Baromètre du Spam

OCTOBRE/NOVEMBRE/DÉCEMBRE 2018

signal spam

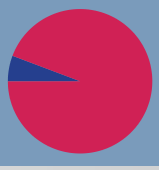
SIGNALER, **C'EST AGIR !**

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 important pour l'analyse du phénomène et la protection collective.

Répartition Marketing / Cybercriminalité

Cybercriminalité

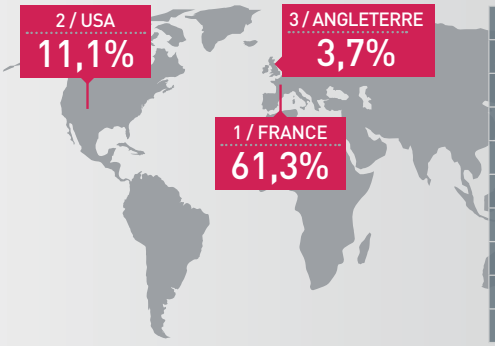
Marketing
94,3 %



SIGNALEMENTS TRIMESTRIEL
D'OCTOBRE À DÉCEMBRE 2018

5 928 654
SIGNALEMENTS

PROVENANCE GÉOGRAPHIQUE DES SIGNALEMENTS

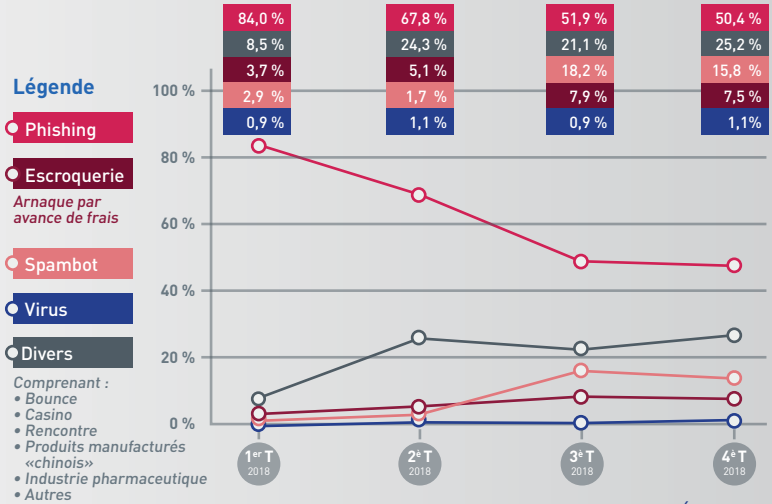


1	FRANCE	61,3%
2	USA	11,1%
3	ANGLETERRE	3,7%
4	ESPAGNE	3,6%
5	POLOGNE	2,2%
6	RUSSIE	1,8%
7	ALLEMAGNE	1,7%
8	BRÉSIL	1,5%
9	CANADA	1,4%
10	ITALIE	1,3 %

LE TOP 10 DES OBJETS

n°	Objet
1	I Missed Fuckbuddy Message
2	Votre mutuelle à partir de 8 euros par mois
3	Enfin une mutuelle qui vous apporte de la sérénité
4	Comparez les prix de votre région
5	Vous cherchez une mutuelle plus economique
6	Votre invitation privilège
7	Tous les meilleurs vins et champagnes à prix imbattable
8	Visite conseil avant travaux gratuite
9	Votre douche à l'italienne à la place de votre baignoire en moins de 8h
10	Evaluez gratuitement le prix actuel de votre voiture

ÉVOLUTION DU SPAM D'ORIGINE CYBERCRIMINELLE



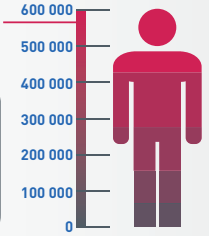
LE TOP DES OBJETS PAR CATÉGORIE

n°	Objet par Catégorie / PHISHING	Objet par Catégorie / SCAMY	Objet par Catégorie / SPAMBOT
1	Rappel : mise à jour requise en raison d'un problème de paiement	NEW MESSAGE FROM *(Banque)* NEW YORK	Obtenez une carte cadeau de 50€ d'*(société d'expédition)*
2	Nouveau message de la Direction Générale des Finances Publiques !	Hello	*(société d'expédition)* Order Confirmation
3	Rappel de paiement	Bonjour	Important
4	Reactiver votre Carte NICKEL	Veuillez mettre à jour les informations d'identification associées au compte *(email)*	Confirmation
5	1 message pas encore lu	Offre de prêts	*You appeared in 8 search this week*

