SCÉNARIO DE RÉCLAMATION

Escroquerie portant sur un chef de la direction

Une entreprise manufacturière transfère des milliers de dollars à des escrocs après avoir succombé à une fraude portant sur son chef de la direction

VICTOR

L'ingénierie sociale consiste à utiliser la tromperie pour manipuler des personnes afin qu'elles accomplissent un acte particulier, comme transférer de l'argent, communiquer des informations confidentielles ou cliquer sur un lien malveillant, et elle cause de graves préjudices financiers aux entreprises du monde entier.

L'un des types d'ingénierie sociale les plus courants est la fraude portant sur le chef de la direction. Il s'agit généralement d'une attaque ciblée au cours de laquelle un fraudeur se fait passer pour le chef de la direction ou un autre cadre supérieur de l'organisation et demande à un membre du département financier d'effectuer un paiement urgent sur un compte particulier pour une raison précise. Le plus souvent, le chef de la direction ou le cadre supérieur en question aura vu son compte de courriels compromis, mais il n'est même pas nécessaire qu'il soit piraté pour que ce type de fraude soit réalisé. Certains fraudeurs se basent sur des informations accessibles au public, découvrant l'adresse électronique du chef de la direction et la modifiant légèrement avant de cibler un employé débutant du département financier, souvent inexpérimenté et désireux d'impressionner ses supérieurs. De nombreux fraudeurs surveillent les sites de médias sociaux et LinkedIn pour savoir quand le chef de la direction ou le cadre supérieur est absent du bureau afin de réduire la probabilité que leur escroquerie soit découverte.

Toute entreprise qui transfère des fonds par voie électronique peut être exposée à des pertes de cette nature. L'un des assurés touchés par un cas de fraude portant sur le chef de la direction était une entreprise manufacturière spécialisée dans la fabrication de machines utilisées dans l'industrie textile. Dans le cadre de ses activités commerciales, l'entreprise utilisait les services d'un certain nombre de fabricants sous contrat qui produisent et fournissent des composants spécifiques utilisés dans les processus de fabrication de l'entreprise.

L’hameçonnage d’identifiants conduit à l’infiltration des boîtes de réception

L’escroquerie a commencé lorsque le chef de la direction s’est laissé prendre au piège d’un courriel d’hameçonnage d’identifiants. **Les courriels d’hameçonnage d’identifiants sont utilisés par des acteurs malveillants pour tenter d’inciter les personnes à communiquer volontairement leurs données de connexion**, généralement en les dirigeant vers un lien qui les conduit à une fausse page de connexion. Dans le présent cas, le chef de la direction a reçu un courriel de ce qu’il pensait être Microsoft. Le courriel indiquait que les détails de son compte devaient être validés afin qu’il puisse continuer à utiliser le service Outlook sans interruption. Comme le courriel semblait provenir d’une source légitime, le chef de la direction a cliqué sur le lien. Le lien l’a conduit à une page de renvoi apparemment légitime, où il a saisi ses données de connexion à ses courriels. Supposant que son compte avait été validé, **le chef de la direction n’a pas réfléchi davantage à l’incident**. Cependant, en saisissant ses informations d’identification sur cette page de connexion, il avait en fait transmis ses coordonnées à un fraudeur qui pouvait désormais accéder à son compte.

En accédant au compte de courriels du chef de la direction, le fraudeur a pu recueillir des informations précieuses sur la manière dont les paiements de factures étaient traités dans cette entreprise. Par exemple, **cela a permis au fraudeur de jeter un coup d’œil aux factures précédentes** qui avaient été envoyées par les fabricants et les fournisseurs sous contrat de l’assuré, et d’identifier la principale personne du département financier de l’assuré responsable du paiement des factures et de l’autorisation des demandes de virement. De plus, cela a également permis au fraudeur d’accéder au calendrier Outlook du chef de la direction et de déterminer son emploi du temps au cours d’une journée de travail donnée.

Après avoir pris connaissance de l’emploi du temps du chef de la direction en fonction de son calendrier, le fraudeur a attendu que le chef de la direction soit en voyage d’affaires à l’étranger pendant quelques semaines. Le chef de la direction étant absent du bureau et les chances de découvrir l’escroquerie étant très réduites, le fraudeur a choisi ce moment pour frapper.

Le plan du fraudeur consistait à se faire passer pour un membre du service comptable de l’un des fabricants sous contrat de l’assuré.

La première étape du fraudeur a été de mettre en place des règles de redirection dans le compte de courriels du chef de la direction. Les règles de redirection sont des paramètres qui peuvent être appliqués à un compte de courriels et qui garantissent que les courriels qui répondent à un critère donné sont automatiquement transférés vers un dossier spécifique ou vers un autre compte de courriels. Dans ce cas, **le fraudeur a mis en place deux règles pour s’assurer que le chef de la direction ne tombe sur aucun des courriels liés à l’escroquerie** alors qu’il était en déplacement. La première règle créée signifiait que tous les courriels de la personne responsable de l’approbation des paiements étaient immédiatement marqués comme lus et envoyés directement dans le dossier des éléments supprimés du compte.

La deuxième règle signifiait que tout courriel comportant un mot clé, tel que « facture » ou des mots utilisés dans le nom commercial de ce fabricant sous contrat particulier, dans la ligne d’objet était marqué comme lu et automatiquement envoyé dans le dossier des éléments supprimés.

