Spam ou pourriel : c'est quoi, que faire ?

Pr Chérif DIALLO, CISSP
Professeur Assimilé (LAFMC CAMES)
Laboratoire d'Algèbre, de Cryptographie, Codes et Applications (LACCA)
Dept Informatique, UFR Sciences Appliquées et Technologie (UFR SAT)
Université Gaston Berger (UGB), BP 234, Saint-Louis, Sénégal
E-mail: cherif.diallo@ugb.edu.sn

" Même de jolies fautes de français, même d'adorables et rares, aussi bien, erreurs d'orthographe, mettaient un charme de plus dans ce courrier presque quotidien." Paul Verlaine, Confessions, 1895.

Résumé: Face à la recrudescence des actes cybercriminels, ce bulletin mensuel de sécurité, qui est une communication de vulgarisation et de sensibilisation, présente aujourd'hui une menace qui est très courante sur la messagerie électronique. Il s'agit du spam (ou pourriel en français) qui désigne la réception d'un message non voulu à des fins publicitaires, commerciales ou malveillantes. Dans la majorité des cas, il s'agit de messages de prospection commerciale ne respectant pas les obligations légales en matière de consentement des destinataires, mais il peut également revêtir un caractère malveillant : astuces pour gagner de l'argent, sollicitation pour transférer des fonds ou encore tentatives d'hameçonnage (ou phishing, voir notre bulletin mensuel de sécurité n°2022-02). Après la définition, nous donnerons les types de spams, les tendances actuelles de cette menace et les solutions avant de conclure.

Mots clés: Cybercriminalité, spam, pourriel, messagerie électronique.

---

1. Définition

Étymologiquement, le mot spam signifie « Spiced Pork and Meat », c'est à dire jambon épicé. Son caractère indésirable vient d'un sketch des Monty Python où il entre dans la composition de chaque plat, obligeant les clients d'un restaurant à en consommer. Le mot « pourriel », quant à lui, vient du mélange entre poubelle et courriel. C'est un message indésirable, le plus souvent publicitaire, commercial ou à but malveillant. Ainsi, le « spamming » ou « spam » est défini par la CNIL (Commission Nationale Informatique et Libertés, France) comme l'envoi massif, et parfois répété, de courriers électroniques non sollicités, à des personnes avec lesquelles l'expéditeur n'a jamais eu de contact et dont il a capté l'adresse électronique de façon irrégulière.

Les expéditeurs de spams ciblent essentiellement les comptes de messagerie, mais peuvent aussi utiliser les messageries instantanées ou les réseaux sociaux. Un spam électronique peut avoir un caractère sexuel, relever de l'escroquerie ou parfois même contenir un virus, un logiciel malveillant (un rançongiciel par exemple, voir bulletin mensuel de sécurité n°2022-01) qui pourrait permettre d'utiliser ou de bloquer votre équipement à votre insu. Souvent envoyé en grande quantité, ses vecteurs sont multiples, et on note d'autres types de spams moins connus mais tout aussi envahissants, comme :

- Les spams sur les mobiles sous la forme de SMS.
- Les spams sur les réseaux sociaux.
- Les spams sur les messageries instantanées comme WhatsApp, Snapchat ou Skype.
- Les spams de liens sur les commentaires de blogs ou de forums.
- Les spams SEO également nommé référencement abusif ou spamdexing dont l'objectif est d'abuser les moteurs de recherche en vue d'obtenir un bon classement. Le spam SEO se produit lorsque des pirates implantent leurs liens à l'intérieur de votre site Web, blog, etc. Ils ciblent vos pages de premier rang et les infiltrent avec leurs liens sans que vous le sachiez.

Les buts recherchés des spams sont multiples :

- Vente de produits ou de services, publicité virale, propagande, etc.
- Diffusion de virus.
- Vol de données personnelles et/ou professionnelles.
- Escroquerie à caractère financier.
- Diffusion de ransomwares et d'autres outils malveillants (malwares).
- Attaques de type hameçonnage (phishing).

