



# GUIDE DE LA SECURITE EN LIGNE POUR LES CYBER-SENIORS

TRUCS ET ASTUCES SUR COMMENT SECURISER SON ORDINATEUR ET SES  
ACTIVITES SUR INTERNET

SABINA DATCU, IOANA JELEA  
SPECIALISTES EN COMMUNICATION ET ANALYSE DES E-MENACES

## Table des matières

Table des matières .....	2
Les seniors sont-ils une cible pour les cybercriminels ?.....	4
Savoir ce qui vous attend sur Internet.....	6
Q1 : Qu'est-ce que le malware ? .....	6
Q2 : Qu'est-ce que le hameçonnage ? .....	6
Q3 : Qu'est-ce que le spam ? .....	7
Q4 : Qu'est-ce que le spyware ? .....	7
Q5 : Qu'est-ce que le adware ? .....	7
Q6 : Qu'est-ce qu'un virus ? .....	7
Q7 : Qu'est-ce qu'un cheval de Troie ? .....	8
Q8 : Qu'est-ce qu'un faux logiciel antivirus ? .....	8
Q9 : Qu'est-ce qu'un keylogger ? .....	9
Etudes de cas .....	10
<i>Les seniors en tant que cibles principales</i> .....	10
Spam concernant les pensions.....	10
Méthodes mensongères de règlement des impôts .....	10
Spam concernant les revenus.....	11
<i>Les seniors en tant que cibles secondaires</i> .....	12
Attaque d'hameçonnage des clients d'AOL.....	12
Distribution de faux logiciels antivirus.....	13
Diffusion de malware par courrier électronique .....	14
Les règles d'or de la sécurité du senior en ligne.....	15
<i>Quand vous naviguez sur le net</i> .....	15

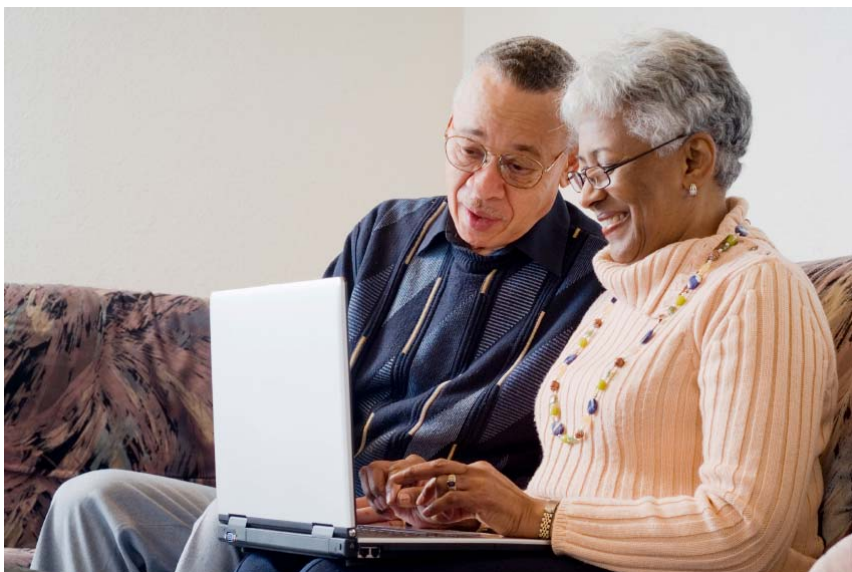
Protection de l'ordinateur.....	15
Version du navigateur et sécurité.....	16
Protection des données personnelles.....	17
<i>Quand vous utilisez la messagerie électronique.....</i>	<i>17</i>
Pour éviter les mails non sollicités.....	17
<i>Quand vous utilisez des applications de messagerie instantanée.....</i>	<i>17</i>
<i>Quand vous effectuez des paiements en ligne.....</i>	<i>18</i>
<i>N'ayez pas peur de porter plainte.....</i>	<i>19</i>
Choisir une solution de sécurité des données.....	20
<i>Existe-t-il un problème de langue ?.....</i>	<i>20</i>
<i>La solution répond-elle à tous mes besoins ?.....</i>	<i>21</i>
<i>A quel degré devrai-je m'impliquer ?.....</i>	<i>22</i>
<i>Puis-je obtenir de l'aide ?.....</i>	<i>23</i>

## Les seniors sont-ils une cible pour les cybercriminels ?

A priori, on pourrait penser que les seniors sont exposés à la cybercriminalité au même titre que les autres utilisateurs inexpérimentés d'Internet, quel que soit leur âge. Néanmoins, en règle générale, pour rendre leurs pièges efficaces, les cybercriminels ont tendance à faire appel à des traits courants de la psychologie humaine comme la curiosité, la cupidité, l'empathie.

Pourquoi les internautes seniors sont-ils visés par ce "traitement spécial" ? D'après une série de conseils de précaution contre les escroqueries publiée sur le site web du FBI sous le titre [Fraud Target: Senior Citizens](#) (Les seniors : une cible pour les escrocs), l'expérience a montré que les seniors constituaient la cible privilégiée des cybercriminels en raison de la conjugaison de facteurs psychologiques, économiques et sociaux particuliers, propres à cette classe d'âge, facteurs qui peuvent se résumer ainsi :

- 1) Les seniors sont en général pris pour cible parce qu'il y a plus de chance qu'ils aient de l'argent, qu'ils aient économisé toute leur vie, soient devenus propriétaires ou aient fait des investissements rentables.
- 2) Du fait de l'éducation qu'ils ont reçue, les seniors ont tendance à être plus confiants et moins au courant de l'évolution des techniques d'escroquerie. Si l'on ajoute une plus grande probabilité qu'ils vivent seuls (que leur famille soit très occupée ou qu'ils n'en aient pas), on obtient un ingrédient très important du mélange : il est probable qu'ils n'ont personne à qui demander conseil. D'autre part, en fonction de leur expérience passée, ils peuvent être vulnérables dans des situations au cours desquelles ils sont confrontés à des étrangers « bienveillants » ou, à l'inverse, plutôt méfiants dans de tels cas.



3) En supposant qu'ils n'ont été que très récemment familiarisés avec les ordinateurs et Internet, les seniors, exactement comme n'importe quel autre débutant dans ce domaine, sont probablement moins à même de se rendre compte immédiatement qu'ils ont été victimes de cybercriminalité. Le délai entre la survenue de l'événement et sa révélation peut poser quelques problèmes en fonction de la manière dont les victimes arrivent à se souvenir des détails de leurs activités en ligne.

4) L'espoir que suscitent les progrès de la science médicale, associé à la nécessité de faire face à différentes situations liées à l'âge, rend très séduisante pour les seniors la perspective de bénéficier de nouveaux médicaments, traitements et vaccins. De ce point de vue, une autre motivation peut naître de la promesse de bénéficier de prix bas.

Un autre élément à prendre en considération, mais qui n'est pas lié à l'âge, est que les gens sont généralement peu enclins à faire part des incidents dont ils ont été victimes en ligne, soit parce qu'ils en sont honteux, soit parce qu'ils ne savent pas à quel service de police s'adresser. Ceci retarde les procédures de recherche, ralentit la vitesse de réaction des autorités et allonge pour les personnes concernées le délai d'obtention de la réparation.

