



**PREMIER MINISTRE**  
SECRETARIAT GÉNÉRAL DE LA DÉFENSE NATIONALE

**DOSSIER DE PRESSE**

**PORTAIL D'INFORMATION « TOUT PUBLIC »  
SUR LA SÉCURITÉ INFORMATIQUE**



*Développer la sensibilisation et la formation  
de tous les utilisateurs à la sécurité informatique*

Contact presse : 01 71 75 84 04 - [communication.dcssi@sgdn.gouv.fr](mailto:communication.dcssi@sgdn.gouv.fr)

# PORTAIL D'INFORMATION « TOUT PUBLIC » SUR LA SÉCURITÉ INFORMATIQUE

## SOMMAIRE

|                                      |         |
|--------------------------------------|---------|
| Présentation                         | page 3  |
| Conception du portail                | page 4  |
| Coordonnées du site                  | page 4  |
| Partenariat                          | page 4  |
| Présentation des partenaires         | page 5  |
| Qui sommes-nous ?                    | page 7  |
| Organisation du portail              | page 8  |
| Contenu du portail                   | page 9  |
| - Les dix commandements              | page 9  |
| - Fiches techniques                  | page 10 |
| - Guides de configuration            | page 11 |
| - Surveillance de l'actualité        | page 11 |
| - Glossaire                          | page 11 |
| - Mémentos thématiques               | page 11 |
| - Questions-réponses                 | page 11 |
| - Liens vers des ressources externes | page 11 |
| - Modules d'autoformation            | page 12 |
| - Logiciel de premier diagnostic     | page 12 |



# PORTAIL D'INFORMATION « TOUT PUBLIC » SUR LA SÉCURITÉ INFORMATIQUE

## PRÉSENTATION

Le Comité interministériel pour la société de l'information (CISI) du 11 juillet 2006, initiant une politique active de soutien à l'usage de l'internet, a décidé que l'État mettrait en place de nouvelles ressources pour contribuer à la sécurité des usagers de l'internet.

Les citoyens et les entreprises sont en effet de plus en plus utilisateurs d'internet comme moyen d'accès à des services en ligne. L'accès à ces services n'est pas exempt de risques : vols de données personnelles, compromission de l'ordinateur qui pourrait ensuite conduire à des attaques à l'insu de son utilisateur légitime, etc.

Ces risques sont particulièrement avérés lorsque les ordinateurs personnels utilisés par le grand public ou par les entreprises sont peu ou mal sécurisés et que les utilisateurs sont peu ou pas sensibilisés. Il est donc essentiel d'informer sur les enjeux de sécurité des systèmes d'information et de fournir les moyens de développer les bons réflexes en la matière.

Il est parallèlement nécessaire de rendre accessibles des informations sur l'actualité de la sécurité informatique, et en particulier de diffuser sous une forme adaptée aux entreprises (particulièrement celles qui ne disposent pas d'un service informatique important) des informations de veille, d'alerte et de réponse.

Il a ainsi été décidé la création d'un **portail de la sécurité informatique**. De nombreux acteurs publics et privés (y compris associatifs) ont contribué à sa réalisation, chacun en fonction de ses compétences. Il a été développé et sera maintenu par la Direction centrale de la sécurité des systèmes d'information (DCSSI).

A travers ce **portail de la sécurité informatique**, la DCSSI et ses partenaires proposent aux particuliers et aux entreprises un contenu pédagogique, exhaustif, technique mais accessible. Il comporte notamment des guides de configuration, des questions/réponses pratiques, des modules d'auto-formation, des fiches d'information, une surveillance de l'actualité et un glossaire. Y figurent aussi des informations sur la menace et des liens vers les sites de ses partenaires. Site de référence, il vise à fédérer au profit du plus grand nombre une information technique de qualité.



## **PORTAIL D'INFORMATION « TOUT PUBLIC » SUR LA SÉCURITÉ INFORMATIQUE**

### **CONCEPTION DU PORTAIL**

Pour atteindre les objectifs fixés par le Comité interministériel de la société de l'information (CISI), nous avons conçu ce portail en ayant constamment à l'esprit les principes suivants :

- le langage utilisé devra être simple et accessible ;
- l'information devra être perçue comme fiable et rationnelle pour un usage au quotidien ;
- l'information ne devra pas impliquer de compétence technique *a priori* ;
- les contenus devront être adaptés à une lecture orientée « particuliers » ou « entreprises » ;
- les utilisateurs devront pouvoir réagir en cas de crise ou d'incident de sécurité ;
- les contenus devront provenir d'une pluralité d'acteurs de la sécurité informatique et de l'internet.

