OUCH! Juillet 2024

Votre bulletin mensuel sur la sensibilisation à la sécurité

Attaques par SMS : la saga du smishing

Marc est resté perplexe face au message, un avis de livraison de colis d'Amazon : "Tentative de livraison manquée ! Cliquez sur le lien pour reprogrammer ou votre colis vous sera renvoyé". Marc ne se souvenait pas d'avoir commandé quelque chose en ligne récemment, mais il commandait tellement de choses en ligne qu'il était facile d'oublier. Ne voulant rater aucun colis, il a cliqué sur le lien et une page s'est affichée, lui demandant ses coordonnées "pour assurer une reprogrammation correcte". Le message semblait un peu étrange, mais Marc s'est dit qu'il valait mieux prévenir que guérir. Il a saisi les détails de son adresse personnelle et s'est vu demander des informations supplémentaires, y compris les données de sa carte de crédit. Faisant confiance à l'entreprise, il a fait tout ce qu'elle lui demandait pour assurer la livraison. La page a ensuite indiqué que son colis devrait être livré sous peu. Dans les quinze minutes qui ont suivi, Marc a reçu un appel téléphonique de la société de gestion de sa carte de crédit l'informant que sa carte avait été utilisée pour effectuer de nombreux prélèvements en ligne dans le monde entier. Mark s'est figé en réalisant qu'il n'y avait pas de colis et que le SMS était une escroquerie visant à lui soutirer toutes ses informations, y compris sa carte de crédit.

Quelles sont les attaques de smishing

Les attaques par messages, également appelées Smishing (combinaison des mots SMS et Phishing), se produisent lorsque des cyber-attaquants utilisent des SMS, des textos ou des technologies de messagerie similaires pour vous inciter à faire une action que vous ne devriez pas faire, comme donner le mot de passe de votre carte de crédit ou de votre compte bancaire ou installer une fausse application mobile. Tout comme dans les attaques de phishing par courriel, les cybercriminels jouent souvent sur vos émotions, en créant par exemple un sentiment d'urgence ou de curiosité. Cependant, ce qui rend les attaques par messages si dangereuses, c'est qu'elles contiennent beaucoup moins d'indices qu'un e-mail par exemple, ce qui rend beaucoup plus difficile pour vous de détecter que quelque chose ne va pas.

Parfois, les cybercriminels combinent même les attaques téléphoniques avec les attaques par messages. Par exemple, vous pouvez recevoir un message urgent de votre banque vous demandant si vous avez autorisé un paiement inhabituel. Le message vous demande de répondre OUI ou NON pour confirmer le paiement. Si vous répondez, le cybercriminel sait maintenant que vous êtes intéressé et il vous appellera en se faisant passer pour le service de fraude de la banque. Il essaiera ensuite de vous soutirer des informations financières et des données relatives à votre carte de crédit, voire le nom d'utilisateur et le mot de passe de votre compte bancaire.

Repérer et arrêter ces attaques

Voici les indices les plus fréquents d'une attaque :

- **L'urgence** : tout message qui crée un énorme sentiment d'urgence, lorsque quelqu'un tente de vous presser ou de faire pression sur vous pour que vous preniez une mesure, par exemple en affirmant que vos comptes seront fermés ou que vous irez en prison.
- **L'avidité** : lemessage semble-t-il trop beau pour être vrai ? Non, vous n'avez pas gagné un nouvel Iphone gratuitement.
- **La curiosité** : si vous recevez un message qui ressemble à l'équivalentd'un "faux numéro" ou à une personne que vous ne connaissez pas qui vous dit simplement "bonjour", n'y répondez pas et n'essayez pas de contacter l'expéditeur ; contentez-vous de le supprimer. Il s'agit de tentatives de cybercriminels d'entamer une conversation avec vous, comme les arnaques à la romance.
- **Informations personnelles** : le message vous renvoie-t-il vers des sites web vous demandant vos informations personnelles, votre carte de crédit, vos mots de passe ou d'autres informations sensibles auxquelles ils ne devraient pas avoir accès ?
- **Les paiments** : méfiez-vous des demandes de paiement inhabituelles, comme l'envoi d'argent par Western Union ou Bitcoin.

Si vous recevez un SMS d'une organisation officielle qui vous semble légitime, rappelez-la directement. Toutefois, n'utilisez pas le numéro de téléphone figurant dans le message, mais plutôt un numéro de téléphone de confiance. Par exemple, si vous recevez un SMS de votre banque vous indiquant qu'il y a un problème avec votre compte ou votre carte de crédit, obtenez un numéro de téléphone de confiance en visitant le site web de votre banque, trouvez le numéro de téléphone sur un relevé de facturation ou au dos de votre carte bancaire ou de crédit, puis appelez en utilisant ce numéro. N'oubliez pas non plus que la plupart des organismes publics, tels que les services fiscaux ou les services répressifs, ne vous contacteront jamais par SMS, mais uniquement par e-mail.

Lorsqu'il s'agit d'attaques par Smishing basées sur des messages, vous êtes votre meilleure défense.

Rédacteur Invité

Destiney Plaza est ingénieur en cybersécurité à l'Institut de génie logiciel de l'université Carnegie Mellon. Elle aime inspirer en donnant des conférences à des publics divers, allant des débutants aux professionnels de la cybersécurité. Elle est titulaire d'un CISSP, d'une licence en informatique et d'une maîtrise en systèmes d'information de gestion.

Ressources

Messages à faire et à ne pas faire :
https://www.sans.org/newsletters/ouch/messaging-dos-and-donts/
Stop aux appels téléphoniques frauduleux : https://www.sans.org/newsletters/ouch/stop-phone-call-scams/
Déclencheurs émotionnels, comment les cyber-attaquants vous piègent-ils ? :
https://www.sans.org/newsletters/ouch/emotional-triggers-how-cyber-attackers-trick-you/

Traduit pour la communauté par : Juliette Busson