RAPPORT NORTON SUR LA CYBERSÉCURITÉ

*Informez-vous sur les vérités de la **criminalité en ligne** et les conséquences personnelles qu'elle peut avoir.*

L'étude a été menée du 25 août au 15 septembre 2015.

Sommaire

INTRODUCTION

Pourquoi devrions-nous nous préoccuper des conséquences humaines de la cybercriminalité ?

La criminalité en ligne est aujourd'hui un fait indéniable.

348 MILLIONS D'IDENTITÉS EXPOSÉES

En 2014, plus de 348 millions d'identités ont été exposées par des **pirates** ayant usurpé l'identité de plusieurs institutions de confiance.

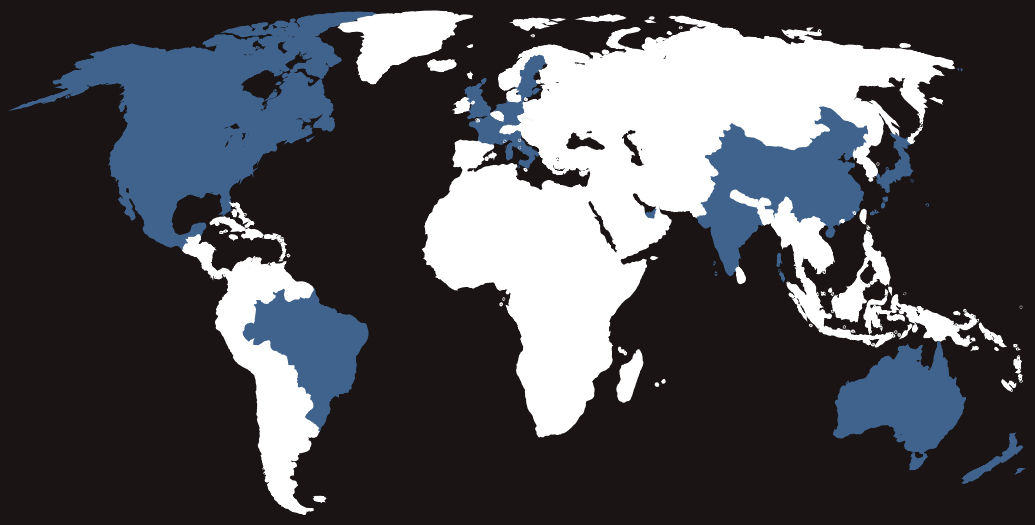
SOURCE | 2015 ISTR.

Alors que beaucoup de gens ont entendu parler de ces violations de données à un niveau sans précédent, et connaissent souvent une personne ayant été victime – voire ont été eux-mêmes victimes – ils n'ont toujours pas pris les mesures adéquates pour se protéger.

Notre étude dévoile les conséquences personnelles de la criminalité en ligne. Nous espérons que les résultats de cette étude permettront aux utilisateurs d'Internet de prendre conscience des menaces en ligne et de mieux appréhender les risques encourus afin de prendre les mesures adéquates pour les éviter.

NOUS SAVONS QUE LES RISQUES DU CRIME EN LIGNE SONT ÉLEVÉS

Les consommateurs du monde entier ont conscience du danger de la cybercriminalité.



594
MILLIONS
DE VICTIMES
DE LA CYBERCRIMINALITÉ
DANS LE MONDE

Alors que beaucoup de ces consommateurs touchés par la criminalité en ligne peuvent avoir été victimes d'une violation de données importante ou d'une autre escroquerie, la majorité des victimes n'est pas sûre de la façon d'appréhender la cybercriminalité.

Fait troublant, de nombreuses personnes vivant dans des pays où le risque est élevé sont moins susceptibles de se sentir personnellement responsables lorsque survient la criminalité en ligne.

Bien que de nombreux français pensent que le cybercrime telle que l'usurpation d'identité, est plus probable de se produire aujourd'hui que par le passé (65 %), ils estiment que leur sécurité en ligne échappe à leur contrôle. **43 %** d'entre eux pensent que les entreprises gérant leurs comptes ont plus de contrôles sur leur sécurité qu'ils n'en ont eux-mêmes.

ET NOUS CONNAISSONS – ET CRAIGNONS – LES CONSÉQUENCES

« NOUS AVONS PERDU EN MOYENNE 21 HEURES ET 328 € PAR PERSONNE AU COURS DE LA DERNIÈRE ANNÉE À CAUSE DE LA CRIMINALITÉ EN LIGNE »

Une fois qu'une personne a été victime de cybercriminalité, les conséquences sur sa vie peuvent être désastreuses. La cybercriminalité a des répercussions bien plus importantes que des questions d'argent. Nous avons perdu en moyenne 21 heures (pour avoir une idée, cela représente environ une saison entière d'une série télé) au cours de la dernière année pour gérer les répercussions d'un acte de cybercriminalité **et 328 € par personne en moyenne, ce qui représente un budget suffisant pour une surveillance domestique d'une année entière**.

Et dans la mesure où nous réalisons tant de transactions en ligne, pour payer nos factures, faire des achats ou des opérations boursières par exemple, devoir gérer une faille de sécurité de nos informations financières serait vraiment ennuyeux et handicapant.