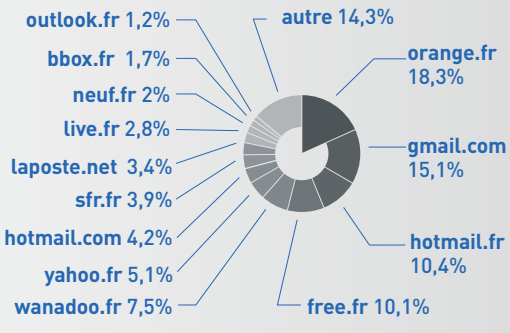
NOMBRE D'UTILISATEURS TOTAL DE SIGNAL SPAM

567 018

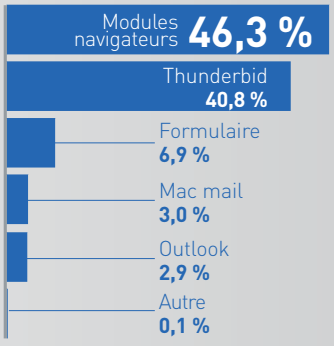
DONT **20 871** NOUVEAUX UTILISATEURS SUR LES TROIS DERNIERS MOIS



MESSAGERIES DES INTERNAUTES INSCRITS À SIGNAL SPAM



MOYEN DE SIGNALEMENTS



FOCUS // KIT DE SENSIBILISATION
SÉCURITÉ DES APPAREILS MOBILES

La plateforme cybermaveillance.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.

FICHE PRATIQUE B

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

SÉCURITÉ DES APPAREILS MOBILES

Les téléphones mobiles intelligents (*smartphones*) et tablettes informatiques sont devenus des instruments pratiques du quotidien, tant pour un usage personnel que professionnel. Leurs capacités ne cessent de croître et les fonctionnalités qu'ils offrent s'apparentent, voire dépassent parfois, celles des ordinateurs. Alors qu'ils contiennent tout autant, voire plus, d'informations sensibles ou permettent d'y accéder, et qu'ils sont plus faciles à perdre ou à se faire voler, ces appareils mobiles sont généralement bien moins sécurisés que les ordinateurs par leurs propriétaires. Cette fiche pratique présente les **10 principales règles à adopter pour assurer au mieux la sécurité de son appareil mobile.**

1 Mettez en place les codes d'accès

Qu'il s'agisse du code de déverrouillage ou du code PIN, ces protections complémentaires (*voir encadré*) empêcheront une personne malintentionnée de pouvoir se servir facilement de votre appareil si vous en perdez le contrôle (perte, vol, abandon) et donc d'accéder à vos informations. Bien entendu, vos codes d'accès doivent être suffisamment difficiles à deviner (évitez 0000 ou 1234, par exemple). Activez également le verrouillage automatique de votre appareil afin que le code d'accès soit demandé au bout de quelques minutes si vous laissez votre appareil sans surveillance.

CODE D'ACCÈS ET CODE PIN, DEUX PROTECTIONS COMPLÉMENTAIRES

Mot de passe, signe, combinaison de touches ou biométrie : **le code de verrouillage empêche de pouvoir se servir de l'appareil si on ne le connaît pas.**

Composé de 4 chiffres, **le code PIN bloque quant à lui l'accès à votre carte SIM** et empêche donc de pouvoir s'en servir dans un autre appareil si on ne le connaît pas.

2 Chiffrez les données de l'appareil

En cas de perte ou de vol, seul le chiffrement des données contenues dans votre appareil vous assurera qu'une personne malintentionnée ne pourra pas contourner les codes d'accès et accéder quand même à vos informations. Tous les appareils récents proposent cette option qu'il suffit d'activer dans les paramètres et qui est quasi transparente à l'utilisation. Et si vous utilisez une carte d'extension mémoire pour stocker vos informations, vérifiez qu'elle est également chiffrée.

3 Appliquez les mises à jour de sécurité

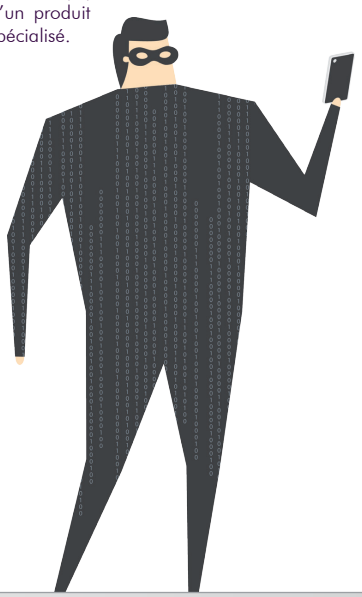
Qu'il s'agisse du système d'exploitation (Android, iOS) ou des applications qui sont sur votre appareil, il est important d'installer sans tarder les mises à jour dès qu'elles sont proposées car elles corrigent souvent des failles de sécurité qui pourraient être exploitées par des cybercriminels pour prendre le contrôle de votre appareil et accéder à vos informations.

