Baromètre du Spam

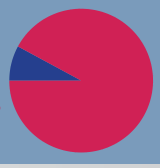
AVRIL / MAI / JUIN 2018

signal spam

SIGNALER, C'EST AGIR !

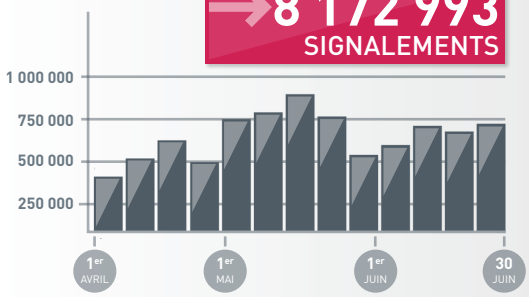
Signal Spam effectue ses statistiques à partir des e-mails signalés comme spam qui sont parvenus jusqu'à l'internaute (c'est-à-dire qui sont délivrés dans sa boîte de réception). La majeure partie du spam (près de 90%) est filtrée en amont par les outils anti-spam des fournisseurs d'accès internet et 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

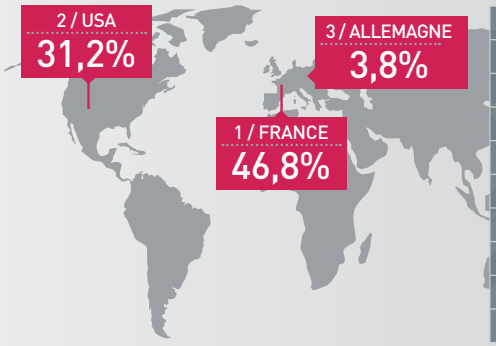


SIGNALEMENTS TRIMESTRIEL
DE AVRIL À JUIN 2018

8 172 993 SIGNALEMENTS



PROVENANCE GÉOGRAPHIQUE DES SIGNALEMENTS

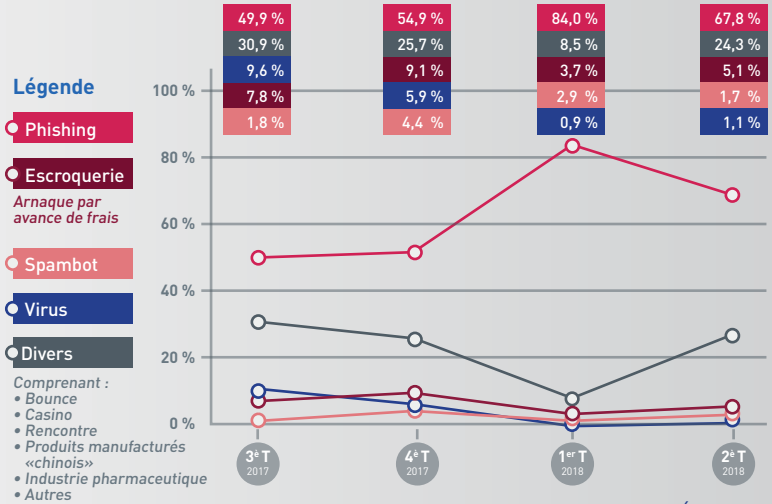


1	FRANCE	46,8%
2	USA	31,2%
3	ALLEMAGNE	3,8%
4	ANGLETERRE	3,6%
5	ESPAGNE	2,9%
6	ITALIE	1,9%
7	ROUMANIE	1,5%
8	PAYS-BAS	1,3%
9	CANADA	1,0%
10	RUSSIE	1,0 %

LE TOP 10 DES OBJETS

n°	Objet
1	Re:
2	Tentez Votre chance de Gagnez 4 Menus Savoureux!!
3	DES ÉRECTIONS PUISSANTES ET DURABLES !!!UN PLAISIR SEXUEL MAXIMAL.
4	ESSAYEZ GRATUITEMENT, PUIS GARDEZ LE PRODUIT!
5	*(Loi)*, le guide 2018 enfin disponible
6	Laissez votre femme etre surpris de votre virilite
7	votre **c_a_d_e_a_u** est en attente de votre **CONFIRMATION** !
8	Essayer_ et_ Gardez_ un_ Aspirateur *(marque)*
9	Votre invitation privilège
10	C'EST OFFICIEL: Vous etes approuve !!

