

Club de la Sécurité de l'Information Français

« Agir pour la sécurité de l'information »



**Social engineering :
manipulations et sécurité
par le comportement**

14 juin 2007

Le Clusif

Association sans but lucratif (création début des années 80)

> 600 membres (50% offreurs, 50% utilisateurs)

Partage de l'information

- Echanges homologues-experts, savoir-faire collectif, fonds documentaire

Valoriser son positionnement

- Retours d'expérience, visibilité créée, Annuaire des Membres Offreurs

Anticiper les tendances

- Le « réseau », faire connaître ses attentes auprès des offreurs

Promouvoir la sécurité

Adhérer...

La dynamique des groupes de travail

Des livrables en libre téléchargement (dont MEHARI)

Des traductions en anglais

Des prises de position publiques ou des réponses consultation

Des espaces d'échanges permanents : MEHARI, menaces, réseau, RSSI

Les groupes actifs en 2007

- Bases de connaissance MEHARI 2007
- Conception d'un centre Informatique sécurisé
- Criminalistique
- Destruction et Récupération d'informations
- Documentation de MEHARI™
- Fiches de sécurité pour la micro-Informatique
- Formation
- Gestion de crise
- Gestion des identités
- Infogérance
- Intégration de MEHARI™
- Métriques 7799
- Malveillance téléphonique
- Panorama de la cybercriminalité
- Réseau privé virtuel (VPN)
- Spam
- Spyware

Une ouverture vers le (grand) public

Evénements

- Conférences
 - Clusif,
 - en partenariat
- Salons (participation aux)
- Activités en région

Médias et interviews

Label Formation

Portail « cybervictime »

Label Formation CLUSIF

Agir pour la sécurité de l'information

Une aide aux entreprises

Le Label Formation CLUSIF est une **aide aux entreprises** pour mieux connaître et **sélectionner des formations** du domaine de la **sécurité** de l'information qui :

- satisfont à un standard établi par la profession réunissant à la fois offreurs et utilisateurs,
- s'engagent en matière d'éthique,
- se soumettent à un suivi régulier par la CLUSIF :
 - elles sont d'actualité, notamment en matière de caractérisation des menaces,
 - elles prennent en compte les évolutions rapides des problématiques de sécurité des SI et de l'information et les évolutions technologiques,
 - elles maintiennent l'accès approprié à un niveau de connaissance adapté,
 - utilisent une pédagogie moderne et adaptée au sujet.

Une aide aux organismes de formation

C'est également une **aide** apportée aux **organismes** de formations et aux **formateurs**. En effet, le Label Formation CLUSIF apporte, directement ou indirectement :

- une meilleure notoriété globale,
- une information sûre vers des sociétés cibles concernées,
- un accès facilité aux sociétés adhérentes au CLUSIF,
- des recommandations du Comité de Labellisation,
- une auto-évaluation compétitive.

Label Formation CLUSIF

- § 1 : Présentation
- § 2 : Attribution
- § 3 : Caractéristiques
- § 4 : Le Comité de labellisation
- § 5 : La FAQ Label Formation CLUSIF
- § 6 : **Liste des formations labellisées**
- § 7 : Vos retours d'expériences

Présenter un dossier de candidature



Des actions en régions : **CLUSIR : Club de la sécurité des systèmes d'information régionaux**

Associations régionales
décentralisées et agréées par le
CLUSIF

Elles ont pour vocation de
rassembler les différents
acteurs de la sécurité des
systèmes d'information tels
que utilisateurs, offreurs de
produits ou de services,
collectivités publiques. Elles
favorisent également les
relations avec les universités



Club de la Sécurité des Systèmes d'Information du Languedoc-Roussillon

Le Millénaire 2
417, rue Samuel Morse
34000 MONTPELLIER
Contact :  Christian FERRAND
Site web :  www.clusir.fr



Club de la Sécurité des Systèmes d'Information de la Région Midi Pyrénées

S/C INSA
Département de Génie Electrique et Informatique
135, Avenue de Ranguel
31077 TOULOUSE CEDEX 04
Contact :  Alexandra VAGNER
Site web :  www.clusir-mp.asso.fr



Club de la Sécurité des Systèmes d'Information de la Région Est

16, rue de Pont-à-Mousson
57000 METZ
Contact :  Thierry RAMARD
Site web :  www.clusir-est.com



Club de la Sécurité des Systèmes d'Information de la Région Provence-Alpes-Côte-d'Azur

