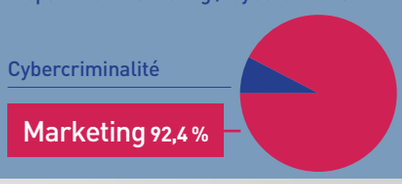
Baromètre du Spam

OCTOBRE/NOVEMBRE/DÉCEMBRE 2019

signal spam
SIGNALER, **C'EST AGIR !**

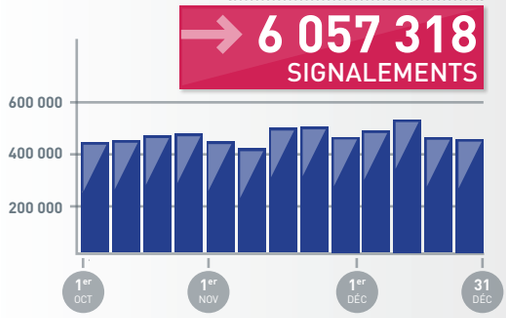
Signal Spam effectue ses statistiques à partir des e-mails signalés comme spam qui sont parvenus jusqu'à l'internaute (c'est-à-dire qui sont délivrés dans sa boîte de réception). La majeure partie du spam (près de 90%) est filtrée en amont par les outils anti-spam des fournisseurs d'accès internet et de messagerie, et ne touche jamais l'internaute. Les signalements effectués auprès de Signal Spam portent sur cette fraction du spam qui parvient jusqu'aux internautes (environ 10%), ce qui les rend d'autant plus importants pour l'analyse du phénomène et la protection collective.

Répartition Marketing / Cybercriminalité

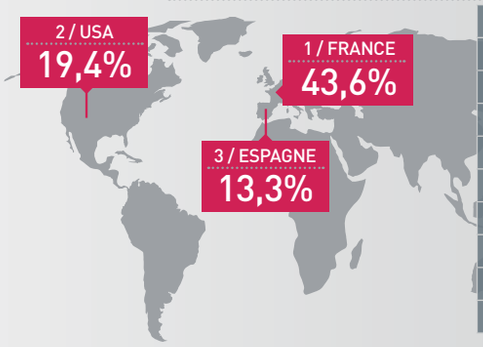


SIGNALEMENTS TRIMESTRIEL
D'OCTOBRE À DÉCEMBRE 2019

6 057 318 SIGNALEMENTS



PROVENANCE GÉOGRAPHIQUE DU SPAM SIGNALÉ

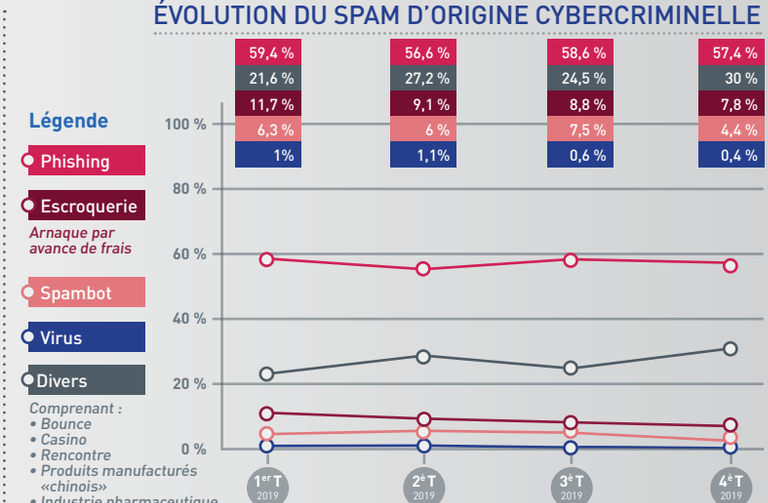


1	FRANCE	43,6%
2	USA	19,4%
3	ESPAGNE	13,3%
4	ALLEMAGNE	4%
5	ANGLETERRE	3,5%
6	POLOGNE	2,2%
7	RUSSIE	1,1%
8	ITALIE	0,8%
9	MONACO	0,7%
10	PAYS-BAS	0,6 %

LE TOP 10 DES OBJETS

n°	Objet
1	Testez votre éligibilité
2	Investissez en résidences services avec Réside Etudes
3	Jusqu'a moins 50 pour cent
4	Votre mutuelle à partir de 8 euros par mois
5	La mode à prix d'usine
6	Isolez vos combles pour 1 euro
7	Chauffage électrique innovant
8	Faites financer vos travaux d'économies d'énergies
9	Sauvegarde 4 en 1
10	nouvelle génération à prix d'usine !