ÉVOLUTION DU SPAM D'ORIGINE CYBERCRIMINELLE



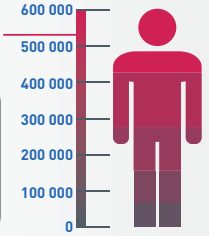
LE TOP DES OBJETS PAR CATÉGORIE

n°	Objet par Catégorie / PHISHING	Objet par Catégorie / SCAMY	Objet par Catégorie / SPAMBOT
1	Cher utilisateur *(nom du service)*	Bonjour	Urgent
2	(1) INBOX Message, Profitez de notre offre exclusive!!	Offre de prêts	Erreur Importante
3	Re:	Merci du fond du Cœur	Rappel
4	Regardez tous vos films preferes Et des emissions de television!	Hello	Important
5	Gangner vos billets maintena	[SPAM] Bonjour	You have purchased an item worth $560

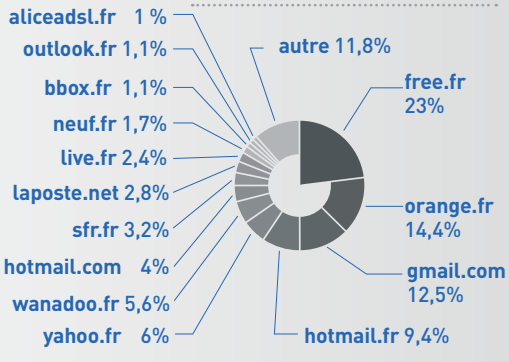
NOMBRE D'UTILISATEURS TOTAL DE SIGNAL SPAM

527 215

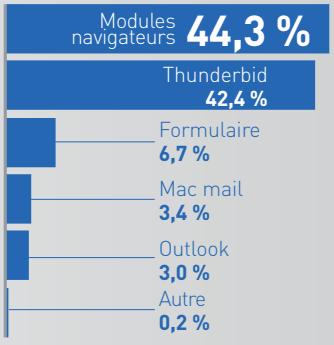
DONT **22 682** NOUVEAUX UTILISATEURS SUR LES TROIS DERNIERS MOIS



MESSAGERIES DES INTERNAUTES INSCRITS À SIGNAL SPAM



MOYEN DE SIGNALEMENTS



FOCUS // KIT DE SENSIBILISATION

LE HAMEÇONNAGE

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 RÉFLEXE 1

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

L'HAMEÇONNAGE

L'hameçonnage (**phishing** en anglais) est une technique frauduleuse destinée à leurrer l'internaute pour l'inciter à communiquer des données personnelles (comptes d'accès, mots de passe…) et/ou bancaires en se faisant passer pour un tiers de confiance. Il peut s'agir d'un faux message, SMS ou appel téléphonique de banques, de réseaux sociaux, d'opérateurs de téléphonie, de fournisseur d'énergie, de sites de commerce en ligne, etc.

BUT RECHERCHÉ

VOLER DES INFORMATIONS PERSONNELLES OU PROFESSIONNELLES
(comptes, mots de passe, données bancaires…) pour en faire un usage frauduleux

SI VOUS ÊTES **VICTIME**

Si vous avez malencontreusement communiqué des éléments sur vos moyens de paiement ou si vous avez constaté des débits frauduleux sur votre compte, **FAITES OPPOSITION IMMÉDIATEMENT** auprès de votre organisme bancaire ou financier et déposez plainte au commissariat de police ou à la gendarmerie la plus proche.

Si vous avez constaté que des éléments personnels servent à usurper votre identité, **DÉPOSEZ PLAINTE** au commissariat de police ou à la gendarmerie la plus proche.

Si vous êtes victime d'une usurpation de votre adresse de messagerie ou de tout autre compte, **CHANGEZ IMMÉDIATEMENT VOS MOTS DE PASSE**.

Si vous avez reçu un message douteux sans y répondre, le **SIGNALER À SIGNAL SPAM** (Signal-spam.fr).

Vous pouvez **SIGNALER UNE ADRESSE DE SITE D'HAMEÇONNAGE À PHISHING INITIATIVE** (Phishing-initiative.fr) qui en fera fermer l'accès.

