Inter//stats
Analyser pour agir

Liberté • Égalité • Fraternité
RÉPUBLIQUE FRANÇAISE
MINISTÈRE DE L'INTÉRIEUR

Insécurité et délinquance en 2016 : premier bilan statistique

Janvier 2017

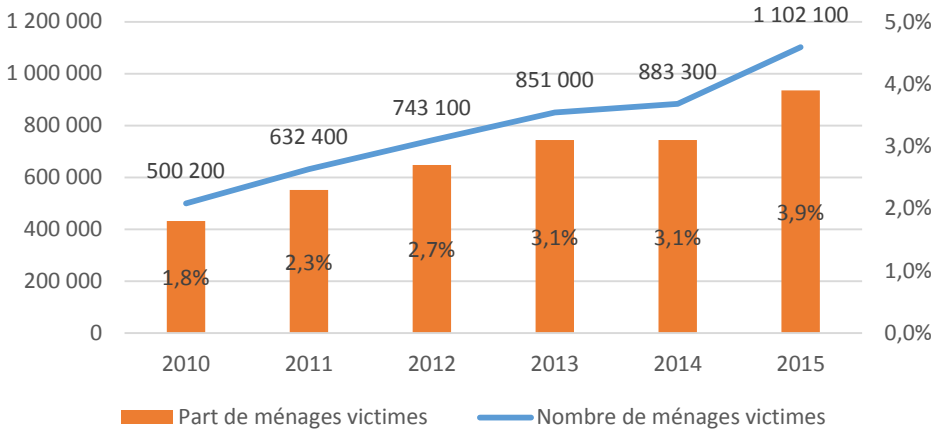
Éléments statistiques relatifs à la cybercriminalité

Avec le développement des applications informatiques dans l'environnement des entreprises et des ménages, la délinquance liée aux nouvelles technologies d'information et de communication prend de l'importance. Des études d'impact de la cybercriminalité sur la société sont conduites au moyen d'enquêtes de victimation : l'enquête « cadre de vie et sécurité » s'intéresse aux ménages et l'enquête TIC 2015 concerne les entreprises. Les conclusions de ces enquêtes sont reprises ci-dessous et sont complétées par les données administratives des plaintes pour atteinte aux systèmes de traitement automatisé de données enregistrées par les forces de l'ordre.

Les escroqueries bancaires ont plus que doublé en 6 ans

Selon l'enquête « Cadre de Vie et Sécurité » (CVS) [1], en 2015, 4 % des ménages de France métropolitaine, soit environ 1 102 000 ménages, ont déclaré avoir été victimes d'une escroquerie bancaire, définie ici comme un retrait d'argent sur un compte bancaire sans accord du titulaire en utilisant des informations personnelles, comme un numéro de carte bancaire, obtenues illégalement [2]. Le nombre de ménages possédant un compte bancaire et se déclarant victimes de débits frauduleux sur compte bancaire a plus que doublé entre 2010 et 2015 (Figure 1).

Figure 1 : Escroqueries bancaires - Nombre et part de ménages victimes



Champ : ménages ordinaires [3] de France métropolitaine.
Source : enquêtes « Cadre de Vie et Sécurité » INSEE-ONDRP-SSMSI, de 2011 à 2016. Traitement SSMSI.
Lecture : En 2015, en France métropolitaine, 1 102 100 ménages ont été victimes d'au moins une escroquerie bancaire, soit 3,9 % d'entre eux.