4 Faites des sauvegardes

Votre appareil mobile contient généralement des informations que vous n'avez nulle part ailleurs comme votre répertoire de contacts, vos messages, vos photos… Pensez à le sauvegarder régulièrement car si vous le perdez, si on vous le vole, ou s'il se casse vous pourriez tout perdre.

5 Utilisez une solution de sécurité contre les virus et autres attaques

De nombreuses solutions de sécurité existent pour aider à se protéger des différentes attaques que peuvent subir les appareils mobiles au même titre que les ordinateurs de bureau, comme les virus, les rançongiciels (*ransomware*), l'hameçonnage (*phishing*)… Des cybercriminels se spécialisent dans les attaques d'appareils mobiles qu'ils savent souvent bien moins sécurisés que les ordinateurs de bureau. Il est donc important d'avoir un bon niveau de protection et de s'équiper d'un produit spécialisé.



6 N'installez des applications que depuis les sites ou magasins officiels

Seuls les sites ou magasins officiels vous permettent de vous assurer au mieux que les applications que vous installez ne sont pas piégées. Méfiez-vous des sites « parallèles » qui ne contrôlent pas les applications qu'ils proposent ou qui offrent gratuitement des applications normalement payantes en téléchargement illégal : elles sont généralement piégées. Consultez le nombre de téléchargements et les avis des autres utilisateurs avant d'installer une nouvelle application. Au moindre doute, n'installez pas l'application et choisissez-en une autre.

7 Contrôlez les autorisations de vos applications

Vérifiez également les autorisations que vous donnez à vos applications lors de leur première installation, mais aussi après leurs mises à jour car leurs autorisations peuvent évoluer. Certaines applications demandent parfois des droits très importants sur vos informations et qui peuvent être « surprenants ». Par exemple, un simple jeu de cartes « gratuit » qui vous demanderait l'autorisation d'accéder à votre répertoire, vos mots de passe, vos messages, votre position GPS ou encore votre appareil photo est évidemment suspect. Au moindre doute, n'installez pas l'application et choisissez-en une autre.

8 Ne laissez pas votre appareil sans surveillance

Une personne mal intentionnée pourrait profiter de votre manque de vigilance pour accéder à vos informations ou piéger votre appareil. Pour ces mêmes raisons, il est fortement déconseillé de laisser un tiers se servir de votre appareil mobile (pour passer un appel par exemple) sans que vous ne puissiez contrôler physiquement l'utilisation réelle qu'il en fait.

9 Évitez les réseaux Wifi publics ou inconnus

Ces réseaux peuvent être contrôlés par des cybercriminels qui peuvent intercepter vos connexions et récupérer au passage vos comptes d'accès, mots de passe, données de carte bancaire… afin d'en faire un usage délictueux. D'une manière générale, désactivez toutes les connexions sans-fil quand vous ne vous en servez pas (Wi-Fi, Bluetooth, NFC, GPS…) car elles sont autant de portes d'entrée ouvertes sur votre appareil. De plus, elles épuisent votre batterie inutilement.

10 Ne stockez pas d'informations secrètes sans protection

Ne notez jamais d'informations secrètes comme vos mots de passe ou vos codes bancaires, dans votre répertoire de contacts, votre messagerie ou un fichier non chiffré sur votre appareil mobile. Un cybercriminel qui aurait pris le contrôle de votre appareil pourrait facilement les récupérer. En outre, certaines applications que vous avez installées peuvent aussi accéder et récupérer ces informations dont vous perdriez alors le contrôle. Pour protéger vos informations secrètes, utilisez une solution de chiffrement avec un mot de passe solide.

CONSERVEZ LE CODE IMEI DE VOTRE APPAREIL MOBILE

Composé de 15 à 17 chiffres, le code IMEI est **le numéro de série de votre appareil mobile.** Il est généralement inscrit sur sa boîte d'emballage. En cas de perte ou de vol, ce code peut permettre de bloquer l'usage du téléphone sur tous les réseaux.

Notez le soigneusement et si vous l'avez égaré **vous pouvez le récupérer en tapant *#06# sur votre clavier.**

POUR ALLER PLUS LOIN :
- Par la CNIL : www.cnil.fr/fr/comment-securiser-au-maximum-lacces-votre-smartphone
- Par l'ANSSI : www.ssi.gouv.fr/particulier/guide/recommandations-de-securite-relatives-aux-ordiphones

DOCUMENT RÉALISÉ AVEC NOS MEMBRES :

Bitdefender · CHAMBRE DE COMMERCE ET D'INDUSTRIE · CLUSIF · e-Enfance

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

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

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.