L’escroquerie par piratage psychologique

Le piratage psychologique est une forme de manipulation habile par courriel, par message texte, par appel téléphonique, ou même en personne. Il s’agit d’une technique très efficace couramment utilisée par les cybercriminels. Les cybercriminels ont souvent recours à la manipulation psychologique pour amener les gens à révéler des renseignements personnels ou à poser des gestes préjudiciables. Voici trois des tactiques couramment utilisées auxquelles il faut porter attention.

Des tactiques couramment utilisées auxquelles il faut porter attention

Manipulation fondée sur la peur. Les escrocs tentent souvent d’exploiter la peur ou l’anxiété pour influencer vos décisions. Ils peuvent envoyer des messages menaçants qui semblent provenir de sources crédibles, comme des forces de l’ordre, des organismes gouvernementaux ou des institutions financières. Ces messages peuvent contenir des avertissements de poursuite judiciaire, des menaces de comptes gelés ou d’autres conséquences graves. Ces tactiques visent à vous pousser à agir dans la panique en vous incitant à fournir des renseignements sensibles ou à verser de l’argent.

Urgence et contrainte de temps. Les fraudeurs créent souvent un faux sentiment d’urgence pour vous pousser à prendre rapidement des décisions. Par exemple, ils peuvent prétendre que votre compte bancaire est sur le point d’être fermé, ou que vous devez réagir immédiatement pour profiter d’une offre limitée dans le temps. L’objectif est de vous empêcher de vérifier des renseignements ou de prendre du recul avant de prendre une décision.

Des occasions irrésistibles. Si une offre semble trop belle pour être vraie, elle l’est probablement. Les escrocs peuvent promettre des applications haut de gamme gratuites, des offres exclusives, des gains inattendus ou encore des emplois très rémunérateurs. En échange, ils pourraient vous demander de divulguer vos justificatifs d’ouverture de session

Attention aux signaux d’alerte

- On vous presse à répondre immédiatement, sous peine de pénalités importantes, sans avoir le temps de réfléchir ou de vérifier la source du message.
- Le message emploie un langage menaçant ou fait référence à des conséquences juridiques ou financières immédiates.
- On vous fait croire que, si vous ne réagissez pas sur-le-champ, votre compte sera suspendu, un service sera annulé ou vous perdrez une offre exclusive.
- Vous recevez une offre de produits, d’argent ou de services gratuits, qui n’exige que très peu d’efforts, voire aucun.
- En échange de la récompense, on vous demande de fournir des renseignements personnels ou vos justificatifs d’ouverture de session.

Façons de vous protéger

- ☐ Prenez le temps d’évaluer la situation. Ne vous laissez pas entraîner par l’urgence d’un message qui cherche à bousculer votre jugement ou votre décision. Prenez le temps de ralentir, d’analyser les détails attentivement et de vérifier les faits avant de poser un geste, quel qu’il soit. Les fraudeurs misent sur des réactions rapides.
- ☐ Vérifiez la source et soyez toujours vigilant quant aux demandes de renseignements personnels. Votre banque ne vous contactera jamais par courriel ou par téléphone pour vous demander de divulguer des renseignements personnels comme votre mot de passe, votre code d’accès à usage unique ou votre numéro de carte de crédit. Cliquez ici pour consulter : Ce que RBC ne vous demandera jamais.
- ☐ Ne fournissez aucun renseignement sur votre compte Banque en direct à quiconque vous appelle. Cela comprend les renseignements comme les mots de passe de Banque en direct, les réponses aux questions de sécurité, les justificatifs d’ouverture de session ou le NIP de votre carte-client ou carte de crédit.
- ☐ Supprimez immédiatement le courriel ou le texto. Supprimez immédiatement tout message que vous jugez indésirable. Vous pouvez nous aider en nous envoyant le courriel d’hameçonnage à l’adresse phishing@rbc.com ou en joignant une saisie d’écran d’un message texte frauduleux à un courriel que vous enverrez à la même adresse.

Soyez cyberfuté RBC
rbc.com/cyberfute