Cybersécurité : fraudes par courriel

Nous recevons tous des messages de courriel indésirables. Achetez ceci! Cliquez ici! Économisez cela! Ces messages sont assez faciles à distinguer dans la plupart des cas, mais les forces de l'ordre indiquent que, pour chaque million de messages de pourriel envoyés, on dénombre huit personnes en moyenne qui se laissent berner. Comme l'envoi du pourriel ne coûte quasiment rien, c'est rentable pour les malfaiteurs!

Comme toute autre entreprise, cependant, les malfaiteurs cherchent toujours à améliorer leur rentabilité. C'est comme cela qu'on se retrouve avec des fraudes ciblant tout particulièrement les entreprises, fraudes qui sont aussi appelées « Business Email Compromises » par le FBI.

Il s'agit de messages de courriel envoyés par des criminels qui sont conçus pour sembler provenir du P.-D.G., d'un autre dirigeant ou d'un membre du conseil d'administration de l'entreprise. Le but est de faire croire à l'employé (généralement au département de la comptabilité ou des ressources humaines) qu'il a l'ordre de faire un virement ou de fournir des renseignements fiscaux confidentiels sur les employés.

Il existe d'innombrables variantes de ce type de fraude. Au Canada atlantique, l'une des versions qui ont récemment fait le tour des entreprises envoyait des messages aux employés leur demandant de se procurer des cartes-cadeaux au nom du P.-D.G. Les messages étaient souvent présentés en disant que le P.-D.G. était sur le point de se rendre à une réunion importante et en demandant à l'employé de ne pas le déranger.

Dans l'un des cas dont j'ai eu connaissance, le message de courriel a été envoyé à des employés bien particuliers de l'entreprise quelques semaines avant Noël. Selon le message, le P.-D.G. s'apprêtait à aller en réunion et voulait que l'employé aille en secret dans un magasin pour acheter des cartes-cadeaux d'Amazon, à raison de 15 cartes d'une valeur de 100 dollars chacune, qui étaient destinées à être offertes aux employés en guise de prime de fin d'année.

Malheureusement, l'un des employés concernés est tombé dans le panneau et n'a pris conscience de son erreur que lorsque le fraudeur lui a demandé de gratter le dos des cartes et de lui envoyer les numéros par courriel, pour que le P.-D.G. puisse envoyer ces « primes de Noël ». L'employé a alors appelé le patron pour vérifier qu'il lui envoyait bien les bons numéros. Il a découvert que la demande était frauduleuse et a ainsi perdu 1500 dollars.

Cela aurait pu être pire. L'Université MacEwan d'Edmonton a ainsi perdu 11,8 millions de dollars quand l'un de ses employés s'est laissé berner. Les forces de l'ordre indiquent qu'il existe de nombreuses variantes de cette forme de fraude, qui ont permis aux malfaiteurs de récupérer 2,3 milliards de dollars au total environ — et ce ne sont là que les pertes qui ont été signalées. Certains spécialistes estiment que le montant réel des pertes pourrait s'élever à jusqu'à 26 milliards de dollars.

La prévention est essentielle dans la lutte contre la cybercriminalité. Assurez-vous que vos employés sont au courant de telles menaces et sont vigilants. Mettez en place une politique selon laquelle l'employé doit appeler l'expéditeur apparent du message de courriel, sans exception, AVANT de virer les fonds ou d'envoyer les informations sensibles. Sinon, votre organisation risque d'être à son tour victime d'une telle fraude!

Scott Beck est P.-D.G. de l'entreprise BeckTek de Moncton (Nouveau-Brunswick), qui est une entreprise en pleine croissance dans le domaine de la cybersécurité et des services de TI. Il est l'auteur de deux livres qui ont atteint le sommet des ventes à l'échelle internationale et il est également un conférencier primé, avec des présentations au NASDAQ et au Harvard Club of Boston. Il est l'une des vedettes du documentaire Cyber Crime *sur Amazon Prime et est souvent invité à s'exprimer sur NBC, ABC, FOX et Global.*