FRAUDE ET CYBERCRIMINALITÉ

Faits intéressants
pour votre entreprise

3 cyberattaques courantes ciblant les entreprises

Hameçonnage/hameçonnage ciblé

L'hameçonnage consiste à envoyer des courriels dont l'auteur prétend être une entreprise réputée afin de tromper les gens en leur demandant de révéler des renseignements personnels, comme des mots de passe et des numéros de carte de crédit. L'auteur d'un hameçonnage demande souvent aux utilisateurs d'entrer des renseignements personnels sur un faux site Web qui correspond à la présentation d'un site légitime.

Ordre de virement frauduleux

Un ordre de virement frauduleux se produit lorsqu'un fraudeur envoie un message à sa victime qui semble provenir d'une source connue de l'entreprise. Le courriel présente une demande apparemment légitime, comme le partage de renseignements financiers pour traiter une demande de paiement.

Logiciel malveillant

Un logiciel malveillant est installé sur un appareil, généralement dans le but de recueillir des renseignements permettant d'identifier une personne et des justificatifs d'identification (nom d'utilisateur, mot de passe) des victimes, qui peuvent ensuite être utilisés pour commettre une fraude.

BMO

Unité Crime financier de BMO – Établir un nouveau point de référence en matière de sécurité financière.
Pour en apprendre davantage, consultez le site bmo.com/securite.

04/21-0720-ACC