



Les télétravailleurs prétendent connaître les problèmes de sécurité, mais la plupart ont un comportement en ligne risqué

Alors qu'une étude réalisée auprès de 1 000 télétravailleurs, dans 10 pays, révèle des contradictions dans l'utilisation à distance de son ordinateur professionnel, **la France est l'un des pays les plus disciplinés.**

Près de 7 personnes sur 10 déclarent avoir les connaissances nécessaires en matière de sécurité informatique, selon une étude réalisée par le cabinet indépendant InsightExpress. Néanmoins, ils sont encore nombreux à ouvrir des courriers électroniques suspects, à utiliser leur ordinateur professionnel à des fins personnelles ou à laisser une tierce personne l'utiliser.

L'étude a été réalisée auprès de plus de 1 000 personnes faisant du télétravail régulièrement ou de façon ponctuelle, dans 10 pays (États-Unis, Royaume-Uni, France, Allemagne, Italie, Japon, Chine, Inde, Australie et Brésil). Cette enquête a notamment permis de mettre en avant la conduite de ces personnes lorsqu'elles se connectaient à distance au réseau de l'entreprise et les répercussions que cela pouvait avoir sur la sécurité des systèmes informatiques.

La France affiche un comportement plus mature

Les résultats montrent que le sentiment de confiance affiché par les utilisateurs peut néanmoins aggraver les problèmes de sécurité par des comportements dangereux pour le réseau de l'entreprise. En effet, si 66 % des personnes interrogées déclarent connaître les risques encourus lors d'une connexion à distance au réseau de l'entreprise, 1/4 admet ouvrir des emails provenant d'un émetteur inconnu. Cependant, **la France affiche un comportement plus mature** avec seulement 15 % des personnes interrogées qui ouvrent un email inconnu sur leur ordinateur professionnel, contre 1/3 des Allemands et des Anglais.

L'une des contradictions les plus flagrantes révélées par l'étude concerne l'utilisation personnelle de son ordinateur professionnel. Près de 30 % admettent utiliser leur ordinateur professionnel pour un usage personnel mais ils sont 40 % à faire leurs achats en ligne. **La France affiche une nouvelle fois l'un des taux les plus bas avec seulement 29 % qui admettent utiliser leur ordinateur professionnel pour acheter en ligne** contre 41 % en Allemagne et jusqu'à 53 % en Angleterre. Les principales raisons évoquées sont que leur ordinateur professionnel est certainement plus sécurisé que leur ordinateur personnel, que les achats en ligne sont sans risque ou encore que l'entreprise ne s'en soucie pas.

L'une des principales failles de sécurité repose donc sur le comportement des utilisateurs. Ces éléments démontrent bien la nécessité pour les entreprises d'intégrer dans la mise en œuvre de leur stratégie en matière de sécurité informatique des éléments qu'elles ne maîtrisent pas.

L'utilisation par une tierce personne

Nombreux sont ceux également qui autorisent une tierce personne (amis ou famille) à utiliser leur ordinateur professionnel pour accéder à Internet en pensant qu'il n'y a aucun mal à cela, que l'entreprise laisse faire, qu'il n'y a pas de risque encourus ou encore que les autres le font aussi. 21 % des personnes interrogées autorisent l'accès à leur ordinateur. En Chine, le pourcentage atteint 42 %. **En France, le chiffre est une nouvelle fois inférieur à la moyenne avec 15 % des personnes qui laissent l'accès à leur ordinateur.**

De manière générale, un pays comme la Chine, affiche des comportements plus risqués que ses homologues américains ou européens. Ce sont près de 6 personnes sur 10 qui ouvrent un email inconnu et 42 % d'entre elles qui autorisent une tierce

personne à utiliser leur ordinateur professionnel. Et le taux atteint 66 % lorsqu'il s'agit de télécharger des dossiers personnels sur son ordinateur à usage professionnel.

« Le piratage de réseau sans fil ou le partage de systèmes professionnels avec des personnes étrangères à l'entreprise entraîne des risques notables pour l'informatique, au niveau mondial », déclare Jeff Platon, vice-président en charge des solutions de sécurité chez Cisco. « Si l'on se base sur les résultats concernant les États-Unis, le comportement de 11 télétravailleurs dans une entreprise de 100 personnes peut mettre le réseau en panne ou entraîner le vol d'informations professionnelles et personnelles. Une seule faille suffit. Pour les grandes entreprises, avec des dizaines de milliers d'employés, et surtout pour celles dont le personnel est réparti au niveau mondial et de cultures différentes, le risque est encore plus grave. »

Selon Jeff Platon, c'est là qu'interviennent l'équipe informatique et le directeur de la sécurité. Les problèmes posés par les travailleurs à distance sont l'occasion pour les équipes informatique et sécurité d'être plus proactives dans la protection de leur entreprise, et de transformer leur image dans l'esprit des utilisateurs, en se dégageant d'un rôle tactique et réactif.