ÉVOLUTION DU SPAM D'ORIGINE CYBERCRIMINELLE

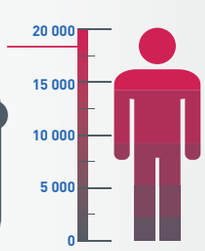


LE TOP DES OBJETS PAR CATÉGORIE

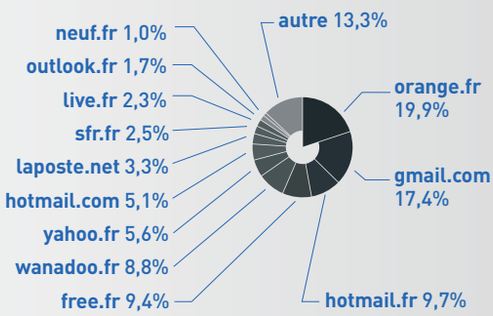
n°	Objet par Catégorie / PHISHING	Objet par Catégorie / SCAMY	Objet par Catégorie / SPAMBOT
1	*(société de livraison)* Réclamez la maintenant	Bonjour	Bonjour
2	[SPAM] *(Banque)* : Vous aves (2) notifications non lu !	Hello	The Last Flashlight You'll Ever Own (and it's Free!)
3	Vous n'avez pas encore activé la validation en 2 étapes	CONFIRMATION: EUROMILLIONS 2019	FLASH SALE! $14.99 for 16x20 Custom Canvas Prints!
4	Avis de Remboursement	Re: Prêt	Serexin - Stronger erections enough to drive your partner crazy!
5	Produisez et consommez votre propre énergie	Dear Friend,	Sell Us Your Unused Diabetic Test Strips and Get CASH!

NOMBRE D'UTILISATEURS DE SIGNAL SPAM

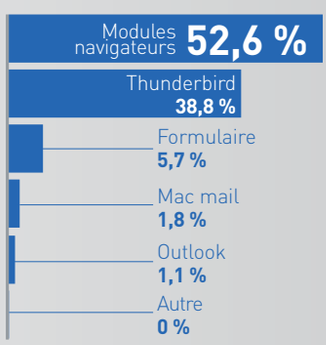
18 613 NOUVEAUX UTILISATEURS SUR LES TROIS DERNIERS MOIS



MESSAGERIES DES INTERNAUTES INSCRITS À SIGNAL SPAM



MOYEN DE SIGNALEMENTS



Signal Spam - Reproduction autorisée si citation de la source - www.signal-spam.fr

FOCUS // KIT DE SENSIBILISATION
LA SÉCURITÉ SUR LES RÉSEAUX SOCIAUX

La plateforme cybermalveillance.gouv.fr à laquelle appartient Signal Spam a produit des fiches réflexe de sensibilisation aux menaces cybercriminelles. Nous proposons en focus de ce baromètre une fiche thématique pour vous aider à mieux vous prémunir contre les risques inhérents aux communications électroniques et à la navigation sur internet.

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

LA SÉCURITÉ SUR LES RÉSEAUX SOCIAUX

ADOPTER LES **BONNES PRATIQUES**

Les réseaux sociaux sont des outils de communication et d'information puissants et facilement accessibles. Aujourd'hui installés dans les usages personnels des internautes, mais aussi dans les usages professionnels des entreprises qui les utilisent comme vitrine de leur activité, ils n'échappent pas aux activités malveillantes. Escroquerie, usurpation d'identité, chantage, vol d'informations, cyberharcèlement, désinformation, diffamation… sont autant de dangers auxquels sont confrontés les utilisateurs de ces réseaux. **Voici 10 bonnes pratiques à adopter pour votre sécurité sur les réseaux sociaux.**

1 PROTÉGEZ L'ACCÈS À VOS COMPTES

Vos comptes de réseaux sociaux contiennent des informations personnelles sensibles (identité, adresse postale ou de messagerie, numéro de téléphone, date de naissance, etc.), qui peuvent être convoitées par les cybercriminels. Pour vous assurer que personne ne puisse utiliser votre compte à votre insu ou usurper votre identité, protégez bien l'accès à votre compte en utilisant des mots de passe différents et suffisamment robustes. Si le service le propose, activez également la double authentification. Tous nos conseils pour bien gérer vos mots de passe sur notre site : www.cybermalveillance.gouv.fr/nos-articles/fiche-pratique-gerer-ses-mots-de-passe.

