www.malwarebytes.com /spam

Qu’est-ce qu’un pourriel (spam informatique utilisé dans le texte)

Pourriels informatiques, pourriels textuels, pourriels d’appels : une communication numérique non désirée et non sollicitée envoyée en masse. Le spam est ennuyeux, mais c’est aussi une menace.

Qu’est-ce qui vous vient à l’esprit lorsque vous pensez au spam ?
Des pilules miracles de pharmacies sur Internet, des demandes d’argent de la part de « princes » d’autres pays, ou peut-être de la nourriture, du spam ?
Cet article est consacré au spam avec un « s » minuscule.
Alors que beaucoup de gens apprécient la nourriture Spam, personne ne veut être trompé en perdant de l’argent ou en téléchargeant des logiciels malveillants à cause de l’autre type de spam.

Le spam est ennuyeux, mais c’est aussi une menace.
Alors que beaucoup d’entre nous pensent que nous sommes assez avisés pour reconnaître n’importe quelle forme de cela, les spammeurs mettent régulièrement à jour leurs méthodes et leurs messages pour tromper les victimes potentielles.
La réalité est que nous sommes tous constamment attaqués par des cybercriminels et la preuve se trouve dans votre boîte de réception.

Lisez donc la suite pour savoir ce qu’est le spam, comment le reconnaître et comment vous en protéger.

Définition du spam

Le spam est tout type de communication numérique non désirée et non sollicitée qui est envoyée en masse. Souvent, le spam est envoyé par courriel, mais il peut également être distribué par SMS, appels téléphoniques ou médias sociaux.

Capture d'écran, pour visionner la vidéo, cliquer le lien YouTube suivant:

https://www.youtube.com/watch?v=vT0Rc_0oB3U

Qu’est-ce que le spam ?

Spam n’est pas l’acronyme d’une menace informatique, bien que certains aient été proposés (logiciels malveillants stupides et inutiles, ennuyeux, par exemple).
L’inspiration pour l’utilisation du terme « spam » pour décrire les messages indésirables de masse est un sketch des Monty Python dans lequel les acteurs déclarent que tout le monde doit manger la nourriture Spam, qu’ils le veuillent ou non.
De même, toute personne disposant d’une adresse e-mail doit malheureusement être gênée par les spams, qu’on le veuille ou non.

Si vous souhaitez en savoir plus sur les origines du spam, consultez la section sur l’historique du spam ci-dessous.

Les spammeurs utilisent de nombreuses formes de communication pour envoyer en masse leurs messages indésirables.
Certains d’entre eux sont des messages marketing vendant des produits non sollicités. D’autres types de spams peuvent propager des logiciels malveillants, vous inciter à divulguer des informations personnelles ou vous effrayer en vous faisant croire que vous devez payer pour vous tirer d’affaire.

Les filtres anti-spam détectent un grand nombre de ces types de messages, et les opérateurs téléphoniques vous avertissent souvent d’un « risque de spam » de la part d’appelants inconnus.
Que ce soit par courriel, SMS, téléphone ou réseaux sociaux, certains spams passent, et vous voulez être en

mesure de les reconnaître et d'éviter ces menaces.
Vous trouverez ci-dessous plusieurs types de spam à surveiller.

Courriels d'hameçonnage

Les courriels d'hameçonnage sont un type de spam que les cybercriminels envoient à de nombreuses personnes, dans l'espoir d'en « accrocher » quelques-unes.
Les courriels d'hameçonnage incitent les victimes à divulguer des informations sensibles telles que les connexions à des sites Web ou les informations de carte de crédit.

Adam Kujawa, directeur de Malwarebytes Labs, déclare à propos des courriels de phishing : « Le phishing est le type de cyberattaque le plus simple et, en même temps, le plus dangereux et le plus efficace.
C'est parce qu'il s'attaque à l'ordinateur le plus vulnérable et le plus puissant de la planète : l'esprit humain.