Il existe donc bien un certain degré de vulnérabilité chez les utilisateurs d'Internet de la catégorie des seniors, mais il est également vrai que, de beaucoup d'autres points de vue, tous les utilisateurs d'Internet sont exposés aux menaces électroniques s'ils ne sont pas correctement informés. Dans la mesure où la connaissance de l'informatique devient une composante des systèmes éducatifs, ce problème deviendra moins important quel que soit l'âge. D'un point de vue pratique, si toutes les personnes ayant accès à l'éducation acquerraient une connaissance de base de l'informatique, leurs compétences dans ce domaine n'auraient alors plus de lien avec leur âge.



## Savoir ce qui vous attend sur Internet



Le conseil le plus important à suivre est de vous familiariser avec ce qu'Internet peut faire et avec les applications que vous êtes susceptibles d'utiliser en ligne (navigateurs, forums de discussion, paiement en ligne, etc.). Essayez de trouver une source d'informations fiable sur les actions potentiellement dangereuses qui peuvent être commises en utilisant chacune de ces applications. N'ayez pas peur de demander « Que se passe-t-il si je fais ceci ? » car toute question est importante s'agissant de votre sécurité sur le Net. Quantité d'informations sur ces sujets et d'autres sont disponibles sur [le site web de BitDefender](#) et sur [le blog sur la sécurité de BitDefender](#).

Evidemment, connaître quels risques vous prenez quand vous entreprenez une activité spécifique en ligne vous rendra moins susceptible de tomber dans les pièges des cybercriminels. Voici quelques questions et réponses à consulter avant d'utiliser Internet :

### Q1 : Qu'est-ce que le malware ?

Ce terme désigne tout type de logiciel créé dans une intention malveillante et destiné à endommager votre ordinateur, nuire à son fonctionnement, rendre vos données inutilisables, s'emparer de vos coordonnées confidentielles pour obtenir de l'argent, etc.

### Q2 : Qu'est-ce que le hameçonnage ?

Il s'agit du nom donné à un mécanisme conçu par les cybercriminels pour inciter les gens à leur fournir des informations confidentielles (numéros de cartes de paiement, codes PIN...). Pour obtenir ces informations, ils créent des sites qui se présentent comme des pages web légitimes (banques, réseaux sociaux, services gouvernementaux, etc.). Croyant avoir affaire aux sites véritables, les utilisateurs entrent leurs données et s'exposent au risque de se faire voler de l'argent.

### Q3 : Qu'est-ce que le spam ?

Le spam est le nom que l'on donne à des courriers électroniques non sollicités envoyés à une multitude de gens, en général pour faire la publicité de divers produits. Ces courriers sont également utilisés comme des leurres masquant des activités plus malveillantes, comme le hameçonnage.

### Q4 : Qu'est-ce que le spyware ?

Il s'agit de programmes qui installent sur votre ordinateur, à votre insu, ce qui s'apparente à un œil étranger regardant par-dessus votre épaule ce que vous êtes en train de faire, ce que vous voulez et ce que vous êtes en train de rechercher. En général, cet inconnu curieux est un pirate ou un autre genre de cybercriminel.

### Q5 : Qu'est-ce que le adware ?

Il s'agit de programmes qui permettent l'ouverture intempestive de fenêtres sur votre écran et d'afficher des publicités sur des produits susceptibles de vous intéresser. Comment ces programmes sont-ils informés de vos préférences ? C'est ici que le spyware intervient.

### Q6 : Qu'est-ce qu'un virus ?

C'est un programme malveillant conçu pour perturber vos activités sur ordinateur en endommageant votre système d'exploitation et en altérant les informations stockées dans votre système ou en les rendant inaccessibles. A la différence des autres types de logiciels malveillants, un virus est capable de se dupliquer et d'envahir tout l'ordinateur. En infestant un support amovible (par exemple un CD, un DVD ou un lecteur USB), le virus peut facilement se répandre également sur d'autres ordinateurs.

## Q7 : Qu'est-ce qu'un cheval de Troie ?

Comme son nom l'indique bien, c'est un programme, apparemment inoffensif, qui permet en fait à un pirate de prendre le contrôle de votre système. Une fois installé, le cheval de Troie donne au pirate la possibilité de s'emparer de vos données, d'installer d'autres logiciels malveillants et, de manière générale, de surveiller et perturber votre activité informatique.

Même après avoir dépassé ce premier stade de familiarisation, n'hésitez pas à poser des questions si vous avez des doutes sur ce que vous devez faire en ligne ou sur les conséquences éventuelles que vos opérations pourraient entraîner. Autrement dit, il est préférable de s'informer régulièrement des précautions à prendre pour naviguer en sécurité sur le web plutôt que de refuser en bloc d'accéder à tout un monde de ressources en ligne parce qu'il constitue une source de dangers sous-jacents. Tout ceci peut sembler difficile à gérer, mais une fois que vous aurez installé et utiliserez une solution de sécurité fiable, la plupart des problèmes de sécurité seront pris en charge sans aucune intervention de votre part.

## Q8 : Qu'est-ce qu'un faux logiciel antivirus ?

C'est un programme malveillant qui tente de vous convaincre de le télécharger en se faisant passer pour un antivirus. Au départ, plusieurs fenêtres s'affichent pour vous signaler une série de problèmes de sécurité détectés sur votre PC. Ces problèmes n'existent pas, l'avertissement a pour but de créer la panique. Si vous acceptez de télécharger ce qui vous est présenté comme un antivirus qui va les résoudre, votre PC sera infecté. Ce qui signifie que vous serez espionné de toutes les manières possibles, le sommet étant atteint lorsque des cybercriminels prennent le contrôle total de votre système.



## Q9 : Qu'est-ce qu'un keylogger ?

Le keylogger surveille votre activité en enregistrant sur quelles touches de votre clavier vous appuyez. Ces applications peuvent véhiculer d'autres caractéristiques, comme la capacité de diffuser sur Internet les résultats de leur surveillance, de faire des saisies de votre écran, etc. Certains keyloggers peuvent même s'emparer des mots de passe apparaissant à l'écran comme une suite d'astérisques.

## Etudes de cas

From: "DR. ROBERT MUELLER" <[redacted]@[redacted].gov>  
 Reply-To: <[redacted]>  
 Subject: YOUR DECEMBER PENSION  
 Date: Sun, 27 Dec 2009 11:54:04 +0100  
 To: [redacted]

Attn: Beneficiary,

This is to Officially inform you that it has come to our notice and we have thoroughly Investigated with the help of our Intelligence Monitoring Network System that you are having an illegal Transaction with Impostors claiming to be Prof. Charles C. Soludo of the Central Bank Of Nigeria, Mr. Patrick Aziza, Mr Frank Nweke, none officials of Oceanic Bank, Zenith Banks, Barrister Bayo Duke, kelvin Young of HSBC, Mr Kolawole, Ben of Fedex, Ibrahim Sule, Larry Christopher, Puppy Scammers are impostors claiming to be the Federal Bureau Of Investigation. During our Investigation, we noticed that the reason why you have not received your payment is because you have not fulfilled your Financial Obligation given to you in respect of your Contract Inheritance Payment.