[1] Enquête réalisée par l'Insee est une enquête de victimation par sondage en population générale de France métropolitaine. L'enquête a lieu chaque année de janvier à mars, depuis 2007. L'objectif de l'enquête est de connaître les faits de délinquance dont les ménages et leurs membres ont pu être victimes dans un temps proche de l'enquête. Elle comporte une section sur les « escroqueries bancaires », dont un des membres des ménages interrogés a pu être victime. Les escroqueries bancaires, définies par le débit frauduleux sur compte bancaire, peuvent avoir un composant « cyber » notamment lorsqu'elles mettent en jeu l'usage d'instruments de paiement contrefaits ou falsifiés ou encore l'utilisation frauduleuse de carte bancaire ou de numéro de carte bancaire.
[2] Sont exclus du champ des escroqueries bancaires les litiges avec les créanciers, les débits résultants d'un vol de chèque, d'un vol de carte ou d'une carte oubliée dans un distributeur ainsi que les cas d'extorsion des données confidentielles par la menace ou la violence.
[3] Ménage ordinaire : Un ménage ordinaire désigne l'ensemble des personnes qui partagent la même résidence principale, que ces personnes aient des liens de parenté ou non. Les personnes vivant dans des habitations mobiles ou résidant en collectivité sont considérées comme vivant « hors ménages ordinaires ».

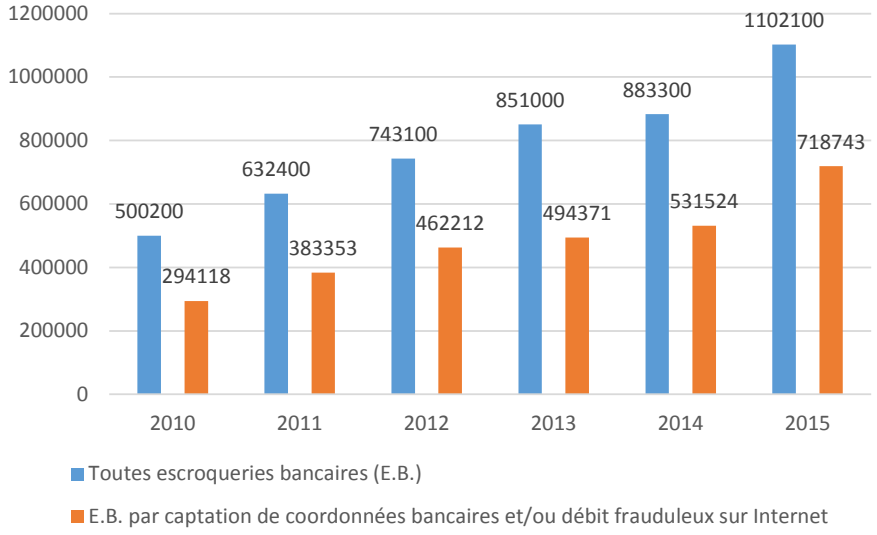
La cybercriminalité, une composante de l'escroquerie bancaire mal évaluée par les victimes [4]

La majorité des ménages victimes d'escroqueries bancaires (55 % en 2015) répondent qu'ils ignorent comment l'auteur du débit frauduleux a procédé pour obtenir des informations personnelles sur leur compte bancaire. Environ 20 % des ménages victimes affirment qu'elles ont été obtenues lors d'un achat ou d'une réservation sur internet et 7 % lors d'un achat effectué dans un commerce traditionnel. Le vol de données bancaires confidentielles lors d'un retrait d'argent à l'aide d'un dispositif installé sur un distributeur de billets (caméra ou autres) est très peu fréquemment rapporté (5 %) tout comme le vol par phishing [5] (2 %), ou par piratage d'un établissement bancaire ou commercial (3 %). Enfin, les autres ménages victimes rapportent que les auteurs ont procédé d'une autre manière que celles précédemment citées.

Si le cyberespace n'intervient qu'une fois sur cinq dans la captation des données bancaires, il est plus d'une fois sur deux le lieu de l'opération du débit : 55 % des débits bancaires frauduleux sont des débits sur des sites de commerce en ligne et 7 % sont des virements.

Le cumul de ces deux types de « cybervictimation » montre qu'en 2015 pratiquement deux tiers des ménages victimes d'escroqueries bancaires sont victimes de débits frauduleux liés à internet : leurs coordonnées ont été récoltées par internet et/ou le débit frauduleux a été effectué par cette voie [6] (Figure 2).