« L'informatique doit avoir un rôle plus stratégique. Elle doit développer des relations plus solides avec les utilisateurs, pour éviter que l'efficacité et les identités ne soient mises à mal par des attaques », poursuit Jeff Platon. Pour de plus amples informations sur les résultats d'ensemble ou des points précis concernant les 10 pays, un [white paper](#) est disponible en ligne.

**Siège social Mondial**

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
Etats-Unis
www.cisco.com
Tél. : 408 526-4000
800 553 NETS (6387)
Fax : 408 526-4100

Siège social France

Cisco Systems France
11 rue Camilles Desmoulins
92782 Issy Les Moulineaux
Cédex 9
France
www.cisco.fr
Tél. : 33 1 58 04 6000
Fax : 33 1 58 04 6100

Siège social Amérique

Cisco Systems, Inc.
170 West Tasman Drive
San Jose, CA 95134-1706
Etats-Unis
www.cisco.com
Tél. : 408 526-7660
Fax : 408 527-0883

Siège social Asie Pacifique

Cisco Systems, Inc.
Capital Tower
168 Robinson Road
#22-01 to #29-01
Singapour 068912
www.cisco.com
Tél. : +65 317 7777
Fax : +65 317 7799

Cisco Systems possède plus de 200 bureaux dans les pays et les régions suivantes. Vous trouverez les adresses, les numéros de téléphone et de télécopie à l'adresse suivante :
www.cisco.com/go/offices

Afrique du Sud • Allemagne • Arabie saoudite • Argentine • Australie • Autriche • Belgique • Brésil • Bulgarie • Canada • Chili • Colombie • Corée
Costa Rica • Croatie • Danemark • Dubaï, Emirats arabes unis • Ecosse • Espagne • Etats-Unis • Finlande • France • Grèce • Hong Kong SAR
Hongrie • Inde • Indonésie • Irlande • Israël • Italie • Japon • Luxembourg • Malaisie • Mexique • Nouvelle Zélande • Norvège • Pays-Bas
Pérou • Philippines • Pologne • Portugal • Porto Rico • République tchèque • Roumanie • Royaume-Uni • République populaire de Chine
Russie • Singapour • Slovaquie • Slovénie • Suède • Suisse • Taiwan • Thaïlande • Turquie • Ukraine • Venezuela • Vietnam • Zimbabwe



Copyright©2006 Cisco Systems, Inc. Tous droits réservés. CCSP, CCVP, le logo Cisco Square Bridge, Follow Me Browsing et StackWise sont des marques de Cisco Systems, Inc. ; Changing the Way We Work, Live, Play, and Learn, et iQuick Study sont des marques de service de Cisco Systems, Inc. ; et Access Registrar, Aironet, ASIST, BPX, Catalyst, CCDA, CCDP, CCIE, CCIP, CCNA, CCNP, Cisco, le logo Cisco Certified Internetwork Expert, Cisco IOS, Cisco Press, Cisco Systems, Cisco Systems Capital, le logo Cisco Systems, Cisco Unity, Empowering the Internet Generation, Enterprise/Solver, EtherChannel, EtherFast, EtherSwitch, Fast Step, FormShare, GigaDrive, GigaStack, HomeLink, Internet Quotient, IOS, IP/TV, iQ Expertise, le logo iQ, iQ Net Readiness Scorecard, LightStream, Linksys, MeetingPlace, MGX, le logo Networkers, Networking Academy, Network Registrar, Packet, PIX, Post-Routing, Pre-Routing, ProConnect, RateMUX, ScriptShare, SlideCast, SMARTnet, StrataView Plus, TeleRouter, The Fastest Way to Increase Your Internet Quotient et TransPath sont des marques déposées de Cisco Systems, Inc. et/ou de ses filiales aux États-Unis et dans d'autres pays.

Toutes les autres marques mentionnées dans ce document ou sur le site Web appartiennent à leurs propriétaires respectifs. L'emploi du mot partenaire n'implique pas nécessairement une relation de partenariat entre Cisco et une autre société. (0502R) 205534.E_ETMG_JD_09/06