Therefore, we have contacted the Federal Ministry Of Finance on your behalf and they have brought a solution to your problem by coordinating your payment in total USD\$950,000.00 in an ATM CARD which you can use to withdraw money from any ATM MACHINE CENTER anywhere in the world with a maximum of \$4000 to \$5000 United States Dollars daily. You now have the lawful right to claim your fund in an ATM CARD.

Since the Federal Bureau of Investigation is involved in this transaction, you have to be rest assured for this is 100% risk free. All I want you to do is to contact the ATM CARD CENTER via email for their requirements to proceed and procure your Approval Slip on your behalf which will cost you \$245.12 only and note that your Approval Slip which details of the agent who will process your transaction.

CONTACT INFORMATION  
 NAME: Mr. Smith Marucs  
 EMAIL: mdr.[redacted]  
 TELEPHONE NUMBER: +234 [redacted]  
 Do contact Mr. Mr. Smith Marucs of the ATM CARD CENTRE with your details with your reference number Ref:No1226/X42/206:  
 FULL NAME:  
 ADDRESS:  
 TELL:  
 CELL:  
 CURRENT OCCUPATION:

Fig. 1 - Spam décrivant un problème de paiement d'une pension

Les menaces électroniques dirigées contre les seniors peuvent être classées en deux catégories principales : dans la première ils sont visés directement, dans l'autre indirectement. Les quelques études de cas qui suivent illustrent les modes opérationnels et les conséquences dans les deux cas.

### Les seniors en tant que cibles principales

Le malware vise directement les seniors en diffusant, notamment sous forme de spam prétextant des erreurs dans l'envoi d'une pension, de prétendues méthodes de réduction d'impôt - spam presque toujours accompagné de malware- et, parfois, de fausses offres d'emploi destinées aux personnes retraitées.

### Spam concernant les pensions

Ce premier exemple présente un spam signalant une prétendue erreur dans l'envoi d'une pension. Pour convaincre le destinataire de sa légitimité, le message est formulé dans un langage administratif. En fait son objectif réel est de dérober des informations sensibles comme le nom, l'adresse, le numéro de téléphone, la profession de l'utilisateur.

### Méthodes mensongères de règlement des impôts

Le second exemple a trait à des méthodes mensongères de règlement des impôts. En utilisant de séduisantes photos de seniors sur fond de vie quotidienne, ces sites arrivent à convaincre leurs visiteurs de communiquer des renseignements personnels, y compris leur nom, leur adresse, ou leur numéro de compte bancaire. Une fois en possession de ces éléments clés, il ne reste plus aux cybercriminels qu'à tranquillement puiser dans les comptes auxquels ils ont illégalement eu accès.

AmericanTaxDebtRelief  
 LIVE FREE OF TAX DEBT

Find Out How **LOW** You Can Settle Your IRS Debt  
 If you owe more than \$10,000 to the IRS we can help!

Start the process of financial freedom today!

Fill out our 60 second form to receive a **FREE ANALYSIS!**

**Start Here for Tax Relief**

Amount Owed

Do You Have a Tax Lien?  Yes  No

Address

Zip Code

First Name

Last Name

Email

Home Phone

Alternate Phone

**Click Here to Get Started Now!**

All information is strictly confidential.

Fig. 2 Page web décrivant une méthode mensongère de règlement des impôts

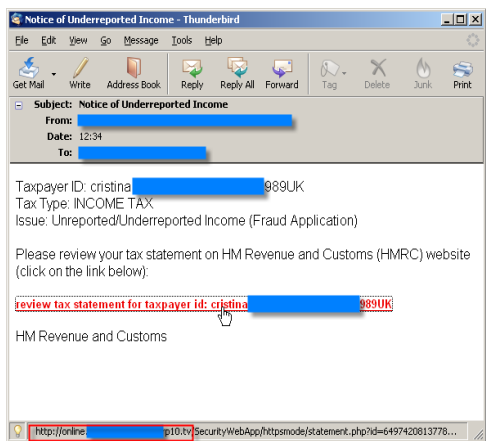
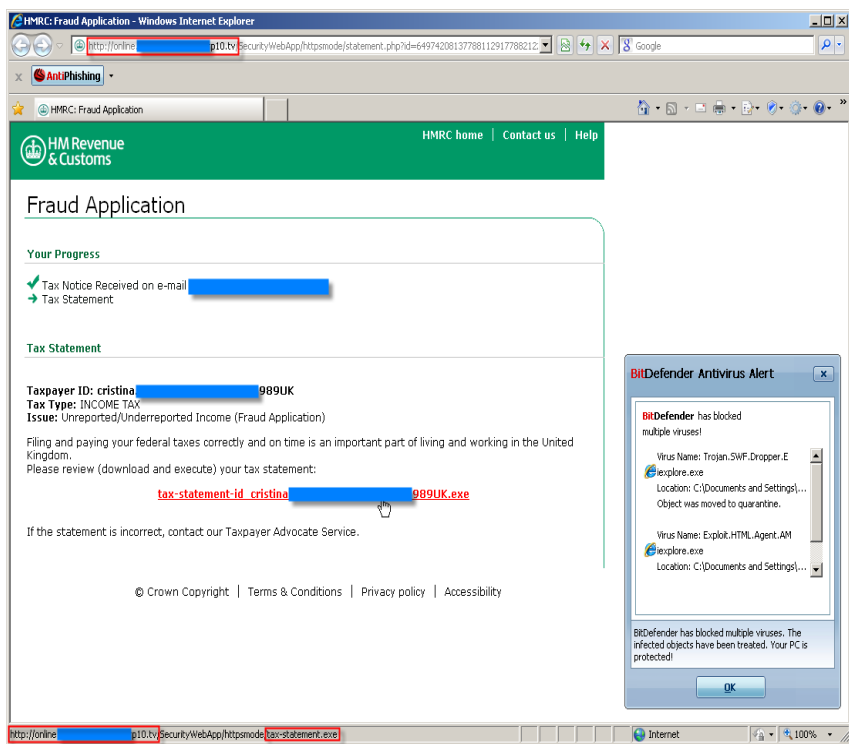


Fig. 3 et 4 - Spam lié aux revenus (ci-dessus) et page web factice prétendant fournir aux utilisateurs un moyen de revoir leur déclaration de revenus (ci-dessous)



## Spam concernant les revenus

Le troisième exemple présente un message non sollicité demandant aux destinataires de revoir et corriger leur déclaration d'impôt. Ce message, identique à celui précédemment utilisé pour mystifier les destinataires des envois imitant ceux du fisc, est un leurre destiné à récolter des données.

Le prétendu lien proposé n'aboutit pas au site web du fisc, mais à une page web de téléchargement qui l'imité, comportant plusieurs éléments d'identification visuelle du site d'origine : logo, en-tête, formatage.

La page propose également un lien vers ce qui ressemble à une déclaration que l'utilisateur doit télécharger et remplir. En dépit de cette apparente légitimité, après avoir cliqué sur le lien, l'utilisateur ne reçoit pas un formulaire électronique, mais un cocktail explosif de malveillances, comme le montre l'image ci-contre.