Le portail est dès aujourd'hui accessible via le nom de domaine suivant :

<http://www.securite-informatique.gouv.fr>

La Direction centrale de la sécurité des systèmes d'information (DCSSI) est tout à la fois le directeur éditorial, l'hébergeur et le maître d'œuvre du site.

### **PARTENARIAT**











Cette première version du portail est le fruit d'une concertation et d'une large coopération avec des acteurs de la sécurité informatique en France. Ces partenaires sont représentatifs des organisations qui ont lancé des initiatives ou contribué à améliorer l'usage de l'internet, de la protection de l'enfance au traitement d'incidents.



**PORTAIL D'INFORMATION « TOUT PUBLIC »  
SUR LA SÉCURITÉ INFORMATIQUE**

|   |   |
|---|---|
|    | <b>Action Innocence</b> - préserver la dignité et l'intégrité des enfants sur internet.<br><a href="http://www.actioninnocence.org">http://www.actioninnocence.org</a>                              |
|    | <b>AFA</b> - Élaborer une déontologie pour les fournisseurs d'accès à l'internet.<br><a href="http://www.afa-France.com/">http://www.afa-France.com/</a>  |
|    | <b>APRIL</b> - Démocratiser et diffuser du logiciel libre.<br><a href="http://www.april.org">http://www.april.org</a>   |
|    | <b>CASES</b> - Portail luxembourgeois de la sécurité de l'information.<br><a href="http://www.cases.public.lu">http://www.cases.public.lu</a>   |
|   | <b>CERT-IST</b> - Assurer des services de prévention des risques et d'assistance au traitement d'incidents.<br><a href="http://www.cert-ist.com">http://www.cert-ist.com</a>                        |
|  | <b>CERT-RENATER</b> - Pour assister ses adhérents dans le domaine de la sécurité informatique.<br><a href="http://www.renater.fr/spip.php?rubrique19">http://www.renater.fr/spip.php?rubrique19</a> |
|  | <b>CLUSIF</b> - Observatoire des pratiques et des risques liés à la sécurité de l'information.<br><a href="http://www.clusif.asso.fr">http://www.clusif.asso.fr</a>                                 |
|  | <b>CNIL</b> - protéger la vie privée et les libertés individuelles ou publiques.<br><a href="http://www.cnil.fr">http://www.cnil.fr</a>   |
|  | <b>Délégation aux usages de l'internet</b> - Pour rendre l'internet plus sûr et plus accessible à tous.<br><a href="http://www.internetsanscrainte.fr">http://www.internetsanscrainte.fr</a>        |

**PORTAIL D'INFORMATION « TOUT PUBLIC »  
SUR LA SÉCURITÉ INFORMATIQUE**

|   |  |
|---|--|
|    | <b>E-enfance</b> - Le net qui laisse toutes ses chances à l'enfance.<br><a href="http://www.e-enfance.org">http://www.e-enfance.org</a>  |
|    | <b>Forum des droits sur l'internet</b> - Pôle de référence en matière de règles et d'usages de l'internet.<br><a href="http://www.foruminternet.org">http://www.foruminternet.org</a>          |
|    | <b>GITSIS</b> - Groupement Interprofessionnel (sécurité des informations sensibles).<br><a href="http://www.gitsis.asso.fr">http://www.gitsis.asso.fr</a>                                      |
|    | <b>Groupement des Cartes Bancaires</b> - Les bons conseils pour utiliser sa carte bancaire en toute sécurité.<br><a href="http://www.cartes-bancaires.com">http://www.cartes-bancaires.com</a> |
|   | <b>INL</b> propose des logiciels libres aux entreprises et administrations.<br><a href="http://www.inl.fr">http://www.inl.fr</a>   |
|  | <b>ITB</b> - Société française de conseil au service des PME et PMI.<br><a href="http://www.itb.fr">http://www.itb.fr</a>  |
|  | <b>MICROSOFT</b> - Pour la sécurité et l'accompagnement des enfants dans l'univers numérique.<br><a href="http://www.microsoft.com/fr/">http://www.microsoft.com/fr/</a>                       |
|  | <b>OCLCTIC</b> - Animer et coordonner la lutte contre la cybercriminalité.<br><a href="http://www.interieur.gouv.fr">http://www.interieur.gouv.fr</a>  |
|  | <b>SIGNAL SPAM</b> - Fédérer les efforts de tous afin de lutter contre le pourriel.<br><a href="http://www.signal-spam.fr">http://www.signal-spam.fr</a>                                       |
|  | <b>UTC</b> - Université de Technologie de Compiègne.<br><a href="http://www.utc.fr">http://www.utc.fr</a>  |

