Protégez-vous contre la fraude financière

Novembre étant le mois de la littératie financière, c'est le bon moment de comprendre comment se protéger contre la fraude financière. D'une part, la technologie a facilité l'exécution des transactions financières, mais d'autre part elle a accru le potentiel de fraude. Bien que les ainés soient particulièrement vulnérables (nous y reviendrons plus tard), tout le monde l'est en fait et nous devrions tous apprendre à nous protéger.

Qu'est-ce que la fraude financière?

La fraude financière se présente sous différentes formes, mais, fondamentalement, elle implique des criminels qui volent les renseignements financiers de quelqu'un d'autre pour en tirer un certain profit. Muni de données personnelles provenant de relevés de comptes bancaires, de cartes de crédit ou de comptes de placement, le criminel peut demander des cartes de crédit ou des prêts au nom de la victime et avoir accès à de l'argent gratuit.

Bien que les institutions financières comprennent bien les dangers du vol d'identité et qu'elles continuent de s'efforcer de fortifier leur sécurité numérique afin de faire entrave à la cybercriminalité sur leurs sites Web et leurs applications, vous pouvez prendre des mesures vous-même pour vous protéger.

Protégez vos informations personnelles

C'est horrible de découvrir que quelqu'un a volé vos données personnelles pour obtenir un faux passeport, une fausse carte de crédit ou un faux permis de conduire. Cette atteinte à la vie privée peut également avoir des conséquences financières.

Faites attention à la façon dont vous traitez les données personnelles comme votre nom, votre adresse, votre numéro d'assurance sociale et les informations relatives à vos comptes financiers. Ne partagez ces informations que lorsque cela est nécessaire et avec des personnes que vous savez légitimes. Déchiquetez les documents imprimés dont vous n'avez plus besoin et conservez ceux qui ont encore de la valeur.

Les criminels utilisent souvent des menaces d'emprisonnement, d'expulsion ou d'autres actions en justice, dans l'espoir de vous intimider pour que vous leur fournissiez les informations qu'ils veulent. Restez calme et demandez-leur leur nom, leur titre et l'entreprise qu'ils sont censés représenter. Ne vous sentez pas obligé d'agir immédiatement. Contactez l'entreprise en question et confirmez si elle essaie de vous joindre et si la personne qui vous a approché est légitime.

Pensez avant de cliquer

Les cybercriminels sont devenus très experts lorsqu'ils escroquent leurs victimes. Ils peuvent vous proposer une « bonne affaire » ou prétendre que vous avez gagné un prix, et ce, dans l'espoir de vous inciter à divulguer des informations financières. Ils créent des sites Web et envoient des courriels ou des textos qui semblent authentiques et dignes de confiance mais, derrière chaque page Web ou texto, se cache un fraudeur qui attend de capturer et d'utiliser à mauvais escient vos renseignements personnels (ce que l'on appelle l'hameçonnage).

Comme la plupart des gens reçoivent de nombreux courriels, ainsi que des textos, et visitent de nombreux sites Web chaque jour, il est facile de cliquer sur un lien sans songer aux conséquences. Traitez chaque interaction numérique avec prudence. Le courriel provient-il d'une source légitime? Le site Web est-il réel? Dans les deux cas, les criminels peuvent créer des adresses qui semblent presque identiques aux adresses légitimes, mais avec une lettre en plus ou en moins, ou avec certaines lettres transposées ou un symbole supplémentaire inséré. Si quelque chose vous semble suspect, signalez-le à l'entreprise d'où provient le courriel, le texto ou le site Web présumé, et elle pourra en déterminer la validité.

De plus, ne partagez pas votre nom de connexion ou votre mot de passe avec quiconque prétendant en avoir besoin. En général, les entreprises et les organismes ne demandent pas des renseignements personnels de ce genre. Pour protéger vos mots de passe, pensez à utiliser l'authentification à deux facteurs et à avoir des mots de passe forts pour chaque site Web au lieu d'utiliser le même pour chaque connexion, ce qui pourrait donner aux criminels un accès instantané à tous vos comptes.

Une vigilance accrue pour les aînés

Les aînés peuvent être particulièrement vulnérables aux cybercriminels et autres escrocs. Bien que de nombreux aînés soient des adeptes de la technologie, beaucoup ne le sont pas. Ils n'ont pas grandi avec des appareils numériques perfectionnés et la technologie n'est donc pas une seconde nature pour eux. Ils peuvent également être atteints de démence ou d'autres troubles cognitifs ou auditifs, ce qui en fait des cibles faciles pour les criminels.

Les escroqueries conçues pour arnaquer les aînés consistent notamment à menacer de couper l'électricité ou d'autres services publics s'ils ne paient pas immédiatement leur « dette » ou à prétendre être un parent qui a désespérément besoin d'argent. Une autre escroquerie consiste à faire semblant de représenter un organisme caritatif et à demander un « don ». Pour aider à prévenir l'abus financier des aînés, prévenez vos proches âgés des escroqueries potentielles et comment y faire face. Il est également utile qu'ils aient un réseau de personnes de confiance - comme un conseiller, un comptable ou un avocat - qui peuvent les soutenir s'ils ont besoin d'aide et de conseils.

Pour en savoir plus sur la manière dont nous pouvons élaborer un plan adapté et vous aider à éviter la fraude financière, veuillez communiquer avec nous dès aujourd'hui.

(22-2129) 11/22

ON S'INVESTIT, POUR VOUS.