2 VÉRIFIEZ VOS PARAMÈTRES DE CONFIDENTIALITÉ

Par défaut, les paramètres de visibilité de vos informations personnelles (numéro de téléphone, adresse email…) et de vos publications sont souvent très ouverts. Vos données peuvent ainsi être partagées à tous les abonnés du réseau social. Il est généralement possible de restreindre cette visibilité en réglant la configuration de votre compte, afin de garder la maîtrise de ce que les autres utilisateurs voient de vos informations et de vos activités. Vérifiez régulièrement ces paramètres de confidentialité qui peuvent être modifiés sans que vous ne le sachiez.

3 MAÎTRISEZ VOS PUBLICATIONS

Les réseaux sociaux permettent de communiquer auprès d'une grande audience que vous ne pourrez jamais complètement maîtriser. Même dans un cercle que l'on pense restreint, vos publications peuvent vous échapper et être rediffusées ou interprétées au-delà de ce que vous envisagiez. Ne diffusez pas d'informations personnelles ou sensibles qui pourraient être utilisées pour vous nuire. Faites également preuve de discernement lorsque vous évoquez votre travail car cela pourrait vous porter préjudice ainsi qu'à votre entreprise. Enfin, respectez évidemment la loi. *Voir encart.*

4 FAITES ATTENTION À QUI VOUS PARLEZ

Les cybercriminels utilisent notamment les réseaux sociaux pour commettre des escroqueries et voler des informations personnelles ou professionnelles. Soyez vigilants, car à leur insu, vos "amis" ou contacts peuvent également vous envoyer ou partager des contenus malveillants, surtout s'ils se sont fait pirater leur compte sans le savoir. Quelques conseils supplémentaires : n'envoyez jamais d'argent à quelqu'un sans avoir vérifié son identité au préalable, n'envoyez jamais de photos ou vidéos intimes à des contacts virtuels qui pourraient en profiter pour vous faire chanter et méfiez-vous des jeux concours, des gains inattendus, ou des « super affaires », qui peuvent cacher des escroqueries (hameçonnage).

5 CONTRÔLEZ LES APPLICATIONS TIERCES

Certaines applications proposent d'interagir avec votre compte de réseau social. Il peut s'agir de jeux, de quiz, de programmes alternatifs pour gérer votre compte. Ces applications demandent des autorisations qu'il faut examiner avec attention car une fois données, ces applications peuvent avoir accès à vos informations personnelles, vos contacts, vos publications, vos messages privés… Ne les installez que depuis les sites ou magasins d'applications officiels, sinon vous risquez de donner l'accès à votre compte à un programme infecté par un virus. Si l'application vous semble trop intrusive dans les autorisations qu'elle demande, ne l'installez pas. Enfin, pensez à désinstaller ces applications ou en révoquer les droits si vous ne vous en servez plus.

RESPECTEZ LA LOI

Internet n'est pas une zone de non-droit et l'anonymat n'y est pas absolu : les propos incitant à la haine ou à la violence, la pédophilie, le cyberharcèlement, l'atteinte au droit à l'image ou au droit d'auteur… sont punis par la loi.

Signal Spam - Reproduction autorisée si citation de la source - www.signal-spam.fr

LE SAVIEZ-VOUS ?

En vertu de la loi n°2018-493 du 20 juin 2018 – Article 20, **un mineur peut consentir seul à un traitement de ses données à caractère personnel à partir de quinze ans.** Avant cet âge, le consentement du titulaire de l'autorité parentale est requis.

6 ÉVITEZ LES ORDINATEURS ET LES RÉSEAUX WIFI PUBLICS

Utiliser un ordinateur en libre accès ou un réseau WiFi public est risqué car ils peuvent être piégés ou contrôlés par un cybercriminel. Lorsque vous vous connectez à votre compte de réseau social par ce moyen, vous pouvez vous faire voler votre mot de passe et donc vous faire pirater votre compte. Évitez dans la mesure du possible de renseigner des informations sensibles ou personnelles sur un matériel ou un réseau qui n'est pas le vôtre. Si vous y êtes contraint malgré tout, pensez à bien vous déconnecter de votre compte après utilisation pour empêcher que quelqu'un puisse y accéder après vous.