## **PORTAIL D'INFORMATION « TOUT PUBLIC » SUR LA SÉCURITÉ INFORMATIQUE**

### **QUI SOMMES-NOUS ?**

Au sein du Secrétariat général de la défense nationale (SGDN), la Direction centrale de la sécurité des systèmes d'information (DCSSI) est en charge de la stratégie gouvernementale en matière de sécurité des systèmes d'information. A ce titre, ses missions sont articulées autour de sept grandes fonctions :

- contribution à la définition interministérielle et à la mise en œuvre de la stratégie gouvernementale en matière de sécurité des systèmes d'information ;
- veille, alerte et réaction aux attaques visant les systèmes d'information de l'État. La DCSSI met en œuvre le Centre opérationnel de la sécurité des systèmes d'information (COSSI) 24 heures sur 24, 7 jours sur 7. Ce centre dispose à la fois d'une capacité de gestion de crise et d'une capacité d'expertise technique de haut niveau sur les attaques informatiques ;
- régulation : délivrance des autorisations, agréments et certificats obligatoires ou facultatifs (labels de confiance des produits de sécurité et des prestataires de service ; exportation des produits de cryptologie, etc.). Un accent tout particulier est mis sur la promotion de produits de confiance, à travers le schéma français d'évaluation et de certification ;
- inspection des systèmes d'information relevant des départements ministériels ;
- conseil, sous la forme de prestations de service, au profit principalement de la sphère publique ;
- centre de référence et d'expertise scientifique et technique, dans l'ensemble des disciplines qui concourent à la sécurité des systèmes d'information ;
- sensibilisation et formation des agents de l'État à la sécurité des systèmes d'information, assurée principalement par le Centre de formation à la sécurité des systèmes d'information (CFSSI).



# PORTAIL D'INFORMATION « TOUT PUBLIC » SUR LA SÉCURITÉ INFORMATIQUE

## ORGANISATION DU PORTAIL

Le portail est organisé autour de quatre grandes parties :

- au centre de la page, sont diffusés les alertes et les faits marquants, régulièrement actualisés ;
- à gauche, un bandeau permanent permet à l'utilisateur d'accéder aux informations en fonction de ses besoins (je suis un particulier, je cherche un guide de configuration, etc.) ;
- à droite, sont référencés les partenaires qui ont contribué au portail ;
- un bandeau horizontal permet l'accès au glossaire, au moteur de recherche et aux 10 commandements de la sécurité informatique.

PORTAILS DE L'ADMINISTRATION • Gouvernement • Service public • Légifrance • Administration 24h/24

RSS CONTACT AIDE

REPUBLIC FRANÇAISE  
PREMIER MINISTRE  
S · G · D · N  
Accueil

Présentation | Dernières modifications | Glossaire | Les dix commandements | Recherche | Surfez intelligent

### Les services du Premier ministre se mobilisent pour l'amélioration de la sécurité sur Internet

Deux services du Premier ministre, le Secrétariat général de la défense nationale (SGDN) et la Direction du développement des médias (DDM), lancent ensemble trois opérations visant à améliorer la sécurité des usagers de l'Internet. Francis Delion, secrétaire général de la défense nationale (SGDN) et Laurence Franceschini, directeur du développement des médias (DDM), s'associent dans une campagne de communication coordonnée afin de lancer respectivement le Portail de la sécurité des systèmes d'information « SSI tout public » et le site « Surfez intelligent : les indispensables » dédié à l'authentification sur Internet. La DDM signera à cette occasion avec ses partenaires une Charte pour la promotion de l'authentification sur Internet.