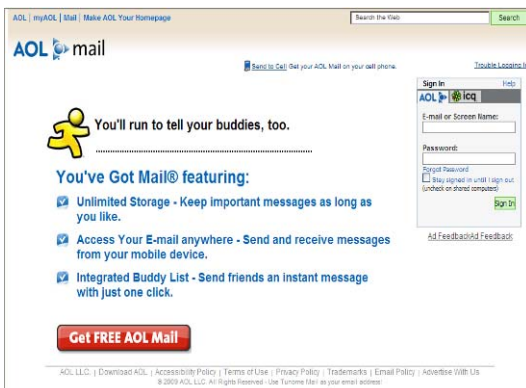


Fig. 5 et 6 - Page web factice d'une tentative d'hameçonnage de clients d'AOL (ci-dessus) et (ci-dessous) formulaire en ligne destiné à obtenir des données sensibles (ex : n° de sécurité sociale)

## Les seniors en tant que cibles secondaires

Les menaces électroniques visant indirectement les seniors consistent en faux logiciels antivirus, malware, tentatives de hameçonnage ou sites web infectés. Sur le plan pratique, leur démarche est indirecte en ce sens qu'elles n'ont pas été conçues pour concerner les seniors en particulier, mais qu'elles les englobent. Ces méthodes sont prises en considération dans ce guide car elles constituent d'importantes sources de malware et que les seniors doivent en être avertis.

## Attaque d'hameçonnage des clients d'AOL

Les clients d'AOL trouvent dans leur boîte aux lettres un message apparemment légitime dans lequel il leur est demandé de mettre à jour leurs données personnelles. Le processus de hameçonnage qui s'ensuit est simple et vise plusieurs cibles à la fois : les comptes utilisateurs des clients d'AOL, les données personnelles sensibles et les autres informations requises pour « récupérer son mot de passe ».

Le faux message électronique censé provenir d'AOL met les utilisateurs en demeure de fournir les renseignements demandés en fixant une limite impérative –le 31 janvier- et en précisant que faute de réponse, leur compte sera suspendu.

Cet e-mail contient également un lien spécial sur lequel les utilisateurs doivent cliquer pour confirmer leur compte électronique AOL et leur mot de passe. Le lien aboutit à une fausse page web AOL, astucieusement conçue pour tromper les utilisateurs naïfs.

Et le hameçonneur devient plus gourmand : l'étape suivante conduit les utilisateurs d'AOL à une page où ils sont censés communiquer différentes informations personnelles comme leur nom, leur adresse, le numéro de leur carte de paiement, leur numéro de sécurité sociale.

Et pour finir se glisse la demande d'une information apparemment anodine : nom de jeune fille de la mère. En sachant que ce renseignement sert à récupérer le mot de passe correspondant à des adresses électroniques ou des comptes bancaires en ligne, cette dernière manœuvre devrait déclencher une bruyante sonnette d'alarme.

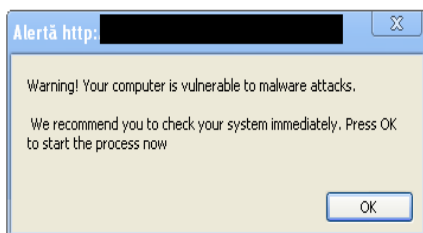


Fig. 7 - Fausse alerte relative à un prétendu problème de sécurité sur le PC de l'utilisateur

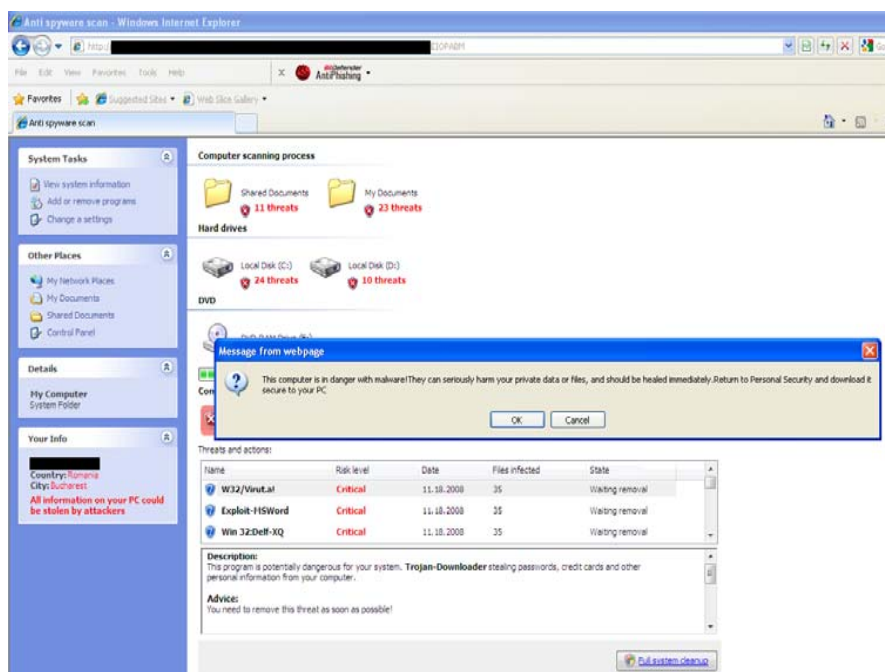


Fig. 8 Après une analyse simulée, l'utilisateur est invité à télécharger le faux antivirus supposé être une solution de sécurité

## Distribution de faux logiciels antivirus

Les cybercriminels continuent de compter sur la curiosité de leurs victimes pour les inciter à compromettre leurs données. Par le procédé « Sujets brûlants Internet », la diffusion du malware est simple et classique : quand l'utilisateur naïf clique sur le lien vers un site web apparemment légitime affiché dans la page de résultats de la recherche, le navigateur est automatiquement redirigé vers une page web qui infecte l'ordinateur avec un faux antivirus.

Le comportement du programme malveillant dans ce cas est comparable à celui d'autres faux antivirus : quand l'utilisateur est redirigé vers la page web de distribution du [malware](#), la fenêtre du navigateur est réduite automatiquement et un message d'alerte s'affiche en même temps. Ce message informe l'utilisateur de plusieurs prétendues infections de son ordinateur et souligne la nécessité d'installer une solution de sécurité.

En cliquant sur le bouton OK ou Annuler des différentes fenêtres qui s'affichent à l'écran, l'utilisateur active une fausse démonstration qui se déploie dans la fenêtre restaurée du navigateur. Cette démonstration imite un processus d'analyse qui détecte des quantités de malware sur le PC, pendant que d'autres fausses fenêtres tentent d'inciter l'utilisateur à télécharger le programme malveillant se faisant passer pour l'antivirus.

A chaque pseudo analyse, un nombre croissant de notifications de fausses détections presse l'utilisateur d'enregistrer le faux antivirus. Une fois installé, ce dernier modifie ou endommage irrémédiablement le contenu de plusieurs fichiers systèmes et ouvre de nombreuses fenêtres sur des problèmes fictifs et des infections inexistantes, tout en continuant aussi à demander à l'utilisateur d'acheter ou de renouveler une licence.