Figure 2 : Nombre et part de ménages victimes de captation et/ou de débit frauduleux sur internet



Champ : ménages ordinaires de France métropolitaine.
Source : enquêtes « Cadre de Vie et Sécurité » INSEE-ONDRP-SSMSI, de 2011 à 2016. Traitement SSMSI.
Lecture : En 2015, la part de débits frauduleux « cyber » est évaluée à 65,2 %. (Evaluation faite à partir du nombre de victimes d'un règlement d'un achat par carte bancaire sur un site de commerce en ligne OU d'un virement OU d'une de captation des données bancaires lors d'un achat ou réservation sur internet rapporté au nombre de victimes de débit frauduleux).

[4] *Ces données sont issues du « Rapport de l'enquête cadre de Vie et Sécurité », décembre 2016, SSMSI.*
[5] *Imitation d'un courrier électronique d'une banque ou d'une administration.*
[6] *Cette approche a été développée par B.Benbouzid et S.Peaucellier dans « L'escroquerie sur Internet, la plainte et la prise de parole publique des victimes », Réseaux, 2016/3 (n° 197-198), La Découverte.*

En 2015, 40 % des ménages victimes d'escroquerie bancaire se sont déplacés au commissariat ou à la brigade : 28 % ont formellement déposé plainte et 12 % ont déposé une main courante ou abandonné leur démarche sur place. À la différence des autres vols, dans le cas d'une escroquerie bancaire, il n'est pas nécessaire de porter plainte pour obtenir un remboursement du préjudice de la part de son établissement bancaire [7]. Cette différence notable explique au moins en partie le faible taux de plainte observé pour cette victimation.

Insécurité numérique dans les entreprises

L'enquête « TIC 2015 » sur l'utilisation des technologies de l'information et de la communication (TIC) et le commerce électronique dans les entreprises [8] porte sur 13 000 entreprises de 10 salariés ou plus en France métropolitaine. Elle prend en compte trois types de risques pour la sécurité des TIC : celui sur l'intégrité des données (destruction ou altération de données due à une attaque ou à un incident inattendu), celui sur la confidentialité des données (divulgation de données confidentielles due à une intrusion, à des attaques par pharming, phishing ou par accident) et celui sur la disponibilité des services (indisponibilité des services TIC due à une attaque extérieure, par déni de service par exemple). Les résultats principaux de l'enquête, publiés par l'Insee dans l'article « Sécurité numérique et médias sociaux dans les entreprises en 2015 » [9] paru en mai dernier, sont reproduits ci-dessous.

Fréquences des incidents

En 2015, une entreprise sur huit a connu un incident de sécurité numérique, cet incident pouvant être la conséquence d'une panne ou d'un acte de malveillance. Entre 2010 à 2015, les incidents de sécurité numérique dans l'ensemble des entreprises ont augmenté de 44 %. 13 % de l'ensemble des sociétés et 24 % des entreprises de grande taille ont subi au moins un incident de sécurité numérique en 2015 contre respectivement 9 % et 20 % en 2010. Les entreprises de 10 à 49 personnes affichent la plus forte une augmentation du nombre d'incidents de sécurité numérique : +50 %.

Les incidents concernent souvent les plus grandes sociétés et celles des secteurs d'activité fortement liées aux TIC, en raison de leur taux d'équipement et de leur usage plus élevé des TIC.

Tableau 1 : Part des sociétés ayant subi un incident informatique au cours de l'année précédente

Taille de la société	2010	2015	Variation %
10 à 49 personnes	8 %	12 %	50 %
50 à 249 personnes	13 %	19 %	46 %
250 personnes ou plus	20 %	24 %	20 %
Ensemble	**9 %**	**13 %**	**44 %**

Champ : sociétés de 10 personnes ou plus, implantées en France, des secteurs principalement marchands hors secteurs agricole, financier et d'assurance.
Source : Insee, enquêtes TIC 2010 et 2015.

