L’escroc par courriel Amazon Prime a perdu

Plus souvent qu’autrement, il est de notre devoir solennel sur ce site de vous tenir informé de la nature et des tactiques des cybercriminels dangereux, rusés et persistants.

Ce n’est pas un de ces jours.

En fait, c’est l’occasion de l’un de ces jours.
Il s’agit d’un spam passable envoyé par un spammeur qui a fait l’équivalent de phishing en arrivant à l’aéroport trois heures plus tôt pour son vol, le lendemain de son départ.

Il s’agit d’un courriel malveillant qui a échoué car, malgré tout ce qu’il a fait, il s’est trompé sur la chose la plus importante, tout en se garantissant un voyage inévitable, rapide et aller simple vers le piège du spam.

Pourtant, il y a de précieuses leçons à tirer de l’échec, et je ne peux pas penser à une meilleure façon d’aggraver la misère du malheureux spammeur que de la transformer en un moment propice à l’apprentissage qui pourrait améliorer la sécurité.

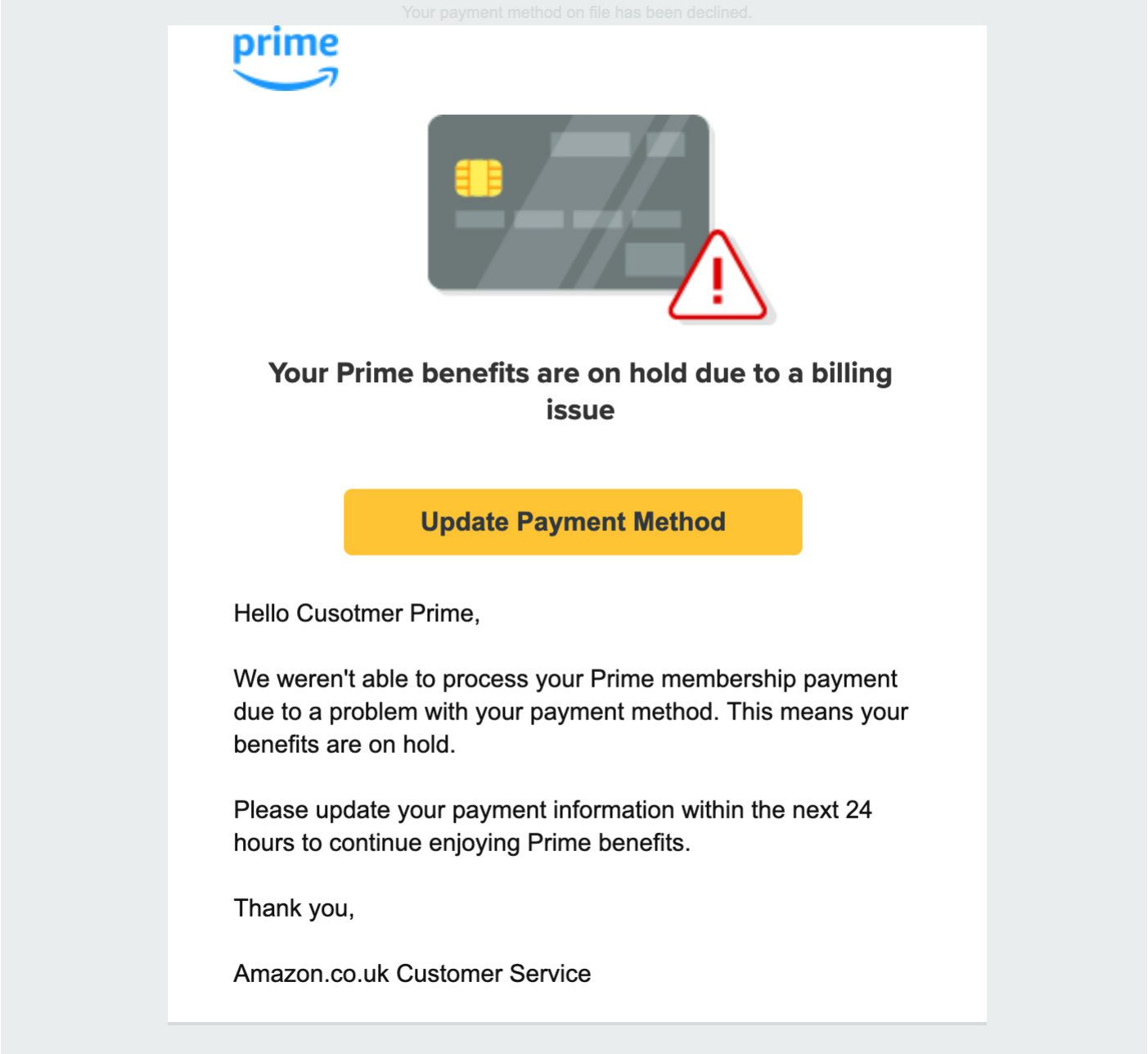
Commençons par ce qui ne s’est pas mal passé.