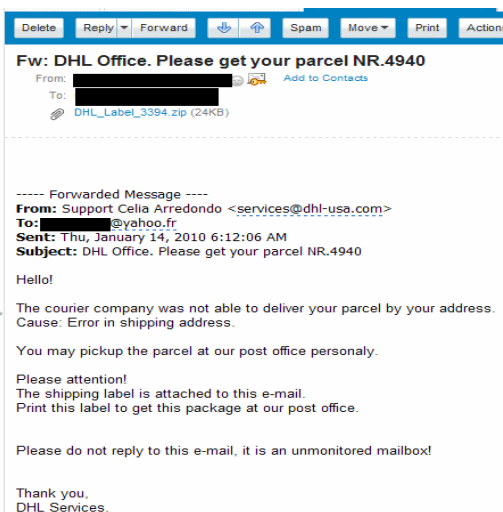
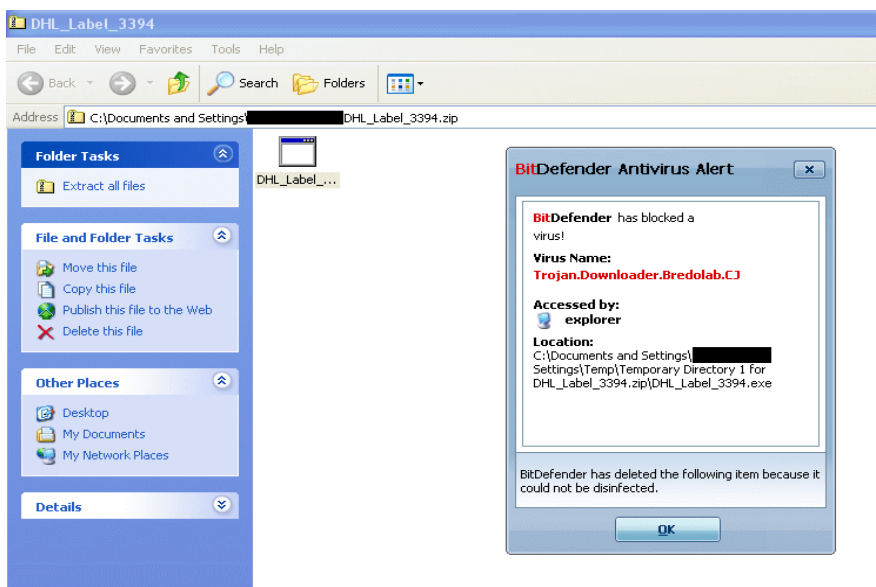


Fig. 9 et 10 - E-mail avec pièce jointe utilisée pour propager du malware (ci-dessus) et alerte antivirus affichée au moment de l'ouverture de la pièce jointe malveillante (ci-dessous)



## Diffusion de malware par courrier électronique

Il existe une catégorie de spam qui utilise frauduleusement des noms de marques très connues pour diffuser du malware. Ce qui suit est un exemple de ce type de spam.

Un e-mail non sollicité déclare qu'une entreprise de transport bien connue rencontre un problème pour livrer un colis parce que l'adresse postale est incorrecte. Dans ce cas, le destinataire de la notification est invité à imprimer une étiquette, jointe au courrier en tant que fichier .zip, et de l'utiliser pour aller retirer son colis à la poste.

Mais le message n'a pas été émis par l'entreprise véritable et la déclaration prétendant que la livraison du colis a échoué à cause d'une erreur d'adresse est fausse. Le colis n'existe pas et le message n'est qu'une ruse conçue pour inciter le destinataire crédule à télécharger la pièce jointe. S'il le fait, l'utilisateur reçoit du malware au lieu d'une étiquette.

Une fois installé dans le système, ce malware peut essayer de télécharger et installer d'autres menaces électroniques, comme des keyloggers, des voleurs de mots de passe et de faux logiciels antivirus.

Les techniques de manipulation des structures sociales (*social engineering*) qui sous-tendent cette campagne de distribution de malware ont prouvé leur efficacité. Que les destinataires utilisent les services de l'entreprise authentique et attendent effectivement un colis, ou qu'ils pensent que quelqu'un leur a envoyé un cadeau, ou qu'ils soient simplement curieux de consulter la pièce jointe, il est probable qu'ils vont tomber dans le piège. Dans tous les cas, le résultat est le même : ouvrir le fichier pour voir ce qu'il contient et pour finir... contracter une infection.

## Les règles d'or de la sécurité du senior en ligne



Respectez quelques règles de bon sens élémentaire pour votre sécurité en ligne. En d'autres termes, ne prenez pas plus de risques en ligne que vous n'en prendriez dans la réalité au cours de vos activités quotidiennes. Le soir vous fermez votre porte, dans la rue vous ne donnez pas le numéro de votre compte bancaire au premier venu. C'est exactement la même chose dans le cyber espace : ne permettez pas à des internautes inconnus d'accéder à votre ordinateur ou à vos données personnelles.

Voici une liste de mesures préventives qui vous aideront à rester en sûreté au cours de vos expériences en ligne.

### Quand vous naviguez sur le net

#### Protection de l'ordinateur

La première chose à faire est d'installer, d'activer, et de mettre continuellement à jour une solution antimalware fiable, apte à vous protéger contre une vaste gamme de menaces électroniques (virus, hameçonnage, spam, etc.). Les solutions de sécurité des données de [BitDefender](#), par exemple, sécuriseront toutes vos activités en ligne. Ce qui signifie que vous serez averti chaque fois que vous vous trouverez dans une situation susceptible d'être dangereuse pour vous, par exemple au moment d'accéder à un site contrefait. Par ailleurs, l'ensemble des outils de sécurité bloqueront tous les virus comme les autres menaces électroniques avant qu'ils puissent endommager votre ordinateur et vos données. Installer et activer une solution de ce type ne prend que quelques minutes et le processus de mise à jour est automatique.

Une fois franchie cette première étape, vous êtes armé pour explorer le web.

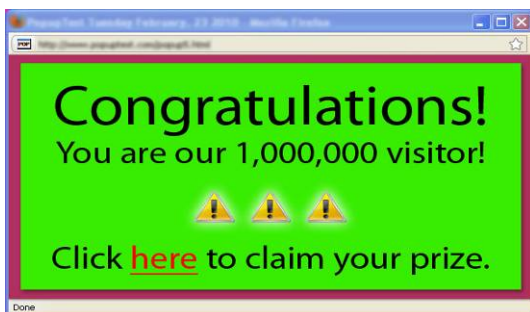


Fig. 11 - Exemple d'une fenêtre intempesitive annonçant au visiteur qu'il a gagné un cadeau



Fig. 12 - Fausse alerte de sécurité



Fig. 13 - Page web factice de présentation d'un produit, exemple de l'arsenal utilisé par les cybercriminels pour vous persuader que vous êtes sur le point de télécharger une vraie solution de sécurité

## Version du navigateur et sécurité

Une autre opération, simple mais efficace, est de vous assurer que vous utilisez bien la plus récente version de votre navigateur Internet (Microsoft® Internet Explorer, Mozilla Firefox, etc.). De cette manière, vous ne serez pas importuné par des fenêtres publicitaires (pop-ups). Les mises à jour des versions des navigateurs sont dans la plupart des cas automatiques. Cependant, si vous souhaitez savoir quelle version vous utilisez ou comment la mettre à jour, consultez la section 'A propos de' dans le menu Aide de votre navigateur, ou bien ouvrez le navigateur et appuyez sur la touche F1.

