La cybercriminalité, un business très lucratif

La fraude frappe de plus en plus d'entreprises

L'époque où des bandes d'escrocs opéraient au moyen d'e-mails de phishing (ou hameçonnage) amateurs, dans un français très approximatif, est bien révolue. La fraude est aujourd'hui devenue une affaire de très gros sous. De plus, les escrocs rivalisent d'imagination et inventent constamment de nouvelles techniques pour abuser de leurs victimes plutôt crédules. Hilde Pottie, du Fraud Competence Center de Belfius, nous guide dans les eaux troubles du monde de la fraude et nous donne des conseils pratiques pour protéger au mieux nos entreprises.

Piratage de la boîte électronique

«Le terme est sans équivoque : cette technique consiste à pirater la boîte électronique des contreparties ou des fournisseurs, de sorte que des entreprises reçoivent des e-mails qui, de prime abord, semblent provenir de leurs fournisseurs, mais qui sont, en réalité, des faux. Il peut s'agir d'une facture – fausse, naturellement – jointe à l'e-mail, ou d'un message indiquant que les factures fournisseurs seront désormais encaissées par une société d'affacturage. Un nouveau numéro de compte est communiqué, généralement détenu à l'étranger», explique Hilde.

«Il arrive aussi que des boîtes électroniques soient tout simplement imitées. L'expéditeur devient subitement Jean Dupond au lieu de Dupont. Ou bien la lettre minuscule 'l' (de Lima) est remplacée, dans le nom d'une entreprise, par la lettre majuscule 'i', une substitution que l'on ne peut déceler à l'écran.»

Facturation frauduleuse

«Il existe essentiellement deux types de facturation frauduleuse: soit une facture électronique arrive par le biais d'une boîte électronique piratée (voir aussi le passage sur le «piratage de la boîte électronique», ndlr), soit une facture papier est interceptée au cours du parcours postal», poursuit Hilde. «Ensuite, des informations de la facture sont modifiées ou la facture est simplement entièrement imitée. Le problème avec la facturation frauduleuse, c'est qu'il faut souvent des semaines avant de se rendre compte de l'escroquerie. Le client pense qu'il a correctement payé la facture, tandis que le bénéficiaire continue d'attendre l'argent. Au moment où la fraude est établie, il est généralement trop tard pour récupérer l'argent.»

QUE FAIRE?

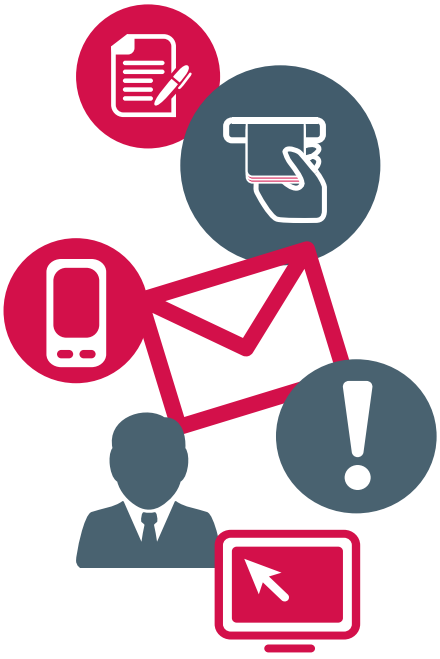
Idéalement, chaque entreprise doit disposer d'une liste de toutes ses contreparties, mentionnant toutes les personnes de contact, avec leur numéro de téléphone et leur numéro de compte. Chaque facture payée peut alors être validée au moyen de cette liste. Autre possibilité: si vous effectuez vos paiements en ligne, vous pouvez travailler avec vos «bénéficiaires sauvegardés». Vous remarquerez alors immédiatement si un fournisseur souhaite soudainement être payé sur un autre compte. Si le numéro de compte du bénéficiaire est différent, prenez alors contact avec la contrepartie en utilisant les informations de la liste générale, et non les données qui figurent sur la facture douteuse.

Ingénierie sociale

«La fraude au CEO est l'exemple le plus célèbre d'ingénierie sociale. Dans cette situation, des collaborateurs d'une entreprise sont d'abord approchés par un fraudeur usurpant l'identité d'une personne de confiance du CEO ou du CFO. Souvent, les fraudeurs se font passer, dans ces premiers contacts, pour avocat, un consultant ou un notaire. Suit un e-mail frauduleux exigeant l'exécution d'un paiement urgent et confidentiel, prétendument sur demande du CEO ou du CFO. L'argent part souvent vers des comptes à l'étranger et les fraudeurs disparaissent dans la nature.»

QUE FAIRE?

Informez votre personnel de cette technique de fraude et indiquez clairement que vous ne demanderez jamais par e-mail ou par téléphone d'exécuter une transaction urgente et confidentielle. Élaborez un protocole clair pour les paiements urgents et respectez-le toujours de manière cohérente. Convenez, par exemple, d'un code que vous n'utiliserez que dans ces situations. De plus, assurez-vous que toutes les transactions (importantes) soient validées par deux signatures. Quatre yeux en voient toujours plus que deux.



