17.03.2023

Peut-on hacker un compte d’e-banking avec l’IBAN, l’adresse et une copie de la carte d'identité du titulaire ? Non, mais...

Dans plusieurs types d’arnaques, les criminels demandent aux victimes de leurs communiquer toute une série de données personnelles (nom, adresse, numéro de téléphone, etc.). Dans certains cas, ils demandent même l'IBAN ou une copie du passeport ou carte d'identité.

Les mesures de sécurité mises en place par les banques étant de plus en plus performantes, les malfaiteurs ont presque toujours recours à l’« ingénierie sociale ». En d’autres termes, ils s’ingénient pour tromper et manipuler leurs victimes afin de les inciter à leur communiquer toutes les informations dont ils ont besoin pour leurs méfaits. Pour cela, ils ont souvent recours à de faux e-mails ou à de faux sites web.

En fait, si l'on considère la réalité des comptes d’e-banking actuels, ces données ne sont pas toutes utiles aux fins de l’arnaque proprement dite, mais servent plutôt à établir une relation de confiance avec les victimes et à souligner le sérieux de l'offre. Il peut s’agir par exemple d’une offre de remboursement ou d’une distribution de bénéfices. Si l'on ne peut pas prélever directement de l’argent d'un compte avec un numéro d’IBAN et une copie de la carte d'identité, il est néanmoins possible de l’utiliser pour effectuer par exemple un paiement par prélèvement bancaire dans une boutique en ligne. Il faut dire cependant que cette pratique ne s’avère pas intéressante pour les arnaqueurs dans la mesure où les victimes ont jusqu’à un an pour contester ces ordres de paiement auprès de la banque et les annuler.

Par contre, si l'on considère la collecte d’adresses et de copies de passeports ou cartes d’identité dans un contexte d’ouvertures de nouveaux comptes auprès d'instituts bancaires ou établissements de crédit à l’étranger, la question prend une tout autre tournure. Munis d'une adresse et de la copie d'un passeport ou d'une carte d’identité, les criminels verront en effet leurs demandes accueillies avec succès par les établissements financiers. L’ordinateur ou le téléphone portable des fraudeurs sont enregistrés auprès de la banque, de sorte que la procédure d’authentification à deux facteurs ne posera aucun problème. L'escroc pourra ensuite disposer pleinement du compte ouvert au nom de la victime. Ce nouveau compte sera utilisé pour les activités illicites du criminel. Dans la mesure où ce n’est pas le nom de l’escroc qui apparaît mais celui de la victime, c’est elle qui portera la responsabilité pénale des agissements du premier. Les éventuelles procédures judiciaires peuvent s’avérer compliquées et longues lorsqu'il faut prouver que la victime de la fraude n’a pas commis de délit.

En règle générale, il convient de faire preuve de scepticisme et de retenue lorsque l'on vous demande de communiquer des données personnelles. Par ailleurs, toute irrégularité doit être immédiatement signalée à votre banque et à la police.