Près de la moitié (41 %) des personnes déclarent être en colère d'avoir été victime d'un acte de cybercriminalité et **81 %** indiquent qu'elles seraient dévastées de savoir leurs données financières compromises.

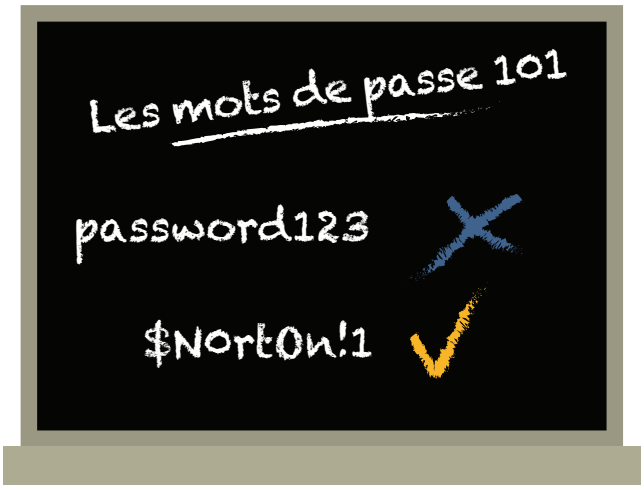
57 % des consommateurs français préfèrent annuler un dîner avec leur meilleur ami que de devoir faire annuler leur carte de débit ou de crédit.

49 % préfèreraient se rendre à un rendez-vous raté que de devoir parler avec leur service client après une faille de sécurité.

MAIS NOUS SOMMES TOUS UN PEU TROP SÛRS QUE CELA N'ARRIVE QU'AUX AUTRES

Quand il s'agit de notre propre sécurité personnelle en ligne, nous pensons que nous ne risquons rien ou presque. Si on demande aux utilisateurs d'Internet de noter leur propres comportements en ligne en ce qui concerne la protection de leur sécurité, ils s'accordent la meilleure note alors que la plupart des comportements que nous adoptons nous rendent pourtant vulnérables.

Dans la réalité, la plupart d'entre nous ne suit même pas les règles les plus basiques de sécurité, c'est à dire **les mots de passe 101**.



Parmi les utilisateurs de mots de passe, moins de la moitié utilisent « systématiquement » un mot de passe sécurisé.

Une personne sur trois n'a aucun mot de passe sur son smartphone ou sur son ordinateur de bureau !

NOUS PARTAGEONS TROP FACILEMENT NOS INFORMATIONS LES PLUS VULNÉRABLES

****

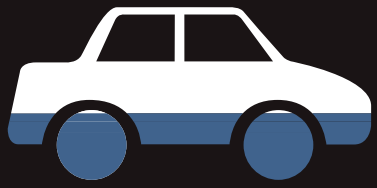
PLUS DE 1/4 (26 %) DES FRANÇAIS PARTAGEANT LEURS MOTS DE PASSE **ONT PARTAGÉ LE MOT DE PASSE DE LEUR COMPTE BANCAIRE !**

Parmi les personnes partageant leurs mots de passe dans le monde, ils l'ont fait en moyenne pour deux de leurs comptes, principalement leur message électronique **(55 %)**, leurs comptes TV/médias **(29 %)** et médias sociaux **(43 %)**.

55 %

29 %

43 %

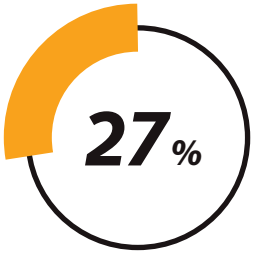


Deux personnes sur trois pensent qu'il est plus risqué de partager un mot de passe de messagerie électronique avec un ami que de lui prêter sa voiture.

GÉNÉRATION Y

Étonnamment, la génération Y a trop confiance et représente le groupe le plus vulnérable à la criminalité en ligne.

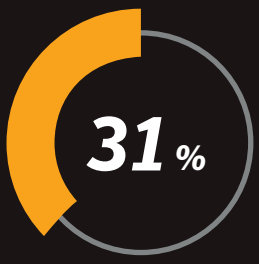
Parmi les générations qui passent le plus de temps en ligne, les personnes de la génération Y sont les plus susceptibles de faire preuve de moins de prudence. Bien qu'ils travaillent, réalisent des transactions et utilisent les médias sociaux en ligne, **27 %** des français de la génération Y ont été victimes d'un crime en ligne au cours de la dernière année.



Les digital natives se sentent les moins concernés par leur sécurité personnelle et

PRÈS DE LA MOITIÉ COMPTENT SUR LES BANQUES ET LES ENTREPRISES DE CARTES DE CRÉDIT

pour les protéger en cas de piratage.



Globalement, les personnes de la génération Y sont également les plus susceptibles de partager leurs mots de passe (**31 %**)

DANS LE MONDE : GÉNÉRATION Y VS BABY BOOMERS

Les baby-boomers sont plus avertis de la technologie qu'on aurait pu le penser.

42 % des baby-boomers utilisant des mots de passe, ont recours à des mots de passe sécurisés.