[7] *À la suite de la directive communautaire sur le commerce électronique (Directive 2000/31/CE) et de l'introduction de l'article L. 133-18 du Code monétaire et financier, l'obligation est faite aux banques de rembourser immédiatement leurs clients en cas de débit non autorisé sans que la victime de la fraude n'ait à déposer une plainte. Ce remboursement, bien que conditionné par une procédure, est quasiment automatique puisque les clients n'ont pas à apporter la preuve d'une fraude.*
[8] *L'enquête sur l'utilisation des technologies de l'information et de la communication (TIC) et le commerce électronique dans les entreprises s'inscrit dans le dispositif d'enquêtes européennes. Elle est réalisée annuellement par l'Insee. L'enquête TIC vise à mieux connaître l'informatisation et la diffusion des technologies de l'information et de la communication dans les entreprises. En 2015, elle a comporté un module de questions liées à la sécurité des TIC dans les entreprise, qui répète à l'identique celui de 2010, ce qui permet des comparaisons temporelles.*
[9] *cf. « Sécurité numérique et médias sociaux dans les entreprises en 2015 », Insee Première – No 1594, paru le 10/05/2016.*

Types d'incidents

En 2015, 13 % des entreprises ont été a été victimes d'un incident sur leurs systèmes d'information. Le plus souvent, les incidents informatiques sont des pannes (8 % des sociétés en ont été victimes), mais les destructions ou altérations de données dues à l'attaque d'un programme malveillant (virus, …) ou à un accès non autorisé concernent 7 % des entreprises ; 3 % sont victimes d'une indisponibilité des services TIC, destruction ou altération de données due à une attaque extérieure (attaque par déni de service DoS, DDoS, etc.) et 2 % de la divulgation de données confidentielles due à une attaque par intrusion, pharming ou phishing. Ce sont donc plus de 20 000 entreprises qui ont été victimes en 2015 d'une indisponibilité de leurs systèmes d'information suite à une malveillance. En l'espace de 5 ans, les pannes ont augmenté de +33 %, les attaques extérieures de 50 %, les incidents dus à des programmes malveillants de +75 % et les divulgations suite à des intrusions de +100 %.

Tableau 2 : Part des sociétés par type d'incident

Type d'incident TIC	2010	2015	Variation 2010/2015
Indisponibilité des services TIC, destruction ou altération de données due à une panne de logiciel ou de matériel	6 %	8 %	33 %
Indisponibilité des services TIC, destruction ou altération de données due à une attaque extérieure (attaque par déni de service DoS, DDoS, etc.)	2 %	3 %	50 %
Destruction ou altération de données due à l'attaque d'un programme malveillant (virus, …) ou à un accès non autorisé	4 %	7 %	75 %
Divulgation de données confidentielles due à une attaque par intrusion, pharming ou phishing	1 %	2 %	100 %
Au moins un incident TIC	9 %	13 %	44 %