2. Types de spams

Comme nous venons de le voir dans la définition, il y a plusieurs types de pourriels (i.e. spams) selon le support de diffusion du spam. Mais on pourrait aussi adopter une typologie des spams en fonction des services ciblés :

- **Services financiers et récompenses**. Les spams de ce type promettent souvent d'aider à régler des problèmes d'argent grâce à des prêts faciles ou à faible taux d'intérêt, une solution à l'endettement ou des récompenses en espèces.
- **Sites de rencontre et contenu réservé aux adultes**. Cette catégorie de spams couvre également plusieurs domaines : des services et agences de rencontres en ligne, sites web pour adultes, promotion ou vente de produits d'amélioration des performances au lit, etc.
- **Santé et prestations médicales.** Voici des sujets parmi les plus préférés des spammeurs : remèdes miracle, méthodes pour perdre du poids rapidement, compléments alimentaires de réputation douteuse, thérapies contre la chute de cheveux, solutions anti-âge, médecines alternatives, etc. La grande majorité de ces produits ne sont que des promesses en l'air.
- **Informatique, Internet et technologie.** Parfois, les spammeurs essaient de profiter des nombreuses personnes qui ne sont pas expertes en informatique. Ne vous laissez pas tromper par des offres de matériel ou de logiciel, de services Internet ou mobiles, ou par des publicités pour de l'électronique grand public.
- **Inscription à un service.** Ici, le spammeur tente de convaincre les victimes à s'inscrire à un service comme des programmes éducatifs, ou des types d'assurances. Très souvent, ce type de pourriel utilise l'urgence comme outil d'ingénierie sociale pour tenter de pousser la cible à prendre une décision rapide.

3. Tendances

Les techniques de spamming ont beaucoup évolué au fil des années. De même, de nombreuses variations du taux de spams ont été notées ces dernières années :

- Dans les années 2000, le taux du spam représentait environ 60% des emails reçus.
- Au cours des années 2009-2010, le nombre de pourriels a connu une hausse conséquente avec en moyenne 90% d'emails indésirables dans les boîtes aux lettres, ce taux a atteint jusqu'à 96% durant les mois de juillet et d'aout 2009.
- En revanche, à la suite de la fermeture de plusieurs botnets, le nombre de spams a pu être diminué entre 2010 et 2012. Depuis février 2013, des hausses et des baisses se succèdent avec une moyenne située à 55% de spams.
- Sur la base de l'analyse d'un échantillon de plus d'un milliard d'emails lors du premier semestre 2018, seul 32% du trafic de courrier électronique a été considéré comme « propre ».
- En 2019, le taux de spams était de 65,26% tandis que celui des mails légitimes tournait légèrement au-dessus de 19%.
- Aujourd'hui, plus de trois millions de spams par seconde sont envoyés sur internet, soit 262 milliards de spams par jour, ce qui représente plus de 95 000 milliards de spams par an.

Outre les désagréments qu'il cause aux usagers, le spam a également un impact environnemental non négligeable en raison de la consommation électrique qu'engendrent ces milliards de courriers électroniques au niveau de l'infrastructure du réseau (serveurs, routeurs) et des ordinateurs. De plus, ils contribuent à la saturation de la bande passante avec comme conséquence une qualité de service amoindrie pour les applications qui ont une demande légitime en bande passante.

4. Solutions

Avant de passer en revue quelques solutions simples face au problème de spams, il est important pour nous de comprendre d'abord pourquoi recevons nous autant de spams :

- De nombreuses entreprises gagnent de l'argent en vendant nos adresses e-mail et autres coordonnées à des tiers. Ainsi face à l'ampleur sans cesse croissante de ce phénomène, l'UE a adopté en 2018 le Règlement général sur la protection des données (RGPD) avec une série de règles visant à limiter ce que les sociétés sont autorisées à faire avec nos données personnelles.
- Les spammeurs utilisent des logiciels (parfois gratuits) qui récupèrent automatiquement les adresses e-mail publiées sur des pages web ou des forums de discussions.
- Générer des adresses au hasard est une opération facile pour les spammeurs. Il leur suffit de combiner les listes de noms et prénoms les plus courants, avec celles des noms de domaines internet les plus populaires. Ainsi, en utilisant toutes les combinaisons possibles (prenom.nom, nom.prenom, etc.), il est possible de générer des centaines de milliers d'adresses de messagerie souvent réelles.

- Lors d'un achat sur internet, vous avez communiqué votre adresse e-mail et oublié de cocher (ou décocher selon les cas) une petite case à la fin du contrat «je souhaite recevoir des informations de vos partenaires». Vous avez ainsi autorisé la diffusion de votre adresse e-mail à des tiers.
- La quasi-gratuité de l'envoi massif de spams garantit au spammeur un bon retour sur investissement dès lors qu'une poignée de destinataires répond favorablement à la campagne.
- Compte tenu du fait que la plupart des spammeurs utilisent l'usurpation d'identité pour masquer leur réelle identité aux destinataires et aux fournisseurs de services Internet, il est donc difficile de les identifier afin de les rendre responsables de leurs actes.
- Ainsi, la faiblesse des coûts et des risques font donc du spam une option intéressante pour les annonces et le transport de virus et de malwares (logiciels malveillants).

