

Ne relayez pas les spams, canulars, chaînes de lettres... | Denis JACOPINI

2

	<p>Ne relayez pas les spams, canulars, chaînes de lettres...</p>
---	--

L'association Clusir (Clusir de la Sécurité de l'Information Région Tahiti, une jeune association de professionnels du secteur) continue de attirer ses 12 membres de la sécurité informatique dans les colonnes. Après avoir appris comment choisir un bon mot de passe et comment sécuriser sa navigation sur le web, l'association s'attaque en ce qui concerne comment.

Le message informatique ne fait pas uniquement appel à des techniques de hacking, il utilise aussi des manipulations qualifiées « d'ingénierie sociale », qui consistent à obtenir des informations confidentielles (identifiant ou mot de passe par exemple) en trompant les victimes. C'est pourquoi, en complément de votre article, il est indispensable de faire preuve de sens critique lors de la lecture de certains messages non officiels.

Le mot est un courriel indubitable, aussi appelé « courriel ». Ce message provient de tout : les services d'un employeur, des établissements de confiance, des amis, des proches, des connaissances, etc.

Les techniques sont aussi plus sophistiquées que jamais, surtout sur les réseaux sociaux, les conseils restent pourtant les mêmes : pour tout message non officiel et non professionnel dont vous ne connaissez pas l'expéditeur, il n'y a qu'une règle : détruisez le message et ne répondez surtout pas.


Certains sont plus d'experts que d'autres pour les lecteurs qui leur donnent suite, en voici quelques exemples :

- Le club
- Diffusion d'un virus « cyber-attaque » ou « cyber-espionnage » généralement envoyé par courriel.
- Des courriels vous sollicitant pour récupérer des sommes d'argent - mais il faut s'être que vous n'avez rien à payer et que vous n'avez rien à payer.
- La police, ce sont les offres de « prêts entre particuliers » par mail, sur Facebook et sur les forums qui sont utilisées de manière abusive par des milliers d'arnaques, faisant des centaines de victimes qui ne reçoivent jamais leur argent.

Le phishing ou hameçonnage

Vous recevez un message qui ressemble à un mail officiel, par exemple Yahoo, Google, Meva, etc. Les clients Meva subissent des tentatives de phishing de ce type, où des courriels ressemblant à ceux de fournisseurs d'accès à internet vous demandent votre mot de passe, votre numéro de carte bancaire, etc.

Mais les experts vous recommandent de ne jamais donner les informations qui leur sont nécessaires sur votre Meva. Si ce n'est vous adressant à un fournisseur de services de votre région, vérifiez-vous d'abord de ne pas tomber dans un message suspecté de phishing.



Il faut être extrêmement vigilant lorsqu'on reçoit un message. Particulièrement si y a beaucoup plus une véritable adresse pour les spammeurs traquer à la recherche de nouvelles adresses mail à piller.

Comme dans le cas de Clusir, des chaînes envoient le lecteur en jouant sur les sentiments. Mais la transmettre ce n'est pas forcément résoudre le problème? Si vous voulez aider, il existe des plateformes en ligne (où l'on peut compter le nombre de votes à une chaîne), des sites dédiés pour faire des dons. Mais ne faites surtout pas suivre une chaîne.

Particulièrement, les chaînes utilisent la supériorité en prétendant qu'il est en fait pas suivre, un cycle sans fin et que des centaines de personnes le produisent. Ne vous laissez pas impressionner : aucun message n'a jamais de succès. Par contre, le non-respect des protocoles de cyber-sécurité peut avoir des effets dramatiques.


Des faux-semblants ?

Un mail suspecté de phishing de nombreuses personnes qui s'agitent dans les groupes, comme une invitation à un événement ou un appel à l'aide, mentionnant toutes les adresses mail dans le champ « Cc » (Cliquez sur l'adresse, appelée également copie cachée). Certains logiciels en anglais notamment ce champ CC (Email Carbon Copy). C'est à cause de personnes qui ne le font pas que vous pouvez parfois commencer à recevoir des spams sur votre courriel alors que vous n'êtes même pas dans la liste.

Si vous recevez un message vous sollicitant de vous adresser à un site officiel, ne cliquez pas sur le lien de votre ordinateur, obtenez le message et faites passer à votre ordinateur qu'il s'agit d'un mail de spam.

Malheureusement, des courriels ne sont pas toujours sur internet, par exemple sur votre ordinateur. Il est possible d'installer un logiciel de sécurité qui vous aide à détecter les courriels. Ne donnez jamais de renseignements personnels ou bancaires, n'ouvrez jamais d'images de vos photos d'identité à un tiers qui vous en fait la demande dans un message.

Enfin, gardez à l'esprit que les cyber-attaques servent à financer des activités criminelles : si jamais vous êtes victime d'une arnaque, allez parler police. Même si les policiers ne trouvent dans un pays étranger, il faut que l'on commette le plus précisément possible les chiffres de la cybercriminalité pour mieux lutter contre elle.



Le Net Expert
INFORMATIQUE
Tahiti

Rejoindre cet article

Source : http://www.tahiti-infos.com/Clusir-Ne-relayez-pas-les-spams-canulars-chaines-de-lettres_a121624.html