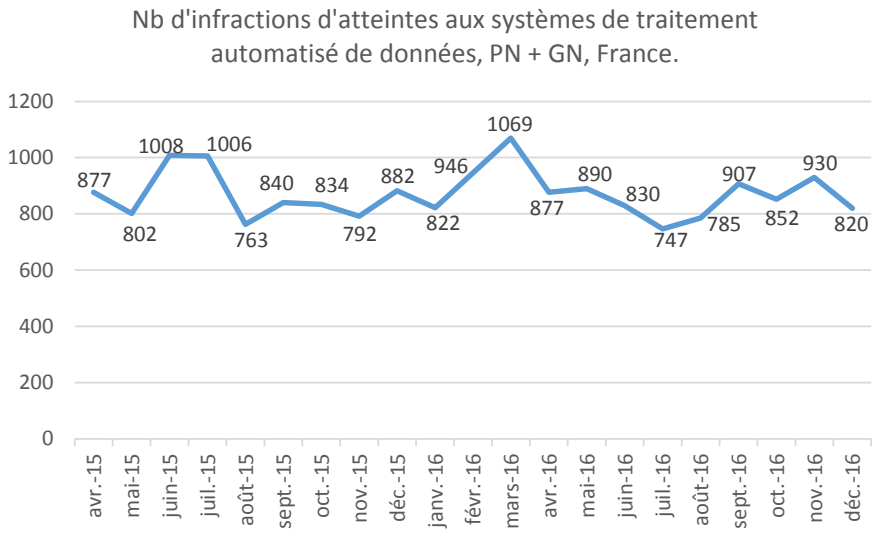
Champ : sociétés de 10 personnes ou plus, implantées en France, des secteurs principalement marchands hors secteurs agricole, financier et d'assurance.
Source : Insee, enquêtes TIC 2010 et 2015.

Données liées à la cybercriminalité issues des systèmes d'enregistrement de la police et de la gendarmerie

Les entreprises, comme les ménages, ne signalent pas à la police ou à la gendarmerie toutes les attaques dont leur système d'information est victime. Outre le fait qu'ils n'en voient pas toujours l'opportunité, cela risque dans le cas des entreprises de nuire à leur image. Il est cependant utile de compléter l'information issue des enquêtes auprès des victimes par les données reflétant les infractions enregistrées par les forces de sécurité. A ce jour, parmi les infractions relevant de la cyberdélinquance, seules les atteintes aux systèmes de traitement automatisé de données (S.T.A.D.) font l'objet d'un repérage rigoureux permettant la production de statistiques fiables.

Les systèmes d'enregistrement des forces de l'ordre permettent de suivre l'évolution des prises de plaintes pour atteintes aux S.T.A.D. Entre avril 2015 et décembre 2016, la police et la gendarmerie ont enregistré 18 279 infractions d'atteintes aux S.T.A.D., soit en moyenne 870 infractions par mois. Pour l'année 2016, 10 475 infractions ont été enregistrées par les services. Le nombre de ces infractions est relativement stable depuis le début de la série en avril 2015.

Figure 3 : Atteintes aux STAD – Nombre d'infractions mensuelles



Champ : France.
Source : SSMSI - Base des crimes et délits enregistrés par la police et la gendarmerie.
Lecture : 820 infractions d'atteintes aux STAD ont été enregistrées par les la police ou la gendarmerie en France en décembre 2016.

Les principales atteintes aux S.T.A.D.

Les accès frauduleux représentent la grande majorité (74,3 %) des atteintes aux S.T.A.D. Viennent ensuite les altérations ou entraves au fonctionnement (13,2 %), les atteintes aux données (10,1 %) et la détention [10] de moyens d'atteinte [11] aux S.T.A.D. (2,4 %). En 2016, les atteintes aux S.T.A.D. enregistrées sont en très légère hausse de 0,7 % par rapport à 2015. La détention de moyens d'atteinte augmente de 22,2 %, l'altération ou l'entrave au fonctionnement de 1,6 % et les accès frauduleux de 0,4 %. En revanche, les atteintes aux données ont diminué de 4,2 %.

Tableau 3 : Atteintes aux STAD – Nombre d'infractions par catégories

Nb infractions par catégorie d'atteinte	2015 *	2016	évolution
1 - Accès frauduleux	7 740	7 769	+0,4 %
2 - Altération ou entrave au fonctionnement	1 367	1 389	+1,6 %
3 - Atteintes aux données	1 080	1 036	-4,2 %
4 - Détention de moyens	219	281	+22,2 %
Somme annuelle	**10 405**	**10 475**	**+0,7 %**

Champ : France.
Source : SSMSI - Base des crimes et délits enregistrés par la police et la gendarmerie.
** L'année2015 est rétropolée à sur la base des données de avril à décembre*