Usurpation d'adresse courriel

Les courriels usurpés imitent ou usurpent un courriel provenant d'un expéditeur légitime et vous demandent de prendre des mesures.
Les usurpations bien exécutées contiendront une image de marque et un contenu familiers, souvent d'une grande entreprise bien connue telle que PayPal ou Apple.
Les spams d'usurpation d'adresse courriel les plus courants sont les suivants :

- Une demande de paiement d'une facture impayée
- Une demande de réinitialisation de votre mot de passe ou de vérification de votre compte
- Vérification des achats que vous n'avez pas effectués
- Demande de mise à jour des informations de facturation

Escroqueries au support technique

Dans le cas d'une escroquerie au support technique, le spam indique que vous avez un problème technique et que vous devez contacter le support technique en appelant le numéro de téléphone ou en cliquant sur un lien dans le message.
À l'instar de l'usurpation d'adresse courriel, ces types de spam sont souvent considérés comme provenant d'une grande entreprise technologique comme Microsoft ou d'une société de cybersécurité comme Malwarebytes.

Si vous pensez avoir un problème technique ou un logiciel malveillant sur votre ordinateur, votre tablette ou votre cellulaire, vous devez toujours vous rendre sur le site officiel de l'entreprise que vous souhaitez appeler pour obtenir une assistance technique afin de trouver les coordonnées légitimes.
L'assistance technique à distance implique souvent un accès à distance à votre ordinateur pour vous aider, et vous ne voulez pas accidentellement donner cet accès à un escroc de l'assistance technique.

Escroqueries liées à l'actualité

Les sujets d'actualité peuvent être utilisés dans les spams pour attirer votre attention.
En 2020, alors que le monde était confronté à la pandémie de Covid-19 et qu'il y avait une augmentation

des emplois à domicile, certains escrocs ont envoyé des spams promettant **des emplois à distance rémunérés en Bitcoin**.
Au cours de la même année, un autre sujet de spam populaire était lié à **l'offre d'une aide financière aux petites entreprises**, mais les escrocs ont finalement demandé des coordonnées bancaires.
Les titres d'actualité peuvent être accrocheurs, mais méfiez-vous d'eux en ce qui concerne les messages de spam potentiels.

Escroqueries liées aux avances de frais

Ce type de spam est probablement familier à tous ceux qui utilisent le courrier électronique depuis les années 90 ou 2000.
Parfois appelé courriels « prince nigérian » car il a été l'expéditeur présumé du message pendant de nombreuses années, ce type de spam promet une récompense financière si vous fournissez d'abord une avance de fonds.
L'expéditeur indique généralement que cette avance de fonds est une sorte de frais de traitement ou d'argent sérieux pour débloquer la somme la plus importante, mais une fois que vous avez payé, ils disparaissent.
Pour rendre les choses plus personnelles, un type d'escroquerie similaire implique que l'expéditeur se fasse passer pour un membre de la famille qui a des problèmes et a besoin d'argent, mais si vous payez, le résultat est malheureusement le même.

Pourriel malicieux

Abréviation de « malware spam » ou « malicious spam », le malspam est un message de spam qui transmet un logiciel malveillant à votre appareil.
Les lecteurs peu méfiants qui cliquent sur un lien ou ouvrent une pièce jointe à un courriel se retrouvent avec un certain type de logiciel malveillant, notamment des rançongiciels, des chevaux de Troie, des bots, des voleurs d'informations, des cryptomineurs, des logiciels espions et des enregistreurs de frappe.
Une méthode de diffusion courante consiste à inclure des scripts malveillants dans une pièce jointe d'un type familier comme un document Word, un fichier PDF ou une présentation PowerPoint.
Une fois la pièce jointe ouverte, les scripts s'exécutent et récupèrent la charge utile du logiciel malveillant.

Appels et SMS indésirables

Avez-vous déjà reçu un appel automatisé ?
C'est ce qu'on appelle le spam.
Un SMS d'un expéditeur inconnu vous invitant à cliquer sur un lien inconnu ?
C'est ce qu'on appelle le spam par SMS ou « smishing », une combinaison de SMS et d'hameçonnage.

