CABINET ROSTAING
EXPERT COMPTABLE - COMMISSAIRE AUX COMPTES

Chère Cliente, Cher Client,

Nous constatons de plus en plus de tentatives de fraude et le monde de l'expertise comptable n'est pas épargné. Récemment, plusieurs cabinets d'expertise comptable ont été victimes, tout comme les établissements bancaires, de tentatives de fraude par téléphone (Spoofing).

Dernièrement nous avons été alertés par le Conseil national de l'ordre des experts-comptables d'une **usurpation d'identité de certains cabinets afin d'obtenir les données bancaires des clients**.

Les clients sont contactés par téléphone par le fraudeur qui utilise le numéro du cabinet d'expertise comptable techniquement détourné. Au motif d'une mise en conformité avec le RGPD remboursée par les impôts, il est demandé au client de se connecter à son compte bancaire.

Les clients qui auraient été victimes de cette arnaque doivent **porter plainte** et signaler à leur banque cet accès frauduleux à leurs coordonnées bancaires pour que l'établissement puisse contrôler les mouvements sur le compte et intervenir si nécessaire.

Pour information

Qu'est-ce que le « spoofing » ?

Le « spoofing » est une technique où le fraudeur vous appelle depuis le numéro de téléphone du cabinet. Il vous aura la plupart du temps contacté quelques jours plus tôt en se faisant passer pour une administration (impôts, URSSAF, CCI…) afin d'obtenir des informations sur le nom de votre cabinet d'expertise comptable et ensuite pouvoir récolter suffisamment d'informations pour vous mettre en confiance.
Il va alors vous demander d'effectuer un virement pour vous acquitter d'une taxe ou d'une opportunité d'investissement ou de financement qui vous serait remboursée par la suite. Il créé un contexte d'urgence en vous invitant à saisir immédiatement le RIB et à réaliser un virement instantané. Il arrive aussi qu'il vous invite à vous connecter sur votre site bancaire et qu'il demande à prendre la main pour réaliser une "opération de validation" qui viserait en fait à réaliser un virement à son profit.

Comment le fraudeur fait-il pour arnaquer ses victimes ?

Le cybercriminel va usurper un numéro d'appel ou un email, qui vont sembler légitime pour la victime. A titre d'exemple, il sera affiché un autre numéro que le sien sur votre téléphone. Le principe de manipulation reste ensuite identique pour tous les modes existants : caractère d'urgence, force de persuasion, autorité, confidentialité, flatterie, sont autant de biais psychologiques qui pourront être utilisés par les fraudeurs pour parvenir à exploiter la naïveté humaine.
Nul n'est à l'abri d'une arnaque de ce type, qui est très facile à initier via un appel, un SMS ou une adresse email, d'apparence officielle. Elle leur permet en effet de brouiller les pistes pour berner la victime plus facilement.
Ces typologies d'attaques sont rendues possibles grâce à la multitude d'informations accessibles pour les cybercriminels, à savoir :

- La collecte d'information facilitée par les réseaux sociaux et professionnels, tels que : nom, prénom, adresse, numéro de téléphone etc.
- Le piratage des cartes bancaires simplifié par le fait que les numéros de la carte de paiement débutent le plus souvent par 6 chiffres identiques, sans qu'elles ne soient spécifiques à chaque client ;
- Le numéro d'IBAN, très simple à récupérer, car il est souvent communiqué à des prestataires, présents sur des sites Web, voir même du Dark Web …
- L'utilisation du bluff permet d'usurper l'identité de prestataires tels que Amazon, la Fnac, Facebook ou des administrations, car il est plus que probable que vous ayez eu des échanges récents avec ces potentielles sources.

Comment se protéger ?

- Ne révélez jamais vos identifiants de connexion ;
- Ne communiquez jamais d'informations sensibles par messagerie ou téléphone ;
- Vérifiez toujours l'URL du site web sur lequel vous vous connectez : positionnez le curseur de votre souris sur ce lien et vérifiez l'adresse du site ;
- Ne validez jamais de transaction ou de connexion à vos comptes à la demande d'un tiers ;
- Si une procédure vous est inconnue ou vous paraît suspecte, vérifiez sa véracité auprès des services habilités ;
- Lisez attentivement les notifications et les messages de vérification par SMS que vous recevez lorsque des transactions sont effectuées sur votre compte. Assurez-vous d'en être à l'origine et que vous reconnaissez l'IBAN et les noms des bénéficiaires ;
- En cas de doute, faites des contre-appels sur les numéros habituels (n'hésitez pas à privilégier les numéros de portables déjà référencés) afin de vérifier l'identité de l'appelant et valider les informations communiquées. En effet, si le fraudeur peut modifier le numéro qui s'affiche lorsqu'il vous appelle, il n'a néanmoins pas la capacité d'intercepter les appels ;
- Méfiez-vous des appels ou email urgents ;
- Sensibilisez vos équipes sur ce risque majeur.

Si vous avez le moindre doute, n'hésitez pas à nous contacter pour toute information complémentaire.

Didier ROSTAING
Expert-Comptable & Commissaire Aux Comptes