Pour en savoir plus

— B.Benbouzid et S.Peaucellier - « L'escroquerie sur Internet, la plainte et la prise de parole publique des victimes », Réseaux, 2016/3 (n° 197-198), Ed. La Découverte - Paris
— SSMSI - « Rapport de l'enquête cadre de Vie et Sécurité », décembre 2016 ;
— ONDRP - La cybercriminalité et les infractions liées à l'utilisation frauduleuse d'internet en 2015 éléments de mesure et d'analyse in rapport annuel de l'ONDRP https ://www.inhesj.fr/fr/content/rapport-annuel-2016 le chapitre du rapport annuel de l'ONDRP sur la cyber. ONDRP - https ://www.inhesj.fr/sites/default/files/fichiers_site/ondrp_ra-016/2016_ra_cyber.pdf
— INSEE - « Sécurité numérique et médias sociaux dans les entreprises en 2015 », Insee Première – No 1594, paru le 10/05/2016. https ://www.insee.fr/fr/statistiques/2121545

[10] La détention est comprise au sens large : détention, importation, exposition, fabrication, location, offre, cession, publicité.
[11] Les moyens d'atteinte aux S.T.A.D. désignent ici l'ensemble des programmes informatiques, équipements, instruments et dispositifs techniques permettant de commettre une atteinte aux S.T.A.D.

Interstats présente des données de référence, des analyses, des études et des séries de chiffres sur l'insécurité et la délinquance mises en ligne par le service statistique ministériel de la sécurité intérieure (SSMSI).

Le SSMSI a été créé en 2014 au sein de l'administration du ministère de l'intérieur. Conformément au décret n° 2014-1161 du 8 octobre 2014, il est placé sous l'autorité fonctionnelle conjointe des directeurs généraux de la police nationale (DGPN) et de la gendarmerie nationale (DGGN) et rattaché organiquement à la direction centrale de la police judiciaire de la DGPN.

Ses missions sont :

— l'assistance aux administrations de la police et de la gendarmerie dans l'accomplissement de leurs missions, par un éclairage statistique sur la délinquance, son contexte et l'impact des politiques publiques. Ceci se traduit par la production de notes d'analyses, d'indicateurs statistiques et de tableaux de bord à destination des cabinets, des directions centrales et des services locaux de ces deux administrations, ainsi que du cabinet du ministre ;

— la mise à disposition du grand public de données statistiques et d'analyses sur la sécurité intérieure et la délinquance, dans le respect des règles techniques et déontologiques de fiabilité et de neutralité de la statistique publique. Suite à son audition par l'Autorité de la statistique publique en juin 2014, le service a été officiellement reconnu comme membre du système statistique national, au sens de la loi de 1951, par un arrêté du 9 décembre 2014, au côté de l'Insee et des 16 autres services statistiques ministériels. L'espace internet Interstats est le vecteur principal de diffusion de ces informations. Le chef du service est le seul responsable, technique et éditorial, des informations et des données qui y sont publiées, ainsi que de leurs dates de publication, conformément aux prescriptions du code des bonnes pratiques de la statistique européenne.

Dirigé par un inspecteur général de l'Insee, le service est composé de 18 agents (8 statisticiens des corps de l'Insee, 2 policiers, 2 gendarmes et 6 membres des corps administratifs et techniques du ministère de l'intérieur).

Inter//stats
Analyser pour agir

SSMSI : place Beauvau 75008 Paris
Directeur de la publication : François Clanché
Rédacteur en chef : Laure Turner
Auteurs : Dominique Baux, François Clanché, Alexandre Estival, Pierre Greffet, Marc Grenon-Mur, André Moreau, Julien Pramil, Olivier Ribon et Laure Turner
Conception graphique : Marc Grenon-Mur

Visitez notre site internet
www.interieur.gouv.fr/Interstats
Suivez-nous sur Twitter @Interieur_stats