Si vous recevez des appels et des SMS indésirables sur votre Android ou iPhone, la plupart des grands opérateurs vous offrent la possibilité de signaler les spams.
Le blocage des numéros est un autre moyen de lutter contre le spam mobile.
Aux États-Unis, vous pouvez ajouter votre numéro de téléphone au registre national des numéros de téléphone

exclus pour essayer de réduire le nombre d'appels de vente indésirables que vous recevez, mais vous devez toujours vous méfier des escrocs qui ignorent la liste.

Comment puis-je arrêter le spam ?

Bien qu'il ne soit peut-être pas possible d'éviter complètement le spam, il existe des mesures que vous pouvez prendre pour vous protéger contre une escroquerie ou l'hameçonnage à partir d'un message de spam :

Apprenez à repérer l'hameçonnage

Nous pouvons tous être victimes d'attaques de phishing.
Nous pouvons être pressés et cliquer sur un lien malveillant sans nous en rendre compte. Si un nouveau type d'attaque par hameçonnage apparaît, il se peut que nous ne le reconnaissions pas facilement.
Pour vous protéger, apprenez à rechercher certains signes clés indiquant qu'un message de spam n'est pas seulement ennuyeux, mais qu'il s'agit d'une tentative d'hameçonnage :

1. Adresse courriel de l'expéditeur :
   Si un courriel d'une entreprise est légitime, l'adresse courriel de l'expéditeur doit correspondre au domaine de l'entreprise qu'elle prétend représenter.
   Parfois, ceux-ci sont évidents, comme example@abkljzr09348.biz, mais d'autres fois, les changements sont moins perceptibles, comme example@paypa1.com au lieu de paypal.com.

2. Informations personnelles manquantes :
   Si vous êtes un client, l'entreprise devrait avoir vos informations et s'adressera probablement à vous par votre prénom.
   Un message d'accueil personnel manquant ne suffit pas à repérer un e-mail d'hameçonnage, mais c'est une chose à rechercher, en particulier dans les messages qui disent qu'ils proviennent d'une entreprise avec laquelle vous faites affaire.
   Recevoir un courriel indiquant que votre compte a été verrouillé ou que vous devez de l'argent est une source d'inquiétude, et parfois nous nous précipitons pour cliquer sur un lien afin de résoudre le problème.
   S'il s'agit d'hameçonnage, c'est exactement ce que l'expéditeur veut, alors soyez prudent et vérifiez si le courriel est générique ou s'il vous est adressé spécifiquement.

3. Liens :
   Méfiez-vous de tous les liens, y compris les boutons dans un courriel.
   Si vous recevez un message d'une entreprise avec laquelle vous avez un compte, il est sage de vous connecter à votre compte pour voir s'il y a un message plutôt que de simplement cliquer sur le lien dans le message sans vérifier au préalable.
   Vous pouvez contacter l'entreprise pour lui demander si un message suspect est légitime ou non.
   Si vous avez des doutes sur un message, ne cliquez sur aucun lien.

4. Erreurs grammaticales :
   Nous en faisons tous, mais une entreprise qui envoie des messages légitimes n'aura probablement pas beaucoup d'erreurs de ponctuation, de grammaire et d'orthographe.
   Ceux-ci peuvent être un autre signal d'alarme pour indiquer que le courriel pourrait être suspect.

5. Offres trop belles pour être vraies :
   De nombreux messages d'hameçonnage prétendent provenir de grandes entreprises bien connues, dans l'espoir de piéger les lecteurs qui font affaire avec l'entreprise.
   D'autres tentatives d'hameçonnage offrent quelque chose de gratuit, comme de l'argent ou un prix convoité.
   Le dicton est souvent vrai que si quelque chose semble trop beau pour être vrai, c'est probablement le cas, et cela peut être un avertissement qu'un message de spam essaie d'obtenir quelque chose de vous, plutôt que de vous donner quelque chose.

6. Pièces jointes :
   À moins que vous ne vous attendiez à recevoir un courriel contenant des pièces jointes, méfiez-vous toujours avant de les ouvrir ou de les télécharger. L'utilisation d'un logiciel anti-malware peut vous aider en analysant les fichiers que vous téléchargez à la recherche de logiciels malveillants.