7 VÉRIFIEZ RÉGULIÈREMENT LES CONNEXIONS À VOTRE COMPTE

La plupart des réseaux sociaux offrent des fonctionnalités qui vous permettent de voir les connexions ou sessions actives sur votre compte depuis les différents appareils que vous utilisez pour y accéder. Consultez régulièrement ces informations. Si vous détectez une session ou une connexion inconnue ou que vous n'utilisez plus, déconnectez là. Au moindre doute, considérez qu'il peut s'agir d'un piratage et changez immédiatement votre mot de passe (voir conseil n°1).

8 FAITES PREUVE DE DISCERNEMENT AVEC LES INFORMATIONS PUBLIÉES

Les réseaux sociaux sont de formidables et rapides outils d'information, mais n'importe qui peut aussi y publier n'importe quelle information, sans aucune vérification. Certaines informations peuvent donc être partiellement ou totalement fausses, parfois délibérément. Avec la puissance des réseaux sociaux, ces fausses informations (appelées « fake news » en anglais) peuvent avoir de graves conséquences sur les personnes qui en sont victimes. Aussi, avant de considérer ou relayer une information, efforcez-vous d'en vérifier la véracité.

9 UTILISEZ EN CONSCIENCE L'AUTHENTIFICATION AVEC VOTRE COMPTE DE RÉSEAU SOCIAL SUR D'AUTRES SITES

Pour s'y connecter, certains sites Internet vous proposent d'utiliser votre compte de réseau social. Cette fonctionnalité peut sembler pratique car elle évite de créer un compte et un mot de passe supplémentaires, mais cela signifie que vous allez communiquer au réseau social des informations sur ce que vous faites sur le site concerné, et à l'inverse que vous allez peut-être donner au site des droits d'accès sur votre compte de réseau social. De plus, si votre compte de réseau social était un jour piraté, le cybercriminel pourrait automatiquement accéder à tous ces sites en usurpant votre identité. Aussi, avant d'utiliser cette fonctionnalité, ayez bien conscience des risques et vérifiez attentivement les autorisations que vous délivrez.

10 SUPPRIMEZ VOTRE COMPTE SI VOUS NE L'UTILISEZ PLUS

Pour éviter que vos informations ne soient récupérées par des tiers ou que votre compte ne soit utilisé à votre insu, notamment pour usurper votre identité, supprimez-le si vous ne l'utilisez plus.

QUE FAIRE EN CAS DE PROBLÈME ?

- **Réagir en cas de piratage de votre compte de réseau social** – Les conseils de la CNIL : www.cnil.fr/fr/prevenir-reperer-et-reagir-face-au-piratage-de-ses-comptes-sociaux
- **Demander la suppression d'une publication gênante ou compromettante sur les réseaux sociaux** – Les conseils de la CNIL : www.cnil.fr/fr/publication-genante-sur-les-reseaux-sociaux-signalez-pour-supprimer
- **Signaler une situation de cyber harcèlement** : contacter Net Écoute gratuitement au 0800200000 et sur www.netecoute.fr
- **Signaler un contenu illicite sur les réseaux sociaux** – Internet Signalement/Pharos (ministère de l'Intérieur) : www.internet-signalement.gouv.fr

DOCUMENT RÉALISÉ AVEC NOS MEMBRES :

e-Enfance · eset · Microsoft · Entrepreneurs d'Assurances · PUBLICIS CONSULTANTS

En partenariat avec l'Agence nationale de la sécurité des systèmes d'information

RETROUVEZ TOUTES NOS PUBLICATIONS SUR :
www.cybermalveillance.gouv.fr

Version 1.0

Licence Ouverte v2.0 (ETALAB)

A PROPOS DE SIGNAL SPAM

Signal Spam œuvre pour la sécurité des réseaux et la restauration de la confiance envers les communications électroniques.
Issue d'un partenariat public/privé, Signal Spam est une association à but non lucratif qui mobilise depuis 2005 les internautes. Après s'être enregistré sur le site www.signal-spam.fr, l'internaute signale tout e-mail qu'il juge indésirable à partir de son logiciel de messagerie ou sur le site www.signal-spam.fr.
Sur la base de ces signalements, Signal Spam alimente les acteurs de l'économie numérique et les autorités publiques en informations permettant d'agir contre le spam et les menaces associées à la cybercriminalité.

Signal Spam - Reproduction autorisée si citation de la source - www.signal-spam.fr