
©JupiterImages

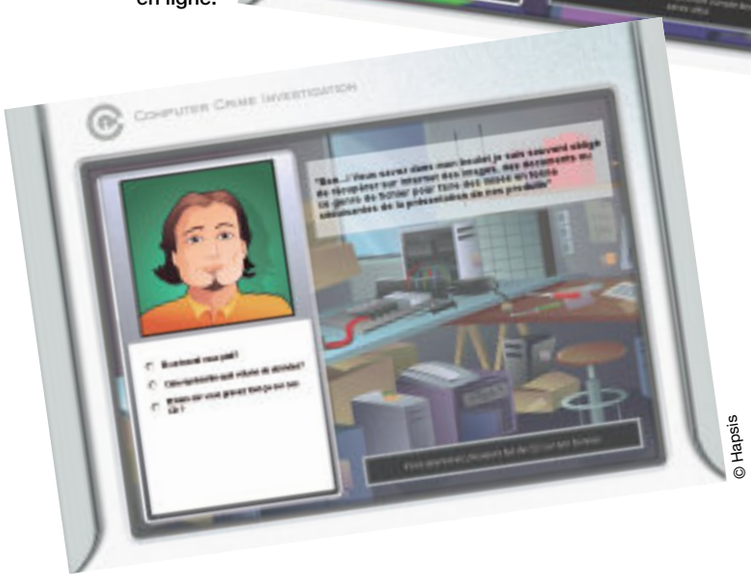
SÉCURITÉ INFORMATIQUE

À vous de jouer !

Gérer les risques informatiques est aujourd'hui vital pour toute entreprise. Et pour que la composante humaine ne devienne pas le maillon faible, le cabinet de conseil Hapsis propose une offre originale et ludique de sensibilisation des utilisateurs par le jeu.

La peste numérique n'en finit pas de gagner du terrain. Toute activité économique génère aujourd'hui des risques qui peuvent présenter des formes multiples (vols de données, espionnage industriel, etc.) et engendrer des conséquences plus ou moins importantes sur la pérennité de l'entreprise. D'après une enquête du Clusif*, pour s'en protéger, plus de 85 % des entreprises françaises envisagent désormais de mener des actions de sensibilisation de leur personnel à la sécurité informatique. Partant du principe que les formations classiques sont souvent perçues comme rébarbatives, la société Hapsis a imaginé une démarche ludique et originale à travers deux jeux pédagogiques. Créé par des professionnels de la sécurité informatique, Hapsis est un cabinet de conseil indépendant spécialisé dans le domaine de la gestion des risques et de la sécurité des systèmes d'information.

© Hapsis



© Hapsis

Computer Crime Investigation, **accessible sur l'intranet de l'entreprise, est un jeu d'enquête en ligne.**

La pédagogie par le jeu

Pour Hapsis, *« la sécurité est souvent perçue de manière négative : surveillance, contrôle et le cas échéant, répression. Dans l'entreprise, la peur du gendarme existe aussi ! De plus, l'idée du « ça n'arrive qu'aux autres » demeure dans les mentalités et les utilisateurs ne perçoivent souvent que les aspects contraignants de la sécurité sans en comprendre le bien-fondé. »*

HAPSIS
La clé de voûte de votre infrastructure sécurisée

La sensibilisation par le jeu favorise l'attention et la mobilisation des participants, mais aussi la concrétisation par le réel de concepts relativement abstraits. Offrant une image différente de la sécurité et des personnes qui en ont la charge, ces jeux suscitent également un sentiment d'implication chez les participants. L'objectif étant non seulement de sensibiliser, mais surtout d'engendrer un changement de comportement des utilisateurs vis-à-vis de la sécurité. Bref, de transformer l'utilisateur en acteur véritable de la sécurité de son entreprise.

Hapsis propose deux types de jeu : SensiRisk et CCI (pour *Computer Crime Investigation*).

SensiRisk reprend le principe du jeu de l'oie. Il peut être utilisé sur tous types de supports ou même être mis en ligne sur l'intranet de l'entreprise, et se jouer ou non sous l'égide d'un animateur. Les équipes participant au jeu se déplacent sur un parcours composé de cases de différentes couleurs. Celles-ci correspondent à plusieurs types de cartes qui vont permettre l'évocation et le traitement des différents thèmes de sensibilisation. La durée du jeu peut varier d'une à trois heures, en fonction du choix ou non de l'option rapide. Les équipes doivent tour à tour répondre aux questions, vivre au gré des incidents et adapter leurs comportements pour réduire l'impact de ces derniers. L'objectif de ce jeu n'est pas de former des experts en sécurité, mais de permettre aux participants de prendre conscience

© Hapsis

SensiRisk sensibilise l'internaute aux différents risques du réseau en se calquant sur le principe du jeu de l'oie.