Vous pouvez en savoir plus sur les e-mails d'hameçonnage et sur la façon de les repérer..

Signaler un spam

Les fournisseurs de messagerie sont devenus assez bons pour filtrer les spams, mais lorsque les messages arrivent dans votre boîte de réception, vous pouvez les signaler. Cela est vrai pour les appels et les messages texte indésirables, car de nombreux opérateurs vous donnent également la possibilité de signaler les spams.
Vous pouvez également choisir de bloquer l'expéditeur, souvent à la même étape que le signalement du message.

Le signalement de spam peut aider votre fournisseur de messagerie ou votre opérateur téléphonique à mieux détecter les spams.
Si des courriels légitimes sont envoyés à votre filtre anti-spam, vous pouvez signaler qu'ils ne doivent pas être marqués comme spam, ce qui fournit également des informations utiles sur ce qui ne doit pas être filtré.
Une autre étape utile consiste à ajouter de manière proactive les expéditeurs dont vous souhaitez avoir des nouvelles à votre liste de contacts.

Utiliser l'authentification à deux facteurs (2FA)

Avec l'authentification à deux facteurs ou à plusieurs facteurs, même si votre nom d'utilisateur et votre mot de passe sont compromis par une attaque de phishing, les cybercriminels ne pourront pas contourner les exigences d'authentification supplémentaires liées à votre compte.
Les facteurs d'authentification supplémentaires incluent les questions secrètes ou les codes de vérification envoyés à votre téléphone par SMS.

Installer un logiciel de cybersécurité

Si vous cliquez sur un mauvais lien ou si vous téléchargez un logiciel malveillant qui vous est envoyé par spam, un bon logiciel de cybersécurité reconnaîtra le logiciel malveillant et l'arrêtera avant qu'il ne puisse endommager votre système ou votre réseau.
Avec des produits pour la maison et l'entreprise, Malwarebytes a ce qu'il vous faut partout où la technologie vous mène.

Historique des spams

L'histoire du spam commence en 1864, plus de cent ans avant Internet, avec un télégramme envoyé en masse à un certain nombre de politiciens britanniques.
Signe prémonitoire des choses à venir, le télégramme était une publicité pour le blanchiment des dents.

Le premier exemple d'e-mail non sollicité remonte à 1978 et au précurseur d'Internet : ARPANET.
Ce proto-spam Internet était une publicité pour un nouveau modèle d'ordinateur de Digital Equipment Corporation.
Cela a fonctionné : les gens ont acheté les ordinateurs.

Dans les années 1980, les gens se sont rassemblés sur des communautés régionales en ligne, appelées tableaux d'affichage (BBS), gérées par des amateurs sur leurs serveurs domestiques.

Sur un BBS typique, les utilisateurs étaient en mesure de partager des fichiers, de publier des avis et d'échanger des messages.
Au cours d'échanges en ligne houleux, les utilisateurs tapaient le mot « spam » encore et encore pour se noyer les uns les autres.
Cela a été fait en référence à un sketch des Monty Python de 1970 dans lequel un mari et sa femme mangeant dans un café de la classe ouvrière découvrent que presque tout sur le menu contient du spam.
Alors que la femme se dispute avec la serveuse au sujet de la prépondérance du spam sur le menu, un chœur de Vikings noie la conversation avec une chanson sur le spam.

L'utilisation du mot « spam » dans ce contexte, c'est-à-dire des messages bruyants et ennuyeux, s'est répandue – au grand dam de Hormel Foods, le fabricant du spam.

Sur Usenet, un précurseur d'Internet qui fonctionne un peu comme les forums Internet d'aujourd'hui, le terme « spam » était utilisé pour désigner les messages multiples excessifs sur plusieurs forums et fils de discussion.
Les premiers spams Usenet comprenaient un tract religieux fondamentaliste, une diatribe politique sur le génocide arménien et une publicité pour des services juridiques de carte verte.