Des factures fictives entraînent des pertes de fonds irrécupérables

Une fois le travail préparatoire effectué, le fraudeur a envoyé un courriel au chef de la direction, prétendant provenir du service comptable du fabricant sous contrat, en joignant une facture de 47 500 $ et en expliquant qu'il y avait eu un changement dans les détails du compte. Pour ajouter un air d'authenticité à l'escroquerie, le fraudeur a utilisé l'une des **factures réelles du fabricant sous contrat comme modèle**. La facture avait donc l'air normale; le logo et l'adresse du fabricant sous contrat figuraient dans l'en-tête de la facture, et un aperçu des travaux effectués y était indiqué. La seule différence était que les détails du compte avaient été modifiés par le fraudeur. En raison des règles de redirection en vigueur, ce courriel a été immédiatement marqué comme lu et envoyé dans le dossier des éléments supprimés. Le fraudeur s'est ensuite connecté au compte du chef de la direction et, se faisant passer pour lui, a transmis ce courriel à la personne du département financier responsable d'autoriser les paiements et a demandé que le paiement soit effectué le jour même. **Comme le chef de la direction n'était pas au bureau et que le courriel demandant le paiement de la facture provenait de son compte, l'employé du département financier a supposé qu'il s'agissait d'une demande légitime** et a dûment payé la facture.

Ayant constaté que cette ruse avait fonctionné, le fraudeur a décidé de tenter sa chance et a envoyé une autre facture quelques jours plus tard.

À cette occasion, étant donné que la dernière facture n'avait été payée que depuis quelques jours, l'employé du département financier a répondu au chef de la direction au sujet de la demande pour confirmer son exactitude. Toutefois, en raison des règles de redirection mises en place, le chef de la direction n'a pas eu connaissance de la réponse de l'employé – seul le fraudeur était au courant. En se faisant passer pour le chef de la direction, le fraudeur a répondu et expliqué que tout était en ordre, et que la facture devait être payée.

L'employé du département financier croyant sincèrement qu'il était en correspondance avec le chef de la direction et ayant reçu une réponse rapide à toute objection ou question concernant les paiements, **le fraudeur a réussi à faire approuver deux autres factures**, portant le montant total payé à 190 000 $. Ce n'est qu'au retour du chef de la direction au bureau que les paiements ont fait l'objet d'une discussion et que l'escroquerie a été découverte. L'assuré a signalé l'incident à la police locale et a tenté de récupérer les fonds auprès de la banque destinataire, mais tout l'argent avait été transféré hors du compte frauduleux, et les chances de réussite du recouvrement ont été jugées faibles. Heureusement pour l'assuré, il avait souscrit une couverture contre la cybercriminalité dans le cadre de sa police d'assurance contre les cyber-risques de Victor et a pu récupérer l'intégralité de la perte.

Notre meilleure défense contre l'augmentation des escroqueries portant sur un chef de la direction

Cette réclamation met en évidence quelques points essentiels. Tout d'abord, **elle illustre comment les chefs de la direction et les cadres supérieurs sont des cibles de choix pour les cybercriminels**. Les chefs de la direction et les cadres supérieurs sont généralement le visage de leurs entreprises respectives et, par conséquent, ils ont tendance à avoir des profils plus importants sur les sites Web de l'entreprise et les comptes de médias sociaux, ce qui permet aux cybercriminels de recueillir des informations précieuses sur eux. En outre, les cybercriminels savent que les employés sont instinctivement moins susceptibles de poser des questions et plus susceptibles d'agir en fonction des instructions des cadres supérieurs. Les chefs de la direction et les cadres supérieurs doivent donc être particulièrement attentifs à respecter les bonnes pratiques en matière de cybersécurité, et **les employés doivent être particulièrement attentifs aux courriels suspects provenant de cadres supérieurs** et mettre en place de solides procédures de contrôle et d'authentification.

Deuxièmement, la réclamation montre que les cybercriminels deviennent beaucoup plus sophistiqués. Par le passé, il n'était pas rare de voir des tentatives flagrantes de fraude consistant en un transfert de fonds par courriel, avec un appel à l'aide urgent ou des prix fictifs à gagner, pour ne citer que deux exemples. **Aujourd'hui, cependant, nous assistons à des attaques beaucoup plus nuancées.** Dans le présent cas, le fraudeur a réussi à inciter le chef de la direction à donner volontairement ses identifiants de connexion aux courriels, à identifier la personne responsable d'autoriser les paiements et à savoir quand le chef de la direction serait absent du bureau pour un voyage d'affaires. Il a également mis en place des règles de redirection dans la boîte de réception du chef de la direction pour éviter d'être détecté et a utilisé l'un des modèles de facture réel du fabricant sous contrat de l'assuré pour ajouter de l'authenticité à l'escroquerie.

Enfin, cette réclamation discrédite également l'une des objections les plus courantes des organisations à l'achat d'une assurance contre les cyber-risques : à savoir qu'en investissant massivement dans la sécurité informatique, elles n'ont pas besoin d'assurance contre les cyber-risques. **Le fait est que la grande majorité des incidents cybernétiques sont le résultat d'une erreur humaine.** Avec l'augmentation des attaques de plus en plus sophistiquées de ce type, il est très difficile pour les employés de faire la différence entre

un vrai courriel et un faux courriel, ou une vraie facture ou une fausse facture. En outre, les transactions financières étant de plus en plus souvent effectuées par voie électronique, les possibilités de vol de ces fonds par les cybercriminels n'ont jamais été aussi nombreuses. La mise en place d'une bonne formation et de procédures d'authentification peut certainement contribuer à réduire le risque qu'un tel événement se produise, mais **il est impossible pour une entreprise d'être totalement imperméable à ce type d'attaques**. C'est pourquoi l'assurance contre les cyber-risques devrait faire partie du programme de gestion des risques de toute organisation prudente, car elle constitue un précieux filet de sécurité si le pire devait se produire.

Visitez assurancevictor.ca/cyber pour en apprendre davantage.