La Newsletter mensuelle de Sensibilisation à la Sécurité destinée aux utilisateurs informatiques

Fraude au Président / E-mails d'imposteurs

Qu'est-ce que la Fraude au Président / Emails d'imposteurs ?

Les cyber attaquants continuent à développer une attaque par courrier électronique appelée la Fraude au Président ou Emails d'imposteurs. Il s'agit d'attaques par courrier électronique ciblées qui amènent leurs victimes à prendre des mesures qu'elles ne devraient pas prendre. Dans la plupart des cas, les criminels cherchent à gagner de l'argent. Ces attaques sont considérées comme dangereuses car les cybercriminels effectuent des recherches sur leurs victimes avant de lancer leur attaque. Il est également très difficile pour les technologies de sécurité d'arrêter ces attaques car il n'y a pas de pièces jointes infectées ou de liens malveillants à détecter. Voici comment fonctionne l'attaque.

Le cyber-attaquant utilise Internet pour rechercher la victime ciblée et les personnes avec lesquelles sa victime interagit. Par exemple, s'il vous cible, il recherche qui est votre patron au travail ou peut-être un agent immobilier avec lequel vous travaillez. Le cyber-attaquant crée alors un courrier électronique, prétendant être l'une de ces personnes et vous l'envoie. L'email semble urgent, vous obligeant à agir immédiatement, par exemple en traitant une facture, en changeant le nom de la personne avec laquelle vous effectuez un paiement ou en vous convainquant de répondre avec des documents sensibles. Le courrier électronique fonctionne en vous invitant à faire ce qu'il veut. Voici deux exemples de la façon dont une telle attaque pourrait fonctionner.

Virement bancaire: un cybercriminel cherche à gagner de l'argent. Il effectue des recherches sur l'entreprise pour laquelle vous travaillez, en identifiant par exemple qui travaille dans les comptes fournisseurs ou toute personne responsable du transfert de fonds. Le criminel conçoit et envoie un courriel à ces personnes en prétendant être leur patron ou un cadre supérieur. L'email leur indique qu'il y a une urgence et que l'argent doit être transféré immédiatement sur un nouveau compte bancaire. Le courrier électronique les pousse à commettre une erreur. En réalité, ils envoient de l'argent au cybercriminel.

Fraude fiscale: les cybercriminels recherchent des informations personnelles à utiliser en cas de fraude fiscale. Un des moyens les plus rapides de les obtenir est de voler les informations de tous les employés d'une entreprise. Les cybercriminels recherchent et identifient qui travaille dans le département des ressources humaines. Ils envoient ensuite de faux courriels à ces personnes, prétendant être un cadre supérieur ou peut-être une personne juridique. Les emails créent une situation urgente, spécifiant que les informations fiscales sur tous les employés doivent être soumises immédiatement. Les membres des ressources humaines pensent qu'ils envoient les documents sensibles au cadre supérieur, alors qu'en réalité ils les envoient à un cybercriminel.

Se protéger

Alors que pouvez-vous faire pour vous protéger? Le bon sens est votre meilleure défense. Voici les indices les plus courants à surveiller :

- **Le courrier électronique est très court et urgent (souvent quelques phrases seulement) et la signature indique que le courrier électronique a été envoyé depuis un appareil mobile.**
- **Il y a un fort sentiment d'urgence, qui vous pousse à ignorer ou à contourner les politiques de votre employeur. Suivez toujours les politiques et procédures de votre entreprise, même si le courriel semble provenir de votre patron ou même du PDG de votre société.**
- **Le courrier électronique est lié au travail, mais utilise une adresse électronique personnelle, telle que @ gmail.com ou @ hotmail.com.**
- **Le courrier électronique semble provenir d'un dirigeant, d'un collègue ou d'un fournisseur que vous connaissez ou avec lequel vous travaillez, mais le ton du message ne sonne pas comme les emails qu'ils ont l'habitude de vous envoyer.**
- **Les instructions de paiement sont fournies et ces instructions diffèrent de celles que vous avez déjà reçues, telle que la demande de paiement immédiat sur un autre compte bancaire.**

Si vous pensez avoir été ciblé, arrêtez toute interaction avec l'attaquant et signalez-le à votre superviseur. Si vous avez été ciblé à la maison ou si vous avez été victime et qu'un virement électronique a été effectué, signalez-le immédiatement à votre banque, puis à la police.

Version Française

La société Pélissier & Partners spécialiste en Intelligence économique a été fondée sur une expérience de plus de quinze ans dans le domaine de la recherche d'information et de la cybersécurité dédiées aux dirigeants d'entreprises suisses.

Editeur invité

Don Cavender *est un ancien agent spécial du FBI, avec plus de 22 années d'expérience en criminalistique numérique et en cybercriminalité. Il a plus récemment ciblé les organisations de cybercriminalité en tant que coordinateur du BEC (Business E-mail Compromise) à Washington DC. Il dispense des formations et mène des recherches en criminalistique numérique et en cyber-enquêtes.* @don_cavender https://www.linkedin.com/in/donald-cavender

Sources

Ingénierie sociale :	https://www.sans.org/u/HE3
Stop au phishing :	https://www.sans.org/u/HE8
Arrêtez les logiciels malveillants :	https://www.sans.org/u/HEd
Verrouillez votre connexion :	https://www.sans.org/u/HEi

Comité de rédaction : Walt Scrivens, Phil Hoffman, Cathy Click, Cheryl Conley | Traduit par : Marilyn Combet