CNSA-LAP WORKSHOP

COMBATE AO SPAM
SPAM-FIGHTING

LISBOA 7-9.10.2009

ANACOM

MÉTODOS DE INVESTIGAÇÃO UTILIZANDO PERSPECTIVAS DE DEFESA DO CONSUMIDOR NA INTERNET

José Faísca

DIRECÇÃO-GERAL
CONSUMIDOR

- CPC
- Sweep Days
- Investigation on the Web
- FraudenaNet
- Development of projects

CPC Network

- Administrative cooperation – why is it necessary?

  Increasing number of fraudulent activities are taking place across borders, making it difficult for the national authorities to pursue enforcement against traders in another country.

CPC Network

REGULATION (EC) No 2006/2004 OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL

of 27 October 2004

On cooperation between national authorities responsible for the enforcement of consumer protection laws (the Regulation on consumer protection cooperation)

CPC Network

- Scope:

  Cross border infringement of EU consumer protection laws (intra-community infringement)

- Infringements of EU Regulations + National law transposing EU Directives that protect consumers' interests (listed in the Regulation Annex – nearly twenty European pieces of legislation)
- Cross-border cases (broad definition)
- Collective interest of consumers

CPC Network

- Objective:

  To promote cooperation among public authorities responsible for the enforcement of consumer protection laws in cross border cases.

CPC Network

- Art. 6: Exchange of information upon request
- Art.7: Exchange of information without request
- Art.8: Request for enforcement measures
- Art.9: Coordination of market surveillance and enforcement activities

CPC Network

- Art.9: Coordination of market surveillance and enforcement activities – **consumer protection in the internet**
- Sweeps
- Providing methods and data for investigations

Sweep Days

What is a “Sweep Day” on the Net

An "EU sweep" is a joint EU investigation and enforcement action to check for compliance with consumer protection laws. It involves carrying out a targeted and coordinated check on a particular sector in order to see where consumer rights are being hindered or denied. National enforcement authorities then follow up on these findings, contacting the incompliant companies and demanding that they come into line with the relevant requirements. Legal action can be taken against operators who violate EU consumer law.

Sweep Days

What is a “Sweep Day” on the Net

Who controls it / how it is done
National participation
Choosing the sectors to be investigated
Establishing the timetable and methodology
Reports and public procedures
Regularity of Investigations

Sweep Days

- **How does a sweep work in practice?**
- There are two phases:
- 1. The first phase is the **co-ordinated sweep action**. National authorities systematically and simultaneously check a particular market for practices which breach EU consumer law. All the authorities use a common checklist of irregularities that they are looking for. For instance, it is against EU-wide consumer rules not to provide full contact details of the trader, or not to inform online buyers clearly about their right to withdraw from the transaction.

Sweep Days

- **How does a sweep work in practice?**

- 2. The second phase is the **enforcement action**. During this phase, authorities will further investigate traders which are suspected of irregularities, and take follow-up actions to ensure that non-compliant conduct is corrected and to impose appropriate sanctions. National authorities will investigate and take enforcement actions for national cases. For cross-border cases (where the trader operates from another country), enforcement authorities can ask for assistance from authorities in other countries.

Sweep Days

- **How does a sweep work in practice?**

  2nd phase: Enforcement action (cont.)

- This is possible thanks to the Consumer Protection Co-operation (CPC) Network of national enforcement authorities from 27 Member States and Norway & Iceland. During this enforcement phase the companies have a right of reply and an opportunity to correct practices which are illegal. Those who fail to do so can face legal action leading to fines and other sanctions or even to their web sites being closed.

Problems with Sweep Days

Choosing the practices or sectors
Different national market problems/complaints
EU Directives not fully harmonized : different National approaches
Public Reports
Legal actions
Repeating the investigation (follow-up sweep)
Regularity of investigations
How to improve actions

Sweep Days

- At an **European** level, DGC worked in three sweeps on the internet, which took place in 2007, 2008 and 2009 (*airplane tickets, mobile rings, electric goods*");
- On a **National** level, DGC, by the work of its Advertising Observatory, does regular sweeps on the internet monitoring the application of legislation concerning advertising, E-Commerce and unfair commercial practices.
- DGC participates also in **international** Sweeps, mostly the ones organized by RICC / ICPEN.