Ce qui ne s’est pas mal passé

Peu importe comment ils sont habillés, les escroqueries se résument presque toujours à une demande urgente d'argent.
La tâche de l'escroc est de rendre sa prise d'argent à bout de souffle aussi plausible que possible, ce qu'il fait en usurpant l'identité de quelqu'un ou de quelque chose dont vous vous attendez à entendre.

Le plus souvent, cela signifie usurper l'identité de marques familières.
Les escrocs aiment les marques mondiales comme Microsoft, Google, Amazon et UPS parce qu'elles sont immédiatement reconnaissables, que leurs logos et leur style sont faciles à copier et que les gens sont habitués à recevoir des courriels de leur part.

Dans ce cas, la demande urgente d'argent est venue enveloppée dans un emballage Amazon, prétendant que mes avantages Prime étaient en attente en raison d'un problème de facturation, avec 24 heures pour résoudre en mettant à jour mon mode de paiement.



La prémisse est plausible, les couleurs sont correctes, le logo aussi, et la signature, « Amazon.co.uk service client », m'a correctement placé au Royaume-Uni.

L'escroc a utilisé quelques autres astuces pour rendre l'arnaque plus crédible aussi.

Exceptionnellement, l'adresse « De » du courriel était un courriel amazon.co.uk honnête, plutôt qu'une tentative mignonne de masquer un e-mail non amazonien.
Il est important de noter que cela ne signifie pas que l'escroc a utilisé l'infrastructure Amazon, ou que le courriel a touché Amazon de quelque manière que ce soit - vous pouvez mettre tout ce que vous voulez dans une adresse courriel De.
Il y a une raison pour laquelle les escrocs ont tendance à opter pour des astuces mignonnes, que nous verrons ci-dessous.

Bien sûr, l'e-mail n'est que l'appât, le vol réel des détails de paiement des utilisateurs doit se produire sur un site Web quelque part, et les escrocs ne font pas souvent tourner leur propre infrastructure.
Pour cela, ils détournent plus souvent quelqu'un d'autre.
Le lien Mettre à jour le mode de paiement dans ce courriel renvoie à une page d'administration sur un site appartenant à un constructeur leader de meubles d'autel au Vietnam.

Parce que son adresse peut sembler étrange à un moteur d'analyse de courriels, ou à un destinataire aux yeux d'aigle, le site de meubles est accessible via une redirection ouverte sur la réponse de la Russie à Facebook, VKontakte, qui est un site Web important et bien établi qui ne sonnera pas l'alarme.

Une redirection ouverte est une URL sur un site qui peut être modifiée pour rediriger vers n'importe quelle autre page du Web.
Bien qu'elles soient largement reconnues comme une faille de sécurité indésirable, les redirections ouvertes sont courantes sur les moteurs de recherche et les sites de médias sociaux, qui les utilisent pour suivre les liens sur lesquels vous cliquez, pour le plus grand plaisir des escrocs.

Mis à part le fait qu'il commence par « Cher *Cusotmer* Prime », le courriel regorge de choses qui le rendent crédible.
Avec tous ces ingrédients en place, vous pourriez penser que ce courriel était destiné au succès, mais quand il est arrivé, il a été instantanément et ignominieusement jeté dans le dossier spam.

Ce qui ne s'est pas bien passé

Vous vous souvenez que amazon.co.uk adresse utilisée par l'escroc?
C'est ce qui ne s'est pas bien passé.
Le courriel dans sa forme pure permet à un expéditeur de mettre tout ce qu'il veut dans l'adresse de l'expéditeur, mais avec un peu de travail, les entreprises peuvent s'assurer qu'il y a des conséquences si les escrocs utilisent leurs domaines comme ça.

