compagnie de téléphone. La chose normale est que celui qui clone votre carte SIM est dans un autre endroit physique. Fondamentalement, ce que vous allez faire avec une attaque d'échange de carte SIM est d'usurper l'identité et de recevoir une carte physique comme si c'était vous. Ce ne sera pas quelqu'un que vous avez à proximité, donc voir que l'emplacement a changé est un bon signe.

### Vous recevez des messages étranges

Vous pouvez également commencer à recevoir des messages étranges, dont vous ne comprenez pas très bien pourquoi. Il se peut que le pirate lui-même vous envoie des instructions pour soi-disant résoudre un problème avec la ligne. C'est ce qui pourrait lui permettre de cloner votre carte, vous ne devriez donc jamais tomber dans ce type de piège. De même, ce clonage peut avoir déjà eu lieu et vous pouvez commencer à recevoir des

e-mails étranges, soit de la part de l'attaquant, soit d'autres services que vous utilisez ou utilisez en votre nom. C'est une autre cause d'alerte. En bref, comme vous pouvez le voir, ces signaux vous aideront à savoir que votre carte SIM a été clonée. Il est essentiel d'éviter les attaques qui utilisent la carte SIM. Vous devez toujours garder le bon sens, avoir les appareils protégés et mis à jour.

---

Continuons à apprendre et à rester à jour sur les questions de protection de la vie privée et de sécurité pour nous donner les meilleures chances d'éviter les piratages et les escroqueries coûteuses.

Pour des commentaires, des informations ou pour savoir comment minimiser votre exposition aux données, n'hésitez pas à nous contacter à l'adresse suivante:

info@ovationamericas.com ou visitez notre site web au: www.ovationamericas.com

OVATION
AMERICAS