Commandement n° 5 – Tu ne relayeras pas les spams, canulars, chaînes des lettres...

1 La messagerie électronique et la sécurité

Nous utilisons la messagerie électronique, sur notre lieu de travail, à nos domiciles ou parfois dans des endroits publics.

Le piratage informatique ne fait pas appel qu'à des techniques d'intrusion complexes, il fait aussi appel à des techniques de 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 antivirus, il est indispensable de faire preuve de sens critique lors de la lecture de certains messages non sollicités.

2 Les différents types de SPAMS

Le spam est un courrier indésirable ou pourriel, il en existe plusieurs catégories, nous allons essayer de voir lesquelles.

Ces messages proposent les services d'un marabout, des médicaments ou d'autres produits contrefaits, un prêt d'argent, voire des rencontres par Internet, etc.

Pour tout message non sollicité 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.

Il est bon de savoir que certains spams sont plus dangereux que d'autres pour les lecteurs qui leur donnent suite, en voici quelques exemples ci-après.

2.1 Le SCAM

Définition d'un scam : "cyber-arnaques" ou "cyber-escroqueries" généralement envoyée par courriel.

Ces courriels vous sollicitent pour récupérer des sommes importantes en échange d'un pourcentage. Ils peuvent aussi se présenter comme la nouvelle d'un gros gain à une loterie à laquelle vous n'avez jamais joué. Ils proviennent de pays en voie de développement et sont souvent rédigés depuis des cybercafés. Ils coûtent parfois très cher aux victimes et cela peut avoir des conséquences graves puisque certaines victimes ont ensuite fait l'objet de chantage et ont été poussées au suicide.

2.2 Le phishing ou hameçonnage

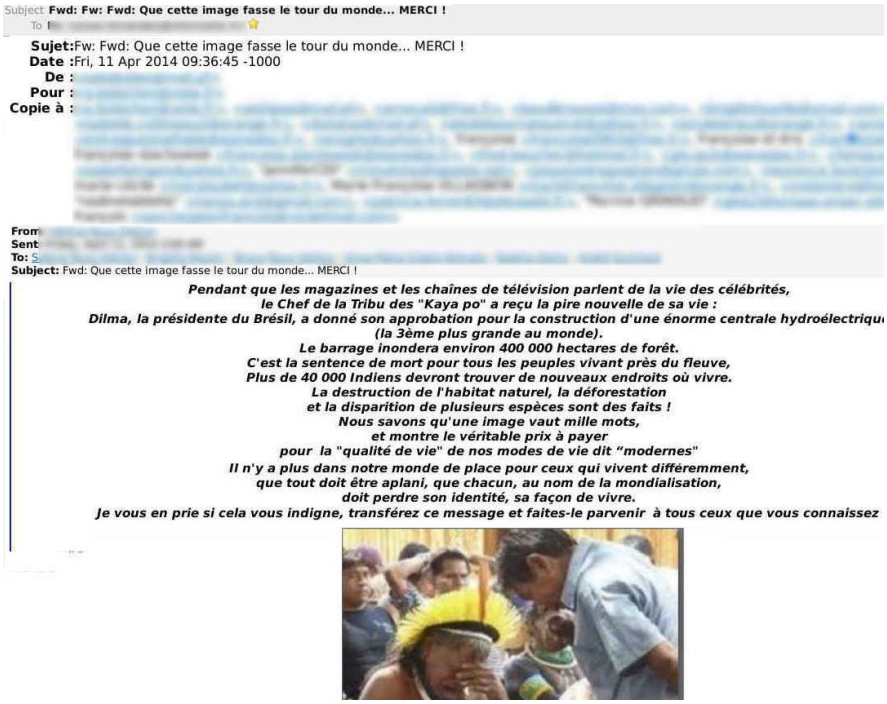
Vous recevez un message qui ressemblerait en tout point à ce que pourrait vous envoyer un site officiel. Par exemple, un fournisseur de service de messagerie (Yahoo, google, etc), votre fournisseur d'accès à Internet, votre fournisseur d'énergie, votre banque, etc.

Mais ces sites, d'organismes qui vous fournissent un service, ont déjà toutes les informations qui leurs sont nécessaires sur vous. Donc ils ne vous demanderont jamais vos identifiants ou vos informations

bancaires de cette façon. Méfiez-vous donc de ce qui semble être un message important mais qui n'est en réalité qu'une imitation.

2.3 Les chaînes ou canulars circulant sur Internet

Ci-après, vous verrez un exemple de chaîne totalement inutile. Si vous voulez aider le chef Raoni, cherchez plutôt la pétition à signer, par exemple. Ce sera plus efficace que de faire suivre aveuglément. .
.



37 adresses électroniques visibles figuraient dans message (avant que je ne les floute), parfois il y en a beaucoup plus. Une véritable aubaine pour les spammeurs toujours à la recherche de listes.

Cette chaîne manipule le lecteur en jouant sur les sentiments :

- Qui aime voir un homme pleurer?
- Qui a envie de se sentir responsable de la tristesse du chef Raoni que presque tout le monde connaît ?

Mais la meilleure question est :

- Qui prend quelques secondes pour se demander si cette chaîne va réellement résoudre le problème?

Faire suivre le message ne résoudra rien... Si vous voulez aider, trouvez autre chose de plus efficace, mais ne faites surtout pas suivre une chaîne.

Parfois, les chaînes utilisent la superstition en prétendant que si on ne fait pas suivre, un cycle sera rompu et que des événement atroces se produiront.

Ne vous laissez pas impressionner. Aucun message n'a autant de pouvoir. Par contre, le non respect des consignes de cybersécurité peut avoir des effets dramatiques.

Conclusion

Si vous recevez un message vous indiquant que vous avez gagné ou que l'on a besoin de vous pour récupérer un héritage ou une grosse d'argent quelconque, ou encore qu'un inconnu, en train de mourir dans un hôpital avec un cancer du cerveau en phase terminale veut vous aider, détruisez ce message et faites savoir à votre entourage qu'ils doivent faire de même.

N'exécutez jamais des instructions qui vous sont données dans un message par quelqu'un dont vous ne pouvez vérifier l'identité. Il est possible d'usurper une identité, y compris celle de quelqu'un représentant l'autorité. Ne donnez jamais de renseignements personnels ou bancaires, n'envoyez jamais d'image de vos pièces d'identité à un tiers qui vous en fait la demande dans un message.

Gardez toujours à l'esprit que si Internet est une invention fabuleuse, son utilisation comporte des risques.

Gardez également à l'esprit que les cyber-escroquerie servent à financer des activités criminelles. Soyez attentifs, lorsque vous consultez votre messagerie, mais si jamais vous êtes victime d'une escroquerie, allez porter plainte.

Même si les pirates se trouvent dans un pays lointain et inaccessible aux enquêteurs, il faut que l'on connaisse le plus précisément possible les chiffres de la cybercriminalité pour mieux lutter contre elle.

J.V. FERNANDEZ – 2014