Quand vous accédez à certaines pages web, de petites fenêtres peuvent s'afficher et tenter de vous persuader de cliquer dedans sous différents prétextes : gagner quelque chose, essayer un nouveau jeu, accéder à une autre page web. Dans la plupart des cas, votre navigateur bloquera ces fenêtres, car cette fonctionnalité est activée automatiquement.

Cependant, si des fenêtres apparaissent lorsque vous naviguez sur le web, évitez de cliquer sur les liens qu'elles présentent, parce que vous ne savez jamais ce qui peut se cacher derrière.

N'installez jamais un logiciel sur votre ordinateur sans avoir d'abord consulté un professionnel, par exemple le conseiller du magasin d'informatique le plus proche de chez vous, ou un parent compétent dans le domaine.

Méfiez-vous des fenêtres qui vous invitent à télécharger un logiciel pour vous protéger contre un prétendu problème de sécurité.

Si vous cliquez sur le lien fourni, vous vous retrouvez probablement sur une page web qui semble tout à fait correcte mais qui constitue en réalité une brèche par laquelle le malware sera téléchargé sur votre ordinateur.



虎年吉祥

138185053591@on165.com

To: [redacted].com

有piao可以优惠对外开出, 请问: 13410120100小高

Fig. 14 - Exemple d'une ligne objet suspecte dans un e-mail

## Protection des données personnelles

N'entrez pas votre adresse électronique ni d'autres informations personnelles sur des sites suspects. De même, évitez de donner votre e-mail dans des livres d'or, des forums, etc. Vous éviterez ainsi de voir votre boîte de réception inondée de messages spam et resterez protégé contre l'usurpation d'identité (des situations où vos données personnelles sont utilisées par quelqu'un se faisant passer pour vous pour obtenir un bénéfice financier).

## Quand vous utilisez la messagerie électronique

### Pour éviter les mails non sollicités

Une bonne idée serait d'avoir deux adresses électroniques : l'une réservée à la correspondance avec les personnes que vous connaissez, l'autre à utiliser quand il vous est demandé de donner votre adresse électronique pour accéder à un service sur Internet. Cette séparation vous aidera à gérer les problèmes de spam, par exemple, et votre boîte de réception personnelle ne sera pas bourrée de messages commerciaux non sollicités.

N'ouvrez pas les courriers ni les pièces jointes provenant d'expéditeurs inconnus ou dont l'objet est suspect ou bizarre.

## Quand vous utilisez des applications de messagerie instantanée

Ne cliquez sur aucun lien reçu par l'intermédiaire de l'application de messagerie instantanée à moins d'avoir confirmation que c'est bien l'un de vos contacts qui vous l'a envoyé et s'est assuré qu'il ne présentait pas de danger.

Les messages contenant des liens peuvent en fait être générés automatiquement par un programme malveillant, qui se sert de votre liste de contacts pour vous inciter à cliquer et attraper une infection. C'est la raison pour laquelle demander simplement à la personne si c'est bien elle qui a envoyé le message vous évitera d'être contaminé.

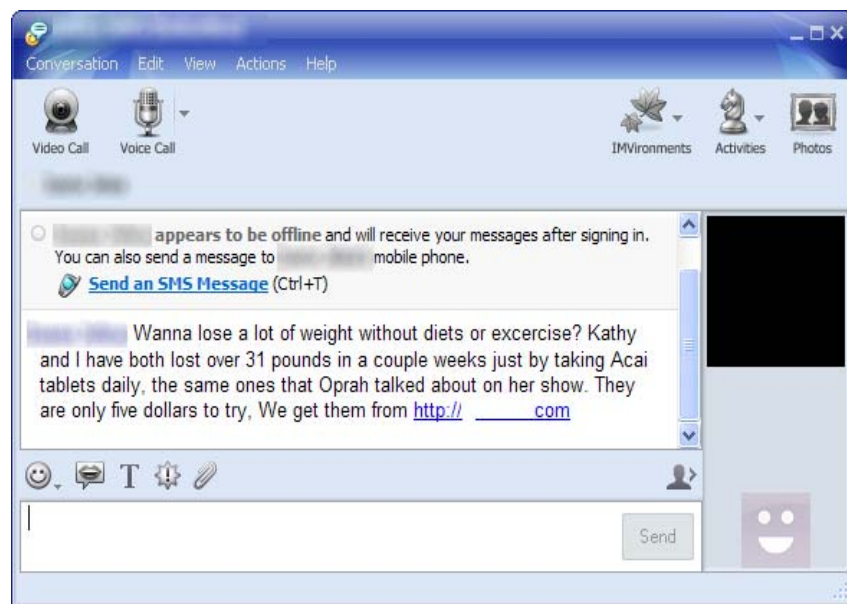


Fig. 15 - Message contenant un lien apparemment envoyé par un correspondant de l'utilisateur, mais qui a été en fait généré automatiquement

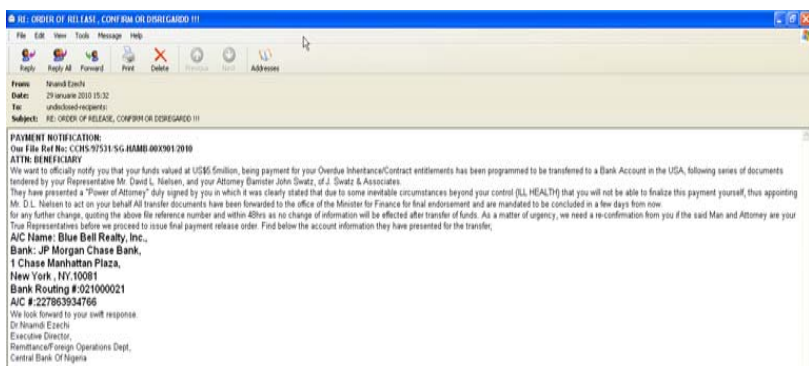


Fig. 16 - Exemple d'un e-mail dans lequel le destinataire est informé qu'il est bénéficiaire de 5,5 milliards d'euros, qu'il perdra s'il n'accuse pas réception

De la même manière, assurez-vous que les fichiers que vous recevez par l'intermédiaire de votre application de discussions en ligne sont sains et analysez-les avant de les ouvrir.

## Quand vous effectuez des paiements en ligne

Réfléchissez bien avant de répondre à toute offre d'investissement qui paraît excessivement avantageuse et qui implique que vous agissiez « immédiatement, avant qu'il ne soit trop tard ». De même, ne répondez pas aux offres / enquêtes / demandes de renseignements dont vous ne comprenez pas le sens.

Avant d'effectuer un paiement en ligne, vous devez vous assurer que la page sur laquelle vous vous trouvez est sécurisée. Comment savoir si la page est sécurisée ? Les pages web sécurisées utilisent un système de cryptage appelé *Secure Sockets Layer (SSL)* qui fait que vos données sensibles sont rendues inutilisables par quiconque chercherait à s'en emparer pendant leur transport entre votre ordinateur et le serveur de la banque.

Il existe deux indicateurs qui signifient qu'une page web est sécurisée : son adresse débute par *https://*, la lettre "s" signifiant sécurisé, et le navigateur Internet contient une icône représentant un cadenas.

