Arnaques par téléphone : les faux services d'assistance

Pour aller à la pêche aux informations confidentielles, les hameçonneurs utilisent non seulement Internet, mais aussi le téléphone. Cette technique s'appelle le « vishing ».

Pour vous protéger :

- mettez fin à tous les appels non sollicités provenant de soi-disant opérateurs de Microsoft ou autres services d'assistance informatique ou d'instituts financiers.
- ne vous fiez pas au numéro qui s'affiche sur l'écran de votre téléphone.
- ne communiquez jamais vos données personnelles (mots de passe ou numéros de cartes de crédit) à d'autres personnes.
- en cas de besoin, composez toujours les numéros de téléphone officiels de Microsoft ou des services d'assistance.
- pour contacter votre institut bancaire, utilisez exclusivement les numéros de téléphone officiels, que vous retrouverez par exemple sur vos extraits de compte.

Le terme « vishing » est la contraction de « Voice-Phishing ». Comme pour les attaques par hameçonnage classique, les criminels manipulent leurs victimes pour les inciter à communiquer de leur plein gré des informations confidentielles ou à installer de prétendus programmes de sécurité, alors qu'il s'agit en réalité de logiciels malveillants ou malwares.

Au téléphone, les escrocs se font souvent passer pour des employés de Microsoft ou d'un centre d'assistance informatique, ou bien encore d'une banque. Le prétexte de leur appel peut être par exemple une infection par virus ou tout autre problème d'ordre technique. Leur véritable intention consiste en revanche à convaincre leur interlocuteur de télécharger un programme ou de consulter un site piraté, mais en apparence parfaitement identique au site officiel.

D'une manière ou d'une autre, les criminels réussissent à accéder directement au dispositif de leurs victimes pour ensuite intercepter leurs mots de passe par exemple, ou espionner les informations stockées sur leur ordinateur, les copier et les traiter. Les prétendus services d'assistance étant parfois payants, les escrocs peuvent aller jusqu'à demander à leurs victimes de communiquer leur numéro de carte de crédit, qu'ils utiliseront ensuite de manière abusive.

Les personnes qui appellent parlent souvent un mauvais anglais. Sachant que les numéros d'appel peuvent être manipulés, la victime peut parfois reconnaître sur l'écran de son téléphone le véritable numéro de la société en question.

S'il est trop tard et que vous avez permis à quelqu'un d'accéder à votre ordinateur, coupez immédiatement la connexion Internet et éteignez-le. Ne rallumez votre appareil que lorsque le réseau est désactivé (par ex. wifi désactivé) et analysez immédiatement l'ensemble de votre disque dur avec un programme antivirus. Modifiez tous vos mots de passe. N'hésitez pas à demander l'aide d'un professionnel si vous n'êtes pas sûr de vous.

Si vous avez communiqué des données confidentielles (par ex. des données bancaires ou des informations concernant votre carte de crédit), contactez immédiatement la société de cartes de crédit et/ou votre institut bancaire, ainsi que la police locale.

*Qu'il s'agisse de Microsoft, d'autres sociétés informatiques ou d'instituts financiers, les services d'assistance n'appellent **jamais** les particuliers pour leur proposer leurs services sans y avoir été sollicités. En cas de problème technique, la prise de contact doit toujours de faire sur l'initiative du client.*

Mémento :

(https://www.ebas.ch/wp-content/uploads/2019/09/supportSKP_fr.pdf)