60, route Enco de Botte
13012 MARSEILLE
Contact :  Marc BERGMAN



Club de la Sécurité des Systèmes d'Information de la Région Rhône-Alpes

SITIV
Passage de l'Avenir
69200 VENISSIEUX
Contact :  Yannick BOUCHET
Site web :  www.clusir-rha.fr



Club de la Sécurité des Systèmes d'Information de la Région Nord Pas de Calais Picardie

1862, avenue Général De Gaulle
59910 BONDUES
Contact :  Gérard MOLINES
Site web :  <http://www.clusif.fr/clusir-npp/>

Des homologues en Europe et dans le monde: **CLUSI : Club de la Sécurité Informatique**

Une forte activité au Québec

Des structures émergentes en Afrique du Nord et Afrique centrale

Une volonté d'action commune auprès des instances européennes



CLUSIB (Club de la sécurité informatique belge)

8, Rue des Sols
1000 Bruxelles
Contact :
Tel : + 32 2 515 08 57
Fax : + 32 2 515 09 85
Secrétariat :  Jan Steenlant




CLUSSIL (Club de la sécurité des systèmes d'information Luxembourg)

c/o CRP Henri Tudor
29 rue John F. Kennedy
L-1855 Luxembourg - Kirchberg
Contact :
Tel : + 352 42 59 91 206
Fax : + 352 42 48 99
Secrétariat :  Anne Gaspard



CLUSIS (Club de la sécurité informatique suisse)

Case postale 9
CH 1026 Lausanne
Contact :
Tel : + 41 21 636 32 39
Fax : + 41 21 636 32 38
Secrétariat :  Sylvie Robert-Progin



CLUSIT (Associazione Italiana per la Sicurezza Informatica)

Università degli Studi di Milano
Dipartimento di Scienze dell'Informazione
Via Comelico 39, 20135 MILANO
Contact :
Tel : + 39 349 776 8882
Fax : + 39 02 700 440 566
 Secrétariat

The screenshot shows the CLUSIF website homepage. At the top, there is a navigation bar with the CLUSIF logo and the text "CLUB DE LA SÉCURITÉ DE L'INFORMATION FRANÇAIS". Below this, there are links for "Accueil", "Evénements", "Partenariats", "Espace Presse", and "Contacts". The main content area is divided into several sections: "Evénements" (with a sub-section for "Conférence CLUSIF : Social Engineering" dated 14 juin 2007), "Formations MEHARI 2007" (highlighted in a green box, with a sub-section for "Sessions de formation MEHARI 2007" dated 14 juin 2007), "Partenariats" (with a sub-section for "CRISIS'2007" dated 2 au 5 Juillet 2007), and "MEHARI 2007 disponible gratuitement !" dated 23 février 2007. On the right side, there is a sidebar with sections for "Le CLUSIF", "Productions", and "Services". The website is displayed in a browser window with the address bar showing "http://www.clusif.asso.fr/".

Social engineering : constats

Ca marche ! (utilisation de ressorts psychologiques et non d'une ressource technologique)

Les enjeux

- Divulcation de l'identifiant et du mot de passe mais aussi toute forme de renseignement
- Sensibiliser vos utilisateurs à cette menace
- Modifier le comportement sécuritaire de vos utilisateurs

Une action en deux étapes

- Imposture à la qualité
- Mise en condition de la personne (obtention de l'information)

Social engineering et hacking

Une action sur site ou à distance (téléphone, mèl dont *phishing*)

Un amateurisme toutefois très souvent performant s'appuyant sur des principes variés

- La technique du caméléon, modification de l'apparence physique, emploi d'accessoires caractérisant une activité...
- Le stress par le degré d'urgence de la requête ou l'énervement de l'interlocuteur
- *A contrario*, le ressort « aide à autrui »

Social engineering : mesures de déception

Camouflage de l'action : la personne ne gardera pas « souvenir » de cette action de captation d'information

Camouflage de la recherche : l'information recherchée est « noyée » dans le flot des échanges

Améliorer son savoir-faire : les apports de la psychosociologie

Social engineering : plan de session

Introduction

- Pascal LOINTIER, ACE Europe

Aspects offensifs : test de pénétration

- Stéphane Jourdois, ARSeO

Les cas vécus par les services d'Etat

- Yves Crespin, BEFTI

Principes de psycho-sociologie

- Danielle Kaminsky, universitaire

Aspects défensifs : comportement sécuritaire des utilisateurs

- Paul Grassart, consultant indépendant