Le spam n'a vraiment commencé qu'avec l'essor d'Internet et de la communication instantanée par e-mail au début des années 90.
Le spam a atteint des proportions épidémiques avec des centaines de milliards de spams submergeant nos boîtes de réception.

En 1999, Melissa, le premier virus qui s'est propagé via des documents Word compatibles avec les macros joints à des courriels, s'est répandu dans le monde numérique.
Il s'est propagé en saccageant les listes de contacts des victimes et en se faisant envoyer des spams à tous ceux que la victime connaissait.
En fin de compte, Melissa a causé 80 millions de dollars de dommages, selon le FBI.

En l'absence d'une loi anti-pourriel, les spammeurs professionnels ont pris de l'importance, y compris l'autoproclamé « roi du spam » Sanford Wallace.
Fidèle à son surnom, Wallace était à un moment donné le plus grand expéditeur de spams et de spams sur les réseaux sociaux sur des sites comme Myspace et Facebook.

Ce n'est qu'au début des années 2000 que les gouvernements du monde entier ont commencé à s'intéresser sérieusement à la réglementation du spam.
Notamment, tous les pays membres de l'Union européenne et le Royaume-Uni ont mis en place des lois qui restreignent le spam.
De même, en 2003, les États-Unis ont mis en place un ensemble de lois effrontément appelées CAN-SPAM Act (une fois de plus, Hormel ne peut tout simplement pas faire de pause).
Ces lois, aux États-Unis et à l'étranger, imposent des restrictions sur le contenu, le comportement d'envoi et la conformité de désabonnement de tous les courriels.

Dans le même temps, les principaux fournisseurs de messagerie Microsoft et Google ont travaillé dur pour améliorer la technologie de filtrage du spam.
Bill Gates a prédit que le spam disparaîtrait d'ici 2006.

En vertu de ces lois, une galerie de spammeurs voyous, y compris le roi du spam, a été arrêtée, poursuivie et emprisonnée pour nous avoir imposé des penny stocks, de fausses montres et des drogues douteuses.
En 2016, Sanford Wallace a été reconnu coupable, condamné à 30 mois de prison et condamné à payer des centaines de milliers de dollars de dédommagement pour avoir envoyé des millions de messages de spam sur Facebook.

Et pourtant, le spam existe toujours.
Désolé, Bill.

Malgré tous les efforts déployés par les législateurs, les forces de l'ordre et les entreprises technologiques, nous luttons toujours contre le fléau des courriels et autres communications numériques indésirables et malveillants.
Le fait est que le commerce du spam nécessite peu d'efforts de la part des spammeurs, peu de spammeurs vont en prison et il y a beaucoup d'argent à gagner.

Dans le cadre d'une étude conjointe sur le spam menée par l'Université de Californie à Berkeley et l'Université de Californie à San Diego, des chercheurs ont observé un botnet zombie en action et ont découvert que les opérateurs du botnet avaient envoyé 350 millions de courriels en un mois.
Sur ces centaines de millions de courriels, les spammeurs ont réalisé 28 ventes.
Il s'agit d'un taux de conversion de 0,00001 %.
Cela dit, si les polluposteurs continuaient d'envoyer des pourriels à ce rythme, ils gagneraient 3,5 millions de dollars en l'espace d'un an.

Alors, quels sont exactement les types de spam qui continuent de remplir nos boîtes de réception à ras bord et que pouvons-nous faire pour y remédier ?

Articles connexes

Qu'est-ce que la sécurité des terminaux ? Comment il peut prévenir les menaces indésirables, comme le spam informatique

Qu'est-ce qu'un VPN | Définition d'un réseau privé virtuel | VPN Types (malwarebytes.com)

Qu'est-ce qu'une adresse IP ? Comment protéger votre adresse IP (malwarebytes.com)

Qu'est-ce que l'empreinte numérique ? Comment gérer et protéger les vôtres (malwarebytes.com)

Qu'est-ce que la cybersécurité ? Principes de base et meilleures pratiques en matière de cybersécurité (malwarebytes.com)

Recherche et mise en page par:
Michel Cloutier
CIVBDL
20240325
"C'est ensemble qu'on avance"