Fraude interne

Dans le cas de la fraude interne, la menace ne vient pas de l'extérieur, mais de l'intérieur de l'entreprise. «Ce sont souvent les cas les plus difficiles à détecter et à résoudre», explique encore Hilde. «Un exemple classique, malheureusement encore trop fréquent: un collaborateur autorisé à accéder aux comptes de l'entreprise abuse de son pouvoir en détournant de temps à autre de l'argent vers ses comptes privés ou des comptes d'amis et de membres de sa famille.»

QUE FAIRE?

Établissez des procédures internes claires, car les bons accords font les bons amis. La règle de la double signature pour les gros montants n'est certainement pas un luxe superflu. Procédez régulièrement à un audit interne et faites savoir à votre personnel, à des fins de dissuasion, que des contrôles sont prévus.

Phish a card

«Dans le domaine du phishing, les fraudeurs changent en permanence de terrain de jeu. Citons ainsi le phishing de cartes bancaires : des clients reçoivent un message leur annonçant que leur carte bancaire arrive bientôt à échéance et qu'ils doivent se connecter, à partir de leur PC, pour saisir certaines informations, dont leur code PIN. Ils sont ensuite invités à envoyer leur carte à une adresse donnée. De cette façon, les phishers disposent à la fois de la carte et du code, ce qui leur permet de piller des comptes en toute facilité», déclare Hilde.

QUE FAIRE?

Ne vous laissez pas duper: les banques ne vous demanderont jamais d'envoyer votre carte bancaire et de saisir simultanément votre code PIN en ligne. En cas de doute, prenez contact avec votre interlocuteur à la banque, en passant par les canaux habituels. Veillez à tenir vos collaborateurs informés de ces pratiques de phishing.

Fraude «boiler room»

«Avec ce type de fraude, les escrocs visent essentiellement les dirigeants d'entreprise ou les directeurs financiers sur le plan privé. Les CEO ou CFO sont généralement approchés depuis l'étranger par de soi-disant experts qui leur proposent des investissements relativement complexes avec de bien meilleurs rendements que ceux des banques belges», raconte Hilde.

«Les fraudeurs sont loin d'être des amateurs: ils maîtrisent le jargon financier à la perfection et semblent particulièrement professionnels. Ils disposent de beaux sites web, de brochures sur papier glacé et de scripts à toute épreuve pour leurs contacts téléphoniques. Les victimes transfèrent assez rapidement des fonds à l'étranger, aveuglés par le rendement potentiel qu'on leur a fait miroiter et rassurés par un récit plausible. Au départ, on parle de quelques milliers d'euros, mais la machine s'emballe assez vite. À votre insu, vous avez été délesté de sommes phénoménales, sans même vous être rendu compte que vous avez été escroqué. Ce n'est qu'au moment où le client veut récupérer une partie de son argent pour financer un achat important que tout contact est rompu et que l'argent est parti en fumée.»

QUE FAIRE?

Ne soyez pas trop crédule. Une histoire vous semble-t-elle trop belle pour être vraie? C'est sans doute qu'elle ne l'est pas.

Vous vous êtes malgré tout laissé prendre au piège? Parlez-en avec votre interlocuteur habituel à la banque et ne publiez pas votre histoire en ligne. Les fraudeurs aussi surfent sur Internet. On connaît des cas de recovery fraud : des bandes d'escrocs proposent leur «aide» en ligne pour vous aider à récupérer une partie de l'argent perdu. Tout ce que le client doit faire, c'est virer d'avance un montant donné pour couvrir une partie des frais. Résultat : les fraudeurs doublent leurs gains et les victimes sont confrontées à un casse-tête financier encore plus complexe.

VOUS AVEZ MALGRÉ TOUT ÉTÉ VICTIME DE FRAUDE?

1. Prenez immédiatement contact avec votre interlocuteur habituel à la banque et communiquez-lui autant de détails que possible sur ce qui vous est arrivé. De cette façon, notre Fraud Competence Center peut essayer de récupérer (une partie de) l'argent.

2. Rendez-vous immédiatement à la police pour faire dresser un procès-verbal. Si vous voulez récupérer l'argent plus tard, vous aurez besoin d'un PV officiel pour pouvoir prouver qu'une fraude a effectivement eu lieu.

Comment éviter ces mauvaises surprises à l'avenir ?

Parlez-en avec votre Corporate Banker! Belfius dispose de nombreux produits et services proposant des solutions pour la lutte contre la fraude. Vous les découvrirez dans notre dossier *Vos opérations bancaires en toute sécurité*.

ET VOUS?

Participez à notre enquête anonyme (3 questions seulement) en cliquant ici et dites-nous si avez déjà été victime de certaines fraudes / tentatives de fraudes.