Pour être conseillé en cas d'hameçonnage : **INFO ESCROQUERIES 0 805 805 817** (numéro gratuit).

MESURES **PRÉVENTIVES**

Ne communiquez jamais d'informations sensibles par messagerie ou téléphone : aucune administration ou société commerciale sérieuse ne vous demandera vos données bancaires ou vos mots de passe par message électronique ou par téléphone.

Avant de cliquer sur un lien douteux, positionnez le curseur de votre souris sur ce lien (sans cliquer) ce qui affichera alors l'adresse vers laquelle il pointe réellement afin d'en vérifier la vraisemblance, ou allez directement sur le site de l'organisme en question par un lien favori que vous aurez vous-même créé.

Vérifiez l'adresse du site qui s'affiche dans votre navigateur. Si cela ne correspond pas exactement au site concerné, c'est très certainement un site frauduleux. Parfois, un seul caractère peut changer dans l'adresse du site pour vous tromper. Au moindre doute, ne fournissez aucune information et fermez immédiatement la page correspondante.

En cas de doute, contactez si possible directement l'organisme concerné pour confirmer le message ou l'appel que vous avez reçu.

Utilisez des mots de passes différents et complexes pour chaque site et application que vous utilisez, afin d'éviter que le vol d'un de vos mots de passe ne compromette tous vos comptes personnels. Vous pouvez également utiliser des coffres forts numériques de type KeePass pour stocker de manière sécurisée vos différents mots de passe.

Si le site le permet, **vérifiez les date et heure de dernière connexion à votre compte** afin de repérer si des accès illégitimes ont été réalisés.

Si le site vous le permet, **activez la double authentification pour sécuriser vos accès.**

CYBERMALVEILLANCE.GOUV.FR
Assistance et prévention du risque numérique

LES **INFRACTIONS**

En fonction du cas d'espèce, les infractions suivantes peuvent être retenues :

• **Escroquerie (article 313-1 du code pénal) :** l'escroquerie est le fait, soit par l'usage d'un faux nom ou d'une fausse qualité, soit par l'abus d'une qualité vraie, soit par l'emploi de manœuvres frauduleuses, de tromper une personne physique ou morale et de la déterminer ainsi, à son préjudice ou au préjudice d'un tiers, à remettre des fonds, des valeurs ou un bien quelconque, à fournir un service ou à consentir un acte opérant obligation ou décharge. Délit passible d'une peine d'emprisonnement de cinq ans et de 375 000 euros d'amende.

• **Collecte de données à caractère personnel par un moyen frauduleux, déloyal ou illicite (article 226-18 du code pénal) :** une telle collecte constitue un délit passible d'une peine d'emprisonnement de cinq ans et de 300 000 euros d'amende.

• **Accès frauduleux à un système de traitement automatisé de données (article 323-1 du code pénal) :** le fait d'accéder ou de se maintenir, frauduleusement, dans tout ou partie d'un système de traitement automatisé de données est passible de deux ans d'emprisonnement et de 60 000 euros d'amende. Lorsqu'il en est résulté soit la suppression ou la modification de données contenues dans le système, soit une altération du fonctionnement de ce système, la peine est de trois ans d'emprisonnement et de 100 000 euros d'amende.

• **Contrefaçon et usage frauduleux de moyen de paiement (articles L163-3 et L163-4 du code monétaire et financier) :** délit passible d'une peine d'emprisonnement de sept ans et de 750 000 euros d'amende.

• **Usurpation d'identité (article 226-4-1 du code pénal) :** le fait d'usurper l'identité d'un tiers ou de faire usage d'une ou plusieurs données de toute nature permettant de l'identifier en vue de troubler sa tranquillité ou celle d'autrui, ou de porter atteinte à son honneur ou à sa considération, est passible d'une peine d'un an d'emprisonnement et de 15 000 euros d'amende.

• **Contrefaçon des marques (logos, signes, emblèmes...) utilisées lors de l'hameçonnage, prévu par les articles L.713-2 et L.713-3 du Code de la propriété intellectuelle.** Délit passible d'une peine d'emprisonnement de trois ans et de 300 000 euros d'amende.

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.