© Hapsis

des enjeux et de changer leurs comportements. Huit thèmes sont abordés : de la gestion des mots de passe aux sauvegardes en passant par la menace virale, l'utilisation d'internet, celle du mail, la sécurité du poste de travail, l'ingénierie sociale et le *phishing*. Rappelons que le *phishing*, ou hameçonnage en français, consiste à collecter les éléments d'identification d'une personne en la sollicitant par e-mail. Il ne reste plus ensuite qu'à usurper son identité pour accéder à des services en ligne, principalement bancaires ou de paiement…

Quant à CCI, c'est un jeu d'enquête qui se déroule en ligne. Il est uniquement constitué de pages web et s'installe sur l'intranet de l'entreprise. L'utilisateur joue le rôle d'une personne qui assiste l'équipe sécurité d'une entreprise fictive afin d'identifier les causes d'un sinistre informatique. Le jeu se déroule en cinq parties pendant lesquelles le joueur progresse dans l'intrigue principale. Il y rencontre un certain nombre de situations intermédiaires qui sont prétexte à aborder tel ou tel thème de sensibilisation. L'objectif n'est pas de faire buter le joueur sur des énigmes difficiles, mais de l'amener, de façon simple et attractive, à mettre en évidence des situations anormales qui pourraient être vécues dans diverses entreprises. Puis de lui montrer les comportements et les règles à respecter pour éviter que ces situations ne se reproduisent.

TDF sur la case départ

C'est le jeu SensiRisk que Guillaume Rincé, responsable de la sécurité des systèmes d'information chez TDF, a choisi pour sensibiliser le personnel de l'entreprise. Et c'est une rencontre avec certains des membres de la société Hapsis, au sein d'associations traitant de la sécurité informatique, qui lui a donné l'envie d'opter pour une méthode originale de faire de la formation. « *Jusqu'alors, notre approche restait académique*, précise Guillaume Rincé, *de type présentation PowerPoint classique. Nous avons cherché un moyen un peu plus interactif et ludique pour retenir l'attention et marquer les esprits des gens qui suivent ces formations. Le but étant qu'ils appréhendent mieux le sujet et retiennent plus de choses qu'avec une formation classique. En effet, la sécurité informatique n'est pas forcément un sujet qui passionne les foules et qui donne lieu aux formations les plus attractives…* »

Quant au choix précis de ce jeu, il s'en explique : « *Notre objectif est de mettre en place des formations pour de petits groupes de personnes et de développer les interactions entre elles. L'autre jeu proposé par la société Hapsis, le CCI, est à mon sens plus adapté à une grande campagne de formation interne, dans le cas où l'on souhaite sensibiliser l'ensemble de l'entreprise. Outre l'absence d'interactivité, il n'offre pas la possibilité d'adapter son contenu. À l'inverse, le jeu SensiRisk est livré avec une base de connaissances et un ensemble de questions standard, mais offre la possibilité d'adapter tout ce qui correspond au contexte et à l'environnement de sa propre entreprise. Nous avons donc pu modifier un certain nombre de choses afin de refléter l'univers de TDF et les objectifs que nous souhaitions atteindre.* »

Le but est aujourd'hui de former près de 200 personnes sur les six derniers mois de l'année. Et s'il est encore trop tôt pour en tirer un bilan, « *le fait est*, constate Guillaume Rincé, *que les participants se prennent au jeu car ils ne se contentent pas de suivre un discours ou de visualiser passivement des informations. Ils sont partie prenante.* »

Alors, à vous de jouer ? ■

Sylvie Albou-Tabart

**Clusif : Club de la sécurité des systèmes d'informations français.*

www.hapsis.fr

Attention *phishing* !

Après le premier cas de *phishing* signalé en France en août 2004, les internautes français ont subi le 27 mai dernier la première attaque de grande ampleur par ce biais. Les détenteurs d'une adresse e-mail en « .fr » ont ainsi reçu un message rédigé en anglais et prétendument envoyé à leurs clients par quatre banques (Société Générale, BNP Parisbas, CIC Banque et CCF). L'attaque consistait à diriger les internautes vers une fausse page de site bancaire où il leur était demandé leur identifiant et leur mot de passe. L'objectif des pirates étant, bien sûr, d'utiliser ces codes d'accès pour vider le compte des victimes en procédant par virement. Les banques ciblées ont rapidement réagi en neutralisant les fausses pages et en prévenant leurs clients du caractère frauduleux de cette requête.