Lorsqu'on clique sur l'icône, des informations s'affichent sur le niveau de sécurité du site.

Étant donné que cette vérification de sécurité requiert un certain niveau de connaissances techniques, si vous avez le moindre doute à ce sujet, n'hésitez pas à consulter un spécialiste (votre conseiller financier par exemple) avant d'effectuer le moindre paiement.

Évitez d'utiliser un ordinateur non sécurisé ou un ordinateur public connecté à Internet (comme dans un café ou une bibliothèque). Assurez-vous que vous connaissez le propriétaire du point d'accès et avez confiance en lui ; abstenez-vous également d'utiliser des connexions publiques sans fil (comme celles des aéroports ou des hôtels) pour envoyer des données par Internet.



Fig. 17 - Indicateurs d'une page web sécurisée



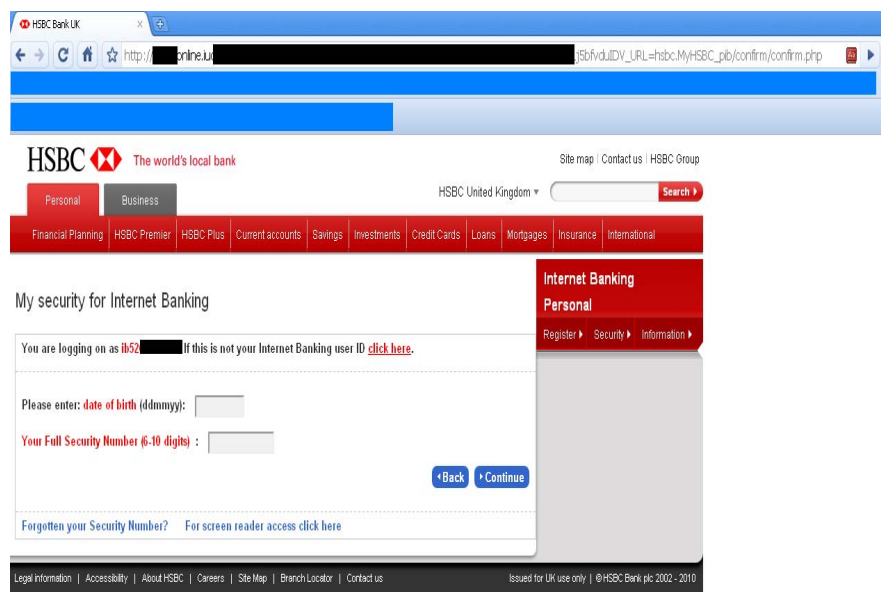


Fig. 18 - Page web bancaire falsifiée destinée à persuader l'utilisateur d'entrer son numéro de sécurité sociale sous prétexte qu'il s'agit d'une procédure de sécurité

Ne parlez de vos finances qu'avec des membres de votre famille, des amis en qui vous avez confiance ou des employés de votre banque personnelle.

Faites vos demandes de devis et de factures exclusivement par écrit et n'effectuez aucun paiement anticipé en ligne pour des marchandises ou des services.

Ne donnez votre code PIN à personne, en aucune circonstance. Au cours d'attaques de hameçonnage, les cybercriminels créent de fausses pages web d'organismes de confiance qui proposent des services de paiement en ligne ou qui réclament la création d'un compte, de manière à recueillir des données personnelles de la victime, parmi lesquelles des codes PIN qui ne doivent jamais être communiqués.

## N'ayez pas peur de porter plainte

Dénoncer des manœuvres frauduleuses ou malveillantes peut permettre de limiter la propagation du phénomène et à aider ceux qui en sont victimes à récupérer ce qu'ils ont perdu ou à limiter les dégâts.

Si vous pensez avoir été piégé en versant de l'argent en ligne à des escrocs, il est important de le signaler immédiatement à votre banque ou au fournisseur de votre carte de paiement pour bloquer votre compte ou votre carte. Vous pouvez aussi demander de l'aide au poste de police le plus proche et prendre contact avec l'organisme de protection des consommateurs pour vous renseigner sur les manières de faire face aux escroqueries sur Internet.

## Choisir une solution de sécurité des données



Fig. 19 - Assistant de configuration


Une solution fiable de sécurité des données vous aidera à éviter les traquenards en ligne. Les principales questions à se poser au moment de la choisir sont les suivantes : quel est le niveau d'efficacité de la solution pour identifier et bloquer les menaces électroniques, et à quel point sera-t-il facile pour vous de l'utiliser.

En ce qui concerne l'efficacité, opter pour une solution antimalware parmi d'autres dépend d'un ensemble d'éléments, comme sa rapidité de réaction aux menaces nouvelles, le niveau de son taux de détection, sa capacité à agir proactivement (c'est-à-dire à identifier et bloquer les menaces avant qu'elles aient une « signature » officielle), etc. BitDefender offre une gamme complète de solutions antivirus adaptées à diverses conditions d'utilisation.

Quant à la facilité d'utilisation, c'est essentiellement à vous de décider ce qui vous convient le mieux. Les indications pratiques qui suivent sont toutefois à prendre en considération.


### Existe-t-il un problème de langue ?

Assurez-vous que la solution de sécurité des données est disponible dans votre langue de manière à ne pas vous retrouver désemparé devant l'affichage de messages incompréhensibles. Les solutions BitDefender, par exemple, sont disponibles en 18 langues. Pour plus d'informations sur la version qui vous concerne, n'hésitez pas à consulter [le site web BitDefender](#).




**STOPPEZ LES VIRUS & SPYWARES**

La protection proactive BitDefender vous défend contre les nouveaux virus et les menaces encore inconnues. L'outil QuickScan détecte des activités malicieuses en utilisant des technologies "in-the-cloud", en généralement moins de une minute, et utilise juste une fraction des ressources du PC.



**PROTEGEZ VOTRE VIE PRIVEE**

Empêchez la fuite de vos données personnelles et protégez vos échanges par e-mails, par messageries instantanées, sur Facebook ou d'autres sites traçant vos activités en ligne.



**PROTEGEZ VOS RECHERCHES SUR LE WEB**

BitDefender vous alerte à propos de sites potentiellement à risques et fournit une notation de sécurité pour tous les sites lors de l'affichage de vos résultats de recherche.

Fig. 20 Les dépliants de BitDefender vous aident à choisir en toute connaissance de cause

## La solution répond-elle à tous mes besoins ?

Examinez la liste des possibilités offertes par la solution pour protéger vos propres activités en ligne et regardez les alertes qu'elle émet dans les situations dangereuses (si elle en émet).

L'exemple ci-dessous présente l'écran BitDefender d'un avertissement anti-hameçonnage. Ceci veut dire qu'au moment où vous êtes sur le point d'accéder à une page web identifiée comme ayant été conçue pour voler des données personnelles, vous serez prévenu du risque que vous prenez.



### BitDefender Total Security 2011

Cette page web a été considérée comme un site web de phishing qui essaiera de vous voler des informations confidentielles et a été bloquée par BitD

Si vous pensez que la page est sûre, veuillez cliquer [ici](#) pour l'ajouter à la liste blanche afin que BitDefender ne vous alerte plus.