Ensuite, il faut savoir reconnaître un spam [Figures 1,2] pour éviter d'être victime d'éventuelles conséquences. Voici une liste non exhaustive de critères qui vous aideront à reconnaître un spam :

- Vous ne connaissez pas l'émetteur de l'e-mail. Attention, même le nom de l'émetteur peut être falsifié.
- L'objet ou le sujet de l'e-mail est vide ou il ne vous concerne visiblement pas.
- Vous recevez un e-mail dans une langue que vous ne connaissez pas.
- Vous identifiez des fautes : mots sans accents, manque de ponctuation, conjugaison et une orthographe approximative, etc.
- Le contenu de l'e-mail contient des questions inhabituelles, demande une action de votre part ou comporte un lien à cliquer. Dans ce cas, méfiez-vous du phishing.

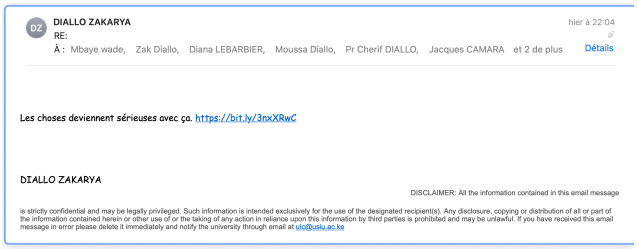

Figure 1: Spam invitant à cliquer sur un lien

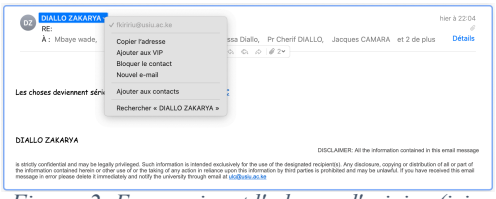

Figure 2: En examinant l'adresse d'origine (ici : fkiririu@usiu.ac.ke), on s'aperçoit que le nom de l'émetteur a été falsifié

Maintenant, nous allons lister quelques solutions simples pour aider à lutter contre les spams et atténuer les dommages si vous êtes victimes de spams :

- **Ne jamais répondre aux messages dont on ignore l'expéditeur**. Ceci afin d'éviter de le renseigner sur la validité de votre adresse de messagerie.
- **Bloquez les expéditeurs de spams**. Vous pouvez bloquer les expéditeurs de spams dans les paramètres de configuration du client de messagerie, réseaux sociaux ou autres services qui le permettent. Vous pouvez également utiliser un filtre ou un logiciel anti-spam pour limiter la réception de ces courriers indésirables. Certains antivirus proposent ce type de protection.
- **Si vous recevez un spam provenant de quelqu'un que vous connaissez, prévenez-le**. Si vous recevez un spam d'un contact de confiance, dites-lui que son compte a été utilisé pour envoyer du spam. Ainsi, il pourra prendre des mesures pour corriger et mieux contrôler sa messagerie.
- **Dans la boîte de réception de votre messagerie, marquez les spams comme « indésirables » et créez des règles dans votre boîte de messagerie**. Cette fonctionnalité existe dans la majorité des clients de messagerie et webmails ainsi que dans le module de Signal Spam. Créez des règles dans votre boîte de messagerie pour filtrer et/ou supprimer automatiquement certains types de messages indésirables.
- **Utilisez les logiciels et les mesures de sécurité actuels pour la gestion des sites web**. Maintenez les systèmes et les applications Web à jour pour vous protéger des spammeurs qui cherchent à exploiter les vulnérabilités. Intégrez également la technologie CAPTCHA sur les pages de connexion, de commentaires et autres zones interactives.
- **Utilisez un logiciel de sécurité efficace**. Pour vous prémunir des spams et autres cybermenaces, vous devez installer une application antivirus capable de vous protéger en temps réel contre les multiples vecteurs d'attaque. Quant aux spam SEO, il existe des scanners et analyseurs très sophistiqués.

5. Pour finir

Même si la tendance est à la baisse par rapport au taux de spams reçus parmi les e-mails qui circulent sur internet, nous devons rester vigilants et apprendre à repérer les spams pour mieux nous en prémunir. En effet, non seulement les spams inondent nos boîtes mail mais, en plus, ils peuvent être dangereux et constituer un vecteur pour d'autres cybermenaces comme les ransomwares, le phishing, les virus, l'arnaque, l'escroquerie, etc.