The Investigation on the Web Project

Initiated early 2008 by 5 EU Member States (PT included)
Has now 14 Member States

Objectives

- To create a special network of investigators
- To train people with skills to investigate
- To create an interacting Web page (portal) within de CPCS page, for E-consumers
- Special information/training sessions s
- Technical Manuals and procedures for investigation
- Taking the investigation further, not limited to legal/publicity aspects

The Investigation on the Web Project

Work in Progress

Better coordination and planning of the common Sweeps

New methodology and timetable

Using new IT Tools

Workshops and mobility of researchers

Promoting more “active” investigations (creating virtual accounts on websites, using e-cards to simulate a purchase…)

The Investigation on the Web Project

Work in progress

Manual for researchers

- Database of directories, domain names offices and specialized units in each country. Database includes reference to other common research tools.
- Tracking down the web
- Identification of persons /domains/IP addresses
- E-mail study/identification of sources/SPAM
- Other procedures according to the e-commerce Directive

The Investigation on the Web Project

Work in Progress

E-information and E-training for E-consumers

- Portal within the CPCS net facility
- Development of interacting tool for consumers
- Quiz, videos, comic strips
- Leaflet and booklet (“Know your rights when purchasing on the E-European space”)
- E-films (“viral” marketing, on line buying)
- Links to national sites

FraudenaNet

safer net = + confident consumers!

- Model: One Week action with closing Workshop (first event in April 2008)
- Motto: **Recognize, Report and Stop fraud on the Net**
- "Little Book of Scams" adapted as an easy guide with real examples
- One real case by day, fully disclosed through the net
- One USB Pen offered to the participants of the seminar and target groups, with the guide, the five daily real cases, the experts presentations, other related material and useful links.

SEMANA DE PREVENÇÃO DA FRAUDE

Trabalho em casa com promessa de rendimento

Maria, à procura de rendimento extra para o seu orçamento familiar, deparou-se com uma mensagem no seu e-mail, com o seguinte conteúdo "Gostaria de ganhar mais de 700 € por semana na tranquilidade da sua casa colando etiquetas em envelopes e dobrando circulares para serem colocadas em envelopes?" Maria, pensou que a mensagem era feita para si, poderia trabalhar à noite quando as crianças já estivessem deitadas e ganhar um rendimento extra. Respondeu, demonstrando o seu interesse. Recebeu rapidamente um formulário ou cupão de inscrição em que lhe foram solicitados os seus dados pessoais e remeteu a quantia que lhe foi pedida "para efeitos de encomenda do material necessário para realizar o trabalho." Esperou pela chegada do material com ansiedade, quando este chegou, Maria, verificou desiludida, que se tratava de um conjunto de fotocópias descrevendo como veicular mensagens idênticas, solicitar dinheiro para o material de trabalho e esperar que outros como ela desejando ganhar um rendimento extra respondessem enviando dinheiro, desta vez para si. Maria, compreendeu então que tinha sido vítima de um esquema enganoso que não existia qualquer oferta de trabalho nem remuneração associada mas apenas um esquema que a levou a perder 30 €.

A DG Consumidor recomenda:

1- Não efectue qualquer pagamento;
2- Obtenha informações claras relativas ao anunciante, nomeadamente sobre os seguintes aspectos:
a) Identificação e morada física,
b) Função a desempenhar,
c) Custos associados ao desenvolvimento do trabalho,
d) Remuneração aplicável e condições de pagamento.

Em caso de dúvida contacte a Direcção-Geral do Consumidor ou o Centro Europeu do Consumidor – CEC e as autoridades policiais.

Amanhã leia Compra de Veículo através a Internet

Dia 10 de Abril no Centro de Congressos do TagusPark, das 14h 30m às 18h 30m.
Esquemas e Fraudes na Net. Protecção dos Consumidores.
Inscrições: fraudenanet@dg.consumidor.pt

www.consumidor.pt

SEMANA DE PREVENÇÃO DA FRAUDE

Phishing-