Amazon a mis en œuvre DMARC (Domain-based Message Authentication, Reporting and Conformance).
Dès que le courrier frauduleux est arrivé, notre infrastructure a vérifié si le courriel avait été signé numériquement par Amazon (ce n'était pas le cas) et si le serveur de l'escroc était autorisé à envoyer des

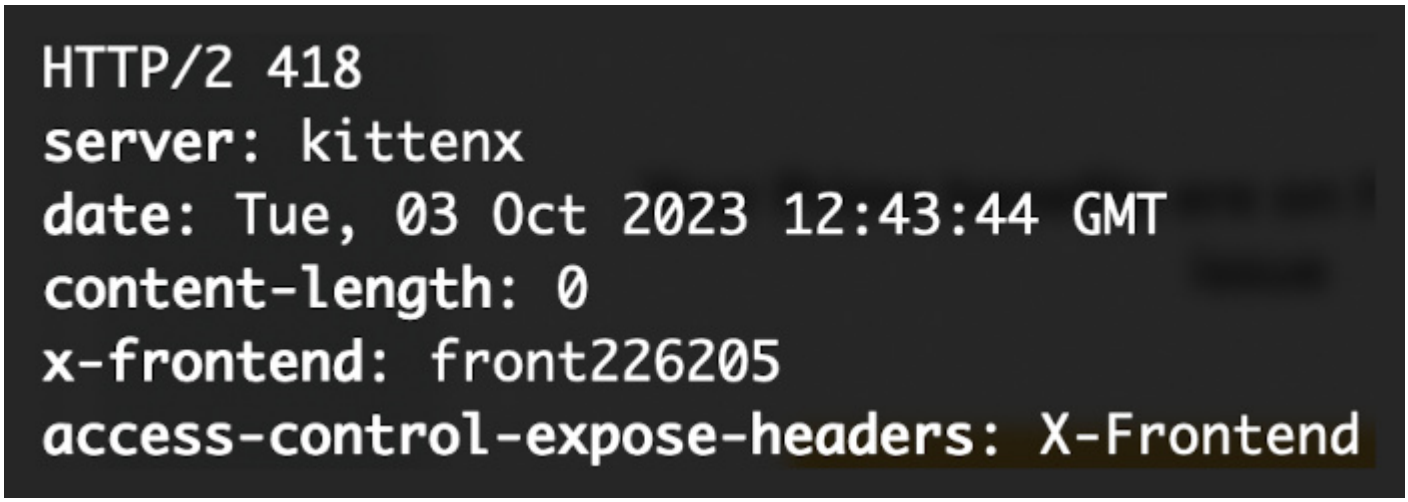
courriels amazon.co.uk (ce n'était pas le cas).
Avec un négatif contre ces chèques, peu importe à quel point le reste du courriel était convaincant.

Maintenant, il y a une chance que l'escroc joue aux échecs 3D ici et l'ait fait délibérément. L'administration des systèmes et des politiques de messagerie peut être difficile, de sorte que de nombreuses organisations, probablement les plus petites, n'ont pas implémenté DMARC ou l'ont désactivé dans une solution lourde à un problème d'authentification des courriels.

Alors peut-être que l'escroc a fait quelques calculs au dos de l'enveloppe et calculé que les avantages de l'utilisation d'une « vraie » adresse courriel l'emportent sur les inconvénients considérables.
Peut-être.
Mais un escroc qui peut le faire peut probablement utiliser un correcteur orthographique aussi, alors je préfère faire confiance au rasoir de Hanlon – « N'attribuez jamais à la malice ce qui est correctement expliqué par la stupidité ».

VKontakte a le dernier rire

Lorsque j'ai vérifié l'URL qui redirigeait via VKontakte, j'ai remarqué quelque chose d'étrange qui suggère qu'il était déjà au courant de l'URL incriminée.
La redirection aurait dû renvoyer un code d'état 301 ou 302, indiquant que la réponse était une redirection, mais ce n'était pas le cas, elle a renvoyé 418, un code d'état qui indique que le serveur est une théière.



Extrait du protocole officiel de contrôle des cafetières hypertexte (HTCPCP/1.0), publié le jour du poisson d'avril 1998 :

> Toute tentative de préparation de café avec une théière devrait entraîner le code d'erreur « 418 Je suis une théière ».
> Le corps de l'entité résultant PEUT être court et robuste.

Gloire.

La leçon la plus importante

Le protocole SMTP sur lequel repose le courrier électronique est une relique vieille de 50 ans d'une époque où Internet était minuscule et confiant.
Son manque intrinsèque de sécurité a été renforcé au fil des ans par une série de technologies qui peuvent garantir que les courriels sont cryptés et que les adresses de l'expéditeur sont fiables.
Cependant, comme ils ne font pas partie de la spécification SMTP, ils sont facultatifs et les entreprises doivent décider de les adopter.

La leçon la plus importante que cette arnaque a pour les entreprises, aussi petites soient-elles, est de mettre en place DMARC.

Que l'escroc soit plus bête que la saleté ou qu'il joue aux échecs en 3D, son courrier électronique allait toujours échouer face aux contrôles anti-usurpation d'identité.

Recherche et mise en page par:
Michel Cloutier
CIVBDL
20231010
"C'est ensemble qu'on avance"