#### Alerte

##### 18/12/2007 Des cartes de vœux malveillantes

Plusieurs sites signalent un envoi massif de courriels, ne contenant aucun contenu, et ayant pour objet "Happy new year !". Un fichier malveillant est joint au message : postcard.exe. Certains anti-virus détectent déjà ce code malveillant, mais des variantes risquent d'apparaître, voire de nouveaux virus exploitant le même filon. L'envoi de carte postale électronique, et notamment de vœux, est en effet un vecteur de propagation de virus, chevaux de Troie ou autres contenus malveillants. Cette pratique est connue depuis longtemps. Il est donc nécessaire, à l'approche de la nouvelle année, de renforcer la vigilance et de sensibiliser les utilisateurs. La note du CERTA rappelle quelques précautions à prendre lors de la réception de tels messages. [26/12/2007 12:36]

#### Faits marquants

#### PARTENAIRES

- DCSSI**  
Site thématique de la sécurité des systèmes d'information.
- Vitez - Lou sur internet**  
Délégation aux usages de l'Internet  
Pour rendre l'Internet plus sûr et plus accessible à tous
- OCLCTIC**  
Animer et coordonner la lutte contre la cybercriminalité.
- CNIL**  
Protéger la vie privée et les libertés individuelles ou publiques.
- CASES**  
Portail luxembourgeois de la sécurité de l'information
- Microsoft**  
Pour la sécurité et l'accompagnement des enfants dans l'univers numérique.



# PORTAIL D'INFORMATION « TOUT PUBLIC » SUR LA SÉCURITÉ INFORMATIQUE

## CONTENU DU PORTAIL

- **Les Dix Commandements** de la Sécurité informatique : cette page énumère les dix principes les plus importants en matière de sécurité informatique et renvoie vers des fiches techniques ou des guides de configuration.

PORTAILS DE L'ADMINISTRATION • Gouvernement • Service public • Légifrance • Administration 24h/24

RSS CONTACT AIDE

Liberté • Égalité • Fraternité  
RÉPUBLIQUE FRANÇAISE

PREMIER MINISTRE  
S · G · D · N  
Accueil

Présentation | Dernières modifications | Glossaire | Les dix commandements | Recherche | Surfez intelligent

### Les 10 commandements de la sécurité sur l'Internet

- Utiliser des mots de passe de qualité.** Le dictionnaire définit un mot de passe "comme une formule convenue destinée à se faire reconnaître comme ami, à se faire ouvrir un passage gardé". Le mot de passe informatique permet d'accéder à l'ordinateur et aux données qu'il contient. Il est donc essentiel de savoir choisir des mots de passe de qualité, c'est-à-dire difficiles à retrouver à l'aide d'outils automatisés, et difficiles à deviner par une tierce personne.  
▶ Voir la fiche **Choisir un bon mot de passe**
- Avoir un système d'exploitation et des logiciels à jour :** navigateur, anti-virus, bureautique, firewall personnel, etc.  
La plupart des attaques tentent d'utiliser les failles d'un ordinateur (failles du système d'exploitation ou des applications). En général, les agresseurs recherchent les ordinateurs dont les logiciels n'ont pas été mis à jour afin d'utiliser la faille non corrigée et ainsi parviennent à s'y introduire. C'est pourquoi il est fondamental de mettre à jour tous ses logiciels afin de corriger ces failles.  
▶ Voir la fiche **Mises à jour de sécurité (patches)**
- Effectuer des sauvegardes régulières**  
Le premier principe de défense est de conserver une copie de ses données afin de pouvoir réagir à une attaque ou un dysfonctionnement. La sauvegarde de vos données est une condition de la continuité de votre activité.  
▶ Voir la fiche **Sauvegarde**
- Désactiver par défaut les ActiveX et les JavaScript**  
Les composants ActiveX ou les JavaScripts permettent certaines fonctionnalités web intéressantes mais ils présentent de nombreux risques de sécurité pouvant aller jusqu'à la prise de contrôle par un intrus d'une machine vulnérable. Il n'est pas question d'en interdire l'usage mais de limiter celui-ci aux sites dans lesquels l'utilisateur a confiance : il s'agit donc de désactiver leur interprétation par défaut et de choisir de ne les activer que lorsque cela est nécessaire et si on estime être sur un site de confiance.  
▶ Voir la fiche **Bien paramétrer son navigateur**
- Ne pas cliquer trop vite sur des liens**  
Une des attaques classiques visant à tromper l'internaute pour lui voler des informations personnelles, consiste à l'inciter à cliquer sur un lien placé dans un message. Ce lien peut-être trompeur et malveillant. Plutôt que de cliquer sur celui-ci, il vaut mieux saisir soi-même l'adresse du site dans la barre d'adresse du navigateur. De nombreux problèmes seront ainsi évités.  
▶ Pour aller plus loin **Filoutage (phishing) ; Bonnes pratiques de navigation**
- Ne jamais utiliser un compte administrateur pour naviguer**



