Arnaque téléphonique société général (SG) carte/compte bancaire

---
Par Treka

Je reçoit l'appel d'un agent des fraudes société générale le 11/05/2022 (13h10, un moment ou les banque sont fermé), m'annonce des activités frauduleuses sur mon compte : Un paiement a été effectué à "Londres" d'un montant de 768?, il me demande alors si c'est bien moi.

Je lui répond que ce n'est pas moi, il me dit que ma carte bleu a était piraté et me propose alors d'annuler le paiement et de faire opposition sur ma carte, action que j'accepte. Je reçoit alors un message avec comme intitulé "SOCIETEGEN", me disant que m'a carte à été opposé et que je reçevrait ma nouvelle carte sous 3j. ensuite je reçoit un second message avec un lien sur lequel je dois cliquer pour valider l'annulation de la transaction. C'est ici que tout commence. Je clique sur le lien (avec mon téléphone), j'attérit sur une page web "https://connexionsg.fr", sur laquel je doit renseigner mon identifiant mot de passe pour me connecter à mon compte, une fois fait je reçoit directement une notification sur le site pour annuler la transaction, je clique donc sur le bouton valider. A ce moment ils avaient réussis à récupérer mon identifiant et mon mot de passe.

Il me fait ensuite remarquer que mon pass sécurité est désactivé (pass sécurité : le fait de recevoir un code de confirmation sur son téléphone pour chaque achat effectué en ligne). Je trouve ça bisard car il a toujours été activé sur mon compte, il me raconte alors une histoire comme quoi il peut y avoir des bugs et que ça peut se désactiver tout seul. Il me propose alors de le réactiver, action que j'accepte. Il me demande alors de me connecter sur l'application de la société générale pour valider l'activation du pass (à ce moment la, ils se sont connecté à mon compte sur leur téléphone et ont fait une demande de transfert du pass sécurité sur leur téléphone. Pour que celle ci soit effective, il faut la valider sur l'ancien téléphone). Sur le moment, je ne me doutait de rien, sachant que je recevait des SMS crédible et que je faisait des manipulation sur mon compte de la SG. Je me connecte donc sur l'application de la SG et je reçoit directement une notification pour "Activer" le pass sécurité. Je clique donc sur le bouton "Activer", qui au lieu de m'activer mon pass sécurité, le transfert sur leur téléphone.

Enfin il me propose d'envoyer un coursier pour récupérer ma carte et me donner une carte de remplacement le temps de recevoir la nouvelle carte dans les 30min qui suivent. Je trouve ça cool comme innovation de la part de la SG et j'accepte sans me douter que cela est une arnaque sachant que j'ai reçu des soit disant "notification" de la part de la personne au téléphone sur mon application SG. Je raccroche donc et je commence à mettre ma carte dans une enveloppe comme demandé.

C'est à ce moment que ma compagne me fait remarquer que c'est quand meme louche, et en y repensant j'admet que c'est quand meme un peu trop d'innovation soudainement. Je cherche donc sur internet et heureusement je tombe sur ce post (merci à la personne qui l'a écrit).
J'appelle donc le service d'urgence, je change le mot de passe de mon compte et retransferer le pass sécurité sur mon téléphone.

Je vous écrit donc pour vous avertir, attention le phishing devient de plus en plus poussé :
- SMS avec comme libellé "SOCIETEGEN"
- URL de site web pas trop déconnant
- Validation d'opération directement sur l'application SG
- Message d'attente au téléphone "Bonjour et bienvenu à la société général, etc...

Ps: Je précise également que cette personne avait tout les renseignements me concernant : Adresse e-mail, adresse postale, vue sur mes comptes (ayant récupéré mes identifiant mdp au début des manipulation) et avant de raccroché il m'a bien demandé si tout me semblait bon sur mon compte (histoire que je ne me reconnecte pas dessus de ci-tot).

Par Henriri

Hello !

Pour le coup vous avez été assez imprudent Treka. J'espère que ces malfrats n'ont pas eu le temps de vous prendre de

l'argent. Mais ce genre de tentative est somme toute assez connue. Et aucune banque ne sollicite ainsi nos identifiants et codes.

A+

Par yapasdequoi

Bonjour,
Merci de cette alerte. Tant qu'l y aura des gens non avertis, les escrocs ont de beaux jours devant eux.

Voici une collection de cas similaires :
[url=https://www.google.com/search?q=arnaques+bancairesau+t%C3%A9l%C3%A9phone&rlz=1C1CHBF_frFR782FR782&ei=Sv2mYpb3BZ2Iur4PubGw-As&ved=0ahUKEwiWxI_ziKr4AhUdhM4BHbkYDL8Q4dUDCA4&uact=5&oq=arnaques+bancairesau+t%C3%A9l%C3%A9phone&gs_lcp=Cgdnd3Mtd2l6EAM6BQgAEIAEOgYIABAeEAc6BAgAEB46BggAEB4QBToECAAQDToGCAAQHhANSgQIQRgASgQIRhgAUABYukBg40JoA3AAeACAAWqIAeYHkgEEMTMuMZgBAKABAcABAQ&sclient=gws-wiz]https://www.google.com/search?q=arnaques+bancairesau+t%C3%A9l%C3%A9phone&rlz=1C1CHBF_frFR782FR782&ei=Sv2mYpb3BZ2Iur4PubGw-As&ved=0ahUKEwiWxI_ziKr4AhUdhM4BHbkYDL8Q4dUDCA4&uact=5&oq=arnaques+bancairesau+t%C3%A9l%C3%A9phone&gs_lcp=Cgdnd3Mtd2l6EAM6BQgAEIAEOgYIABAeEAc6BAgAEB46BggAEB4QBToECAAQDToGCAAQHhANSgQIQRgASgQIRhgAUABYukBg40JoA3AAeACAAWqIAeYHkgEEMTMuMZgBAKABAcABAQ&sclient=gws-wiz[/url]