Si vous voulez voir la page Internet seulement cette fois, cliquez [ici](#).

ATTENTION : consulter ou entrer des informations personnelles sur cette page n'est peut-être pas sûr.

Fig. 21 - Alerte antihameçonnage de BitDefender



Fig. 22 - Vous pouvez sélectionner le degré de complexité du processus d'installation/configuration.

## A quel degré devrai-je m'impliquer ?

Si vous choisissez une des solutions BitDefender, ce sera à vous de décider à quel point vous souhaitez être impliqué dans la manière dont la solution fonctionne.

Comme l'illustre l'exemple présenté à gauche, vous pouvez décider quels éléments du produit vous souhaitez personnaliser en lançant l'assistant de configuration initial. D'un seul clic, vous pouvez opter pour une installation facile ou personnalisée.

Vous pouvez également décider du nombre d'informations que vous souhaitez avoir sur l'activité antivirus sur votre ordinateur. En choisissant l'un des trois modes disponibles – Standard, Intermédiaire, Expert – vous pouvez interagir avec la solution autant que vous voulez, ou même simplement la laisser tourner à l'arrière plan pour ne vous consacrer qu'à ce que vous êtes en train de faire sur votre ordinateur.



Fig. 23 - En mode standard BitDefender prend seul la plupart des décisions concernant la sécurité de votre PC

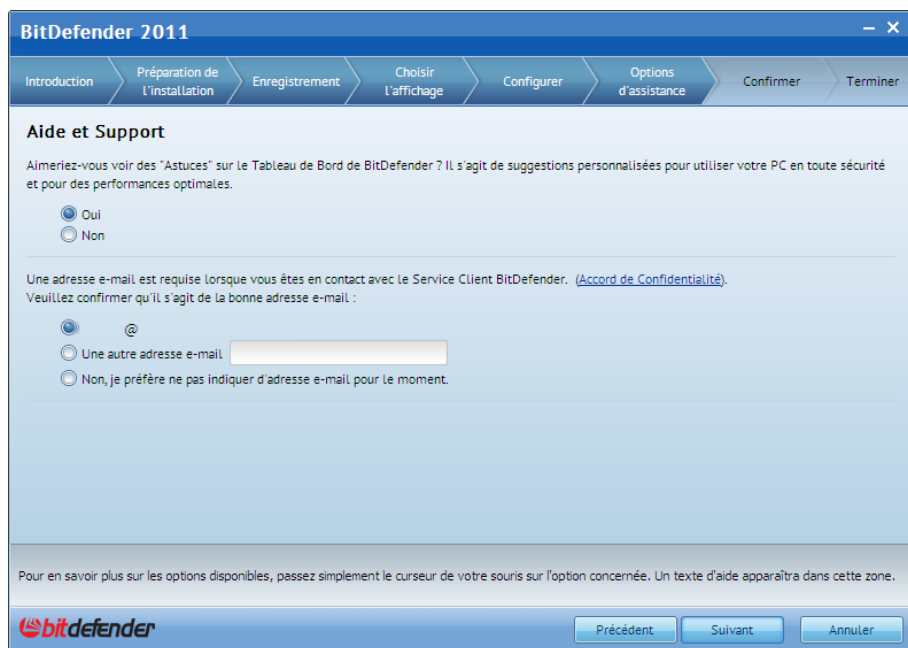


Fig. 24 - Deux clics dans l'assistant d'installation initial suffisent pour obtenir l'aide dont vous avez besoin.

## Puis-je obtenir de l'aide ?

Il est important de savoir où trouver des réponses au moment où on se pose des questions. Le manuel de l'utilisateur de la solution est tout indiqué, à condition que ses instructions soient claires et pertinentes

Par exemple, si vous recherchez plus d'informations sur la façon dont les solutions BitDefender gèrent le problème du spam, le manuel contient une rubrique sur ce sujet dans laquelle vous pourrez apprendre : que les messages spam portent la mention [spam] dans la ligne d'objet du courrier ; quels sont les clients de messageries compatibles avec les solutions ; où trouver les courriers spam identifiés comme tels en fonction du client de messagerie, etc.

En outre, l'assistance est facilement accessible lorsque vous en avez besoin. Toutes les solutions BitDefender fournissent des Astuces : des explications claires et personnalisées sur la façon d'utiliser votre ordinateur en toute sécurité et dans des conditions de performance optimales. Mieux : en confirmant votre adresse électronique, vous pouvez avoir la certitude que vos demandes d'assistance par e-mail parviendront à l'équipe Clients et qu'elle y répondra rapidement.

Les informations et données contenues dans ce document sont la représentation de l'opinion de BitDefender® sur les sujets traités le jour de la publication. Ce document et les informations qui y sont contenues ne doivent pas être interprétés comme un engagement ou un accord de la part de BitDefender.

Même si toutes les précautions ont été prises lors de la rédaction de ce document, l'éditeur, les auteurs et les contributeurs ne pourront être tenu responsables en cas d'erreurs et/ou omissions. Aucune responsabilité ne peut non plus être engagée pour des dommages résultant de l'utilisation d'informations contenues dans ce document. De plus, les informations contenues dans ce document peuvent faire l'objet de corrections, sans annonce préalable. BitDefender, l'éditeur, les auteurs, et les contributeurs ne peuvent garantir la mise à disposition de nouveaux documents ou d'informations supplémentaires en rapport avec ce document-ci.

Ce document et les données contenues dans celui-ci n'ont qu'un but informatif. Si une assistance professionnelle est nécessaire, une personne compétente dans ce domaine devra être contactée. Ni BitDefender, l'éditeur, les auteurs ou les contributeurs ne peuvent être tenus responsables de dommages en résultant.

Le fait qu'un individu ou une organisation, un travail individuel ou collectif (incluant les documents imprimés, les documents électroniques, sites web, etc.) soient cités et/ou soient source d'informations n'implique pas que BitDefender, l'éditeur, les auteurs ou les contributeurs soient responsables des informations ou recommandations que ceux-ci pourraient fournir. Les lecteurs doivent prendre en compte que BitDefender, l'éditeur du document, les auteurs ou les contributeurs ne peuvent garantir la justesse de toute information après la date de publication, comme les adresses web et liens Internet listés dans le document, et qui pourraient avoir changé ou disparu entre le moment où ce document a été rédigé et publié, et le moment où il est lu.

Les lecteurs doivent se conformer aux lois internationales régissant la propriété intellectuelle, concernant toute partie de ce document. Aucune partie de ce document ne peut être reproduite, stockée, ou transmise sous quelque forme ou par quelque moyen que ce soit (électronique, mécanique, photocopie, enregistrement, etc.) ou pour toute autre raison, sans la permission écrite de BitDefender.

BitDefender peut avoir breveté des applications, marques, droits d'auteur, ou toute autre propriété intellectuelle couvrant des sujets traités dans ce document. Sauf stipulation expresse dans un contrat de licence écrit de la part de BitDefender, ce document ne donne aucun droit sur les brevets, marques, droits d'auteur ou autre propriété intellectuelle.

Copyright © 2010 BitDefender. Tous droits réservés.

Tous les autres produits et noms d'organisations cités dans ce document le sont à simple but d'identification et sont la propriété et/ou marques de leurs propriétaires respectifs.