SEULEMENT 15 % des baby-boomers ont partagé leurs mots de passe.

SEULEMENT 16 % des baby-boomers dans le monde ont été victimes d'un acte de cybercriminalité l'année dernière.

Bien qu'ils n'aient pas grandit à l'ère du numérique, les baby-boomers sont plus avertis que prévu : **31 %** des consommateurs français estiment que les générations plus âgées sont les plus vulnérables à la cybercriminalité, alors que ce groupe présente des comportements en ligne plus sûrs que ceux des jeunes générations :

Ils sont moins susceptibles de partager leurs mots de passe (seulement **20 %**).

En conséquence, seuls **19 %** des baby-boomers ont connu une expérience de cybercriminalité au cours de la dernière année.

CE QUE NOUS CRAIGNONS

Nous approchons du point où les risques en ligne nous effraient plus que les risques du monde réel.

Jusqu'à récemment, les gens ne considéraient généralement pas Internet comme une source potentielle de danger comme on peut l'entendre de la vie réelle. Le directeur du FBI, James Comey, a appelé Internet, « le parking le plus dangereux possible » et a mis en garde la population, nous invitant à prendre conscience de l'existence des escroqueries, des sites Web compromis, des logiciels malveillants et des autres menaces qu'il peut présenter au même titre que la vraie vie.

Heureusement, les consciences s'éveillent et les gens comprennent le niveau de risque de notre vie en ligne :

6 consommateurs sur 10 pensent que les Wi-Fi publics sont plus risqués que des toilettes publiques.

Les consommateurs du monde entier pensent que les risques de se faire voler leurs informations de carte de crédit en ligne sont deux fois plus importants que de se faire voler leurs portefeuilles.

4 personnes sur 5 sont inquiètes d'être victime de cybercriminalité.

65 % des consommateurs français pensent que le vol d'identité est plus susceptible de se produire aujourd'hui qu'il ne l'a jamais été auparavant.

LA MOITIÉ

des consommateurs français **(50 %)** pensent que conserver leurs informations bancaires ou de carte de crédit dans le cloud

EST PLUS RISQUÉ QUE DE NE PAS PORTER DE CEINTURE DE SÉCURITÉ.

51 % des parents du monde entier considèrent

LE HARCÈLEMENT EN LIGNE

PLUS PROBABLE DE SE PRODUIRE QUE LE HARCÈLEMENT À L'ÉCOLE OU AU TRAVAIL (49 %).

LA CYBERSÉCURITÉ EN PRATIQUE DANS UN MONDE D'ÉVOLUTIONS TECHNOLOGIQUES.

Vous ne pouvez pas toujours savoir qui se cache là-bas dans les « limbes » mais voici quelques conseils pour vous assurer votre sécurité :

1) Choisissez un mot de passe intelligent, sécurisé et unique pour chaque compte que vous avez en ligne. Pour obtenir des conseils sur la façon de procéder, **cliquez ici**.

2) Supprimer les e-mails provenant d'expéditeurs que vous ne connaissez pas et ne cliquez pas sur les pièces jointes ou des liens des e-mails suspects.

3) Sur les sites de médias sociaux, si une offre semble trop belle pour être vraie, c'est peut-être bien le cas. Évitez de cliquer sur des publications qui offrent un « voyage gratuit pour Tahiti ». surtout si elles ne viennent pas directement d'une page d'entreprise digne de confiance et « officielle ».

4) Faites un suivi régulier de vos comptes bancaires pour vous assurer qu'aucune activité inhabituelle n'y apparait. Si vous voyez une dépense que vous n'avez pas faite, signalez-la immédiatement. Souvent, les cybercriminels prélèvent un tout petit montant pour vous « tester » avant d'essayer de vider votre compte en banque.

5) Ne repoussez pas la mise à jour de votre logiciel. Oui, ces pop-ups de mise à jour sont ennuyeux, mais les mises à jour contiennent souvent des correctifs importants pour les failles de sécurité dangereuses que les cybercriminels peuvent utiliser pour accéder à votre appareil.

6) Utilisez une solution de sauvegarde sécurisée pour protéger vos fichiers et sauvegardez régulièrement vos données afin que les criminels ne puissent pas les retenir et les échanger contre une rançon.

7) Utilisez une protection multicouche de confiance offrant un support et une promesse 100 % contre les virus* comme **Norton Security**. Vous en avez pour votre argent. Il y a tant d'escrocs en ligne visant vos appareils et toutes les informations qu'ils contiennent, cela vaut la peine de payer un logiciel de sécurité complet.

Pour plus d'informations sur la façon intelligente de rester protégé, visitez le **Blog Norton Protection** sur la communauté Norton.

*Soumis à conditions. Pour en bénéficier, achetez, renouvelez ou mettez à jour votre abonnement Norton directement auprès de Symantec, ou enregistrez-vous au service de renouvellement automatique Norton™
Consultez la page fr.norton.com/nortonlive/information.jsp?type=guarantee&sel=y&ctsel=28 pour plus de details.

AVANCEZ CONFIANT, PAS AVEUGLÉMENT