## PORTAIL D'INFORMATION « TOUT PUBLIC » SUR LA SÉCURITÉ INFORMATIQUE

- Des **fiches techniques**, portant sur tous les sujets d'intérêts pour les utilisateurs, de l'Anti-espionnage au Wifi, sont disponibles. Elles seront complétées et mises à jour périodiquement.

PORTAILS DE L'ADMINISTRATION • Gouvernement • Service public • Légifrance • Administration 24h/24

[RSS](#)   [CONTACT](#)   [AIDE](#)

PREMIER MINISTRE  
**S · G · D · N**  
Accueil

# Portail de la Sécurité informatique

[Présentation](#) | [Dernières modifications](#) | [Glossaire](#) | [Les dix commandements](#) | [Recherche](#) | [Surfez intelligent](#)

### Fiches techniques

#### Mises à jour de sécurité

|                            |   |
|----------------------------|---|
| Qui est concerné ?         | Particuliers  |
| Combien de temps faut-il ? | 5 minutes   |
| Quel gain ?                | Comprendre ce que sont les mises à jour de sécurité et la nécessité de les déployer régulièrement |

**Qu'est-ce que c'est ?**

Les logiciels, comme toute création humaine, comportent des défauts appelés bogues. Parmi ces défauts, on trouve des défauts portant atteinte à la sécurité. C'est ce que l'on appelle des vulnérabilités. Ainsi, les éditeurs de logiciels, à l'instar des constructeurs automobiles ayant découvert un défaut sur un de leurs modèles effectuent des campagnes de correction des problèmes. La différence, c'est qu'il n'est pas nécessaire de rapporter votre logiciel au service après vente ; il suffit de télécharger une rustine logicielle pour réparer le défaut de sécurité. Cette rustine est ce que l'on appelle une mise à jour de sécurité. On dit aussi correctif de sécurité ou patch de sécurité.

**Et si je ne m'en soucie pas ?**

Si une vulnérabilité a été découverte sur un des logiciels que vous utilisez, une personne malintentionnée pourrait essayer d'en tirer profit pour essayer de prendre le contrôle de votre ordinateur, voler des informations, provoquer le dysfonctionnement ou l'arrêt de votre machine, propager un ver, installer du contenu illicite, etc.

Il est donc primordial de toujours maintenir à jour vos logiciels et d'appliquer systématiquement toutes les mises à jour de sécurité au fur et à mesure qu'elles sont publiées afin de

▶ **Je suis...**  
Particulier  
Entreprise

▶ **Je cherche...**  
Autoformation  
Fiche technique  
Guide de configuration  
Mémento  
Question / Réponse  
Une solution pour me protéger  
Lien

▶ **Actualités**  
Alerte  
Faits marquants

## PORTAIL D'INFORMATION « TOUT PUBLIC » SUR LA SÉCURITÉ INFORMATIQUE

- Des **guides de configuration** explicitent les moyens de mettre en application les recommandations préconisées dans les fiches techniques et les mémentos.

PORTAILS DE L'ADMINISTRATION • Gouvernement • Service public • Légifrance • Administration 24h/24

RSS CONTACT AIDE

Portail de la  
**Sécurité informatique**

Présentation | Dernières modifications | Glossaire | Les dix commandements | Recherche | Surfez intelligent

### Guides de configuration

#### Mise à jour sous Mac OS X

|                            |                                |
|----------------------------|--------------------------------|
| Qui est concerné ?         | Particuliers, entreprises      |
| Combien de temps faut-il ? | 5 minutes                      |
| Quel gain ?                | Garder ses applications à jour |

Manuellement La fonctionnalité de mise à jour intégrée à Mac OS X permet de mettre à jour simplement tous les logiciels Apple. Elle ne permet pas de mettre à jour les autres logiciels que vous avez installés.

Pour vérifier la présence de nouvelles mises à jour, cliquez sur le menu « pomme » en haut à gauche de l'écran et cliquez sur « Mise à jour de logiciels... ».

On trouve aussi :

- une surveillance de l'**actualité**, présentée sous la forme d'alertes et de faits marquants, relevés par les services de la DCSSI ;
- un **glossaire**, qui porte sur tous les mots et expressions dont la compréhension est nécessaire pour comprendre la sécurité informatique, d'Accaparement de nom de domaine à **Zombie** ;
- des **mémentos** thématiques rassemblant des informations ciblées ;
- des **questions-réponses** organisées thématiquement ;
- des **liens** vers nos partenaires et des liens externes vers des ressources supplémentaires.



## PORTAIL D'INFORMATION « TOUT PUBLIC » SUR LA SÉCURITÉ INFORMATIQUE

- Des **modules d'autoformation** permettant à tous d'apprendre par eux même. Il s'agit dans cette rubrique d'approfondir les connaissances des utilisateurs sur la sécurité informatique grâce à des modules interactifs d'autoformation. Trois modules sont actuellement disponibles (mot de passe, politique de sécurité, authentification). D'autres modules viendront les compléter afin de couvrir progressivement l'essentiel des thèmes fondamentaux de la sécurité.

PORTAILS DE L'ADMINISTRATION • Gouvernement • Service public • Légifrance • Administration 24h/24

RSS CONTACT AIDE

Liberté • Égalité • Fraternité  
REPUBLIQUE FRANÇAISE

PREMIER MINISTRE  
S • G • D • N  
Accueil

Présentation | Dernières modifications | Glossaire | Les dix commandements

### Je cherche une autoformation

Nous vous proposons d'approfondir ou de rafraîchir vos connaissances sur la sécurité informatique grâce à ces modules interactifs d'autoformation. Trois modules sont actuellement disponibles. D'autres modules viendront les compléter afin de couvrir progressivement l'essentiel des thèmes fondamentaux de la sécurité. L'enrichissement de cette offre tiendra compte des remarques que vous accepterez de nous faire au travers du questionnaire ci-dessous. Pour que nous puissions répondre à vos souhaits, nous vous remercions de bien vouloir le remplir aussi précisément que possible.

▣ **Authentification**  
La demande d'authentification sur les sites internet, ou sur des systèmes d'information, en particulier sur des sites internet, est systématique. Mais s'authentifier, qu'est ce que cela veut dire ? Sur quels principes se fonde cette notion ? Comment identifier les menaces qui pèsent sur les systèmes d'authentification distante ? Destiné avant tout aux décideurs et aux concepteurs ce **module** pourra aussi intéresser tous les utilisateurs de ces systèmes qui sont curieux de savoir quels sont les concepts sous-jacents à ce qui leur est demandé.

▣ **Mot de passe**  
Le mot de passe est l'un des moyens d'authentification les plus répandus dans les systèmes d'information mais l'utilisation de mots de passe triviaux est malheureusement beaucoup trop fréquente, et facilite considérablement les intrusions. Ce **module** aidera tous les utilisateurs à faire des choix offrant une résistance suffisante dans la plupart des cas.

▣ **Politique de sécurité des systèmes d'information - PSSI.**  
Cet ensemble de documents, de procédures, etc. a pour objectif la protection d'un système d'information. Il va structurer toute la réflexion présente et future et canaliser les actions afin de les rendre cohérentes et efficaces. Ce **module** va permettre d'en découvrir le contenu et d'apprendre à la construire et à s'en servir tout en montrant les avantages sécuritaires, organisationnels et économiques

▣ **Votre avis nous intéresse !**  
Si vous avez des remarques sur les modules d'autoformation, nous vous remercions de bien vouloir prendre quelques instants pour nous faire part de vos suggestions.

**Je suis...**  
Particulier  
Entreprise

**Je cherche...**  
Autoformation  
Fiche technique  
Guide de configuration  
Mémento  
Question / Réponse  
Une solution pour me protéger  
Lien

**Actualités**  
Alertes  
Faits marquants

- Le portail proposera prochainement un **logiciel de premier diagnostic**, développé par la DCSSI. Se basant sur un diagnostic technique de son ordinateur, il vise à rendre l'utilisateur conscient des risques liés à l'utilisation de l'informatique, et responsable de ses choix de comportement et de configuration. Ce logiciel établit un diagnostic puis oriente l'utilisateur vers des recommandations techniques et comportementales afin d'améliorer la sécurité de son ordinateur. Il est exécutable hors ligne, est libre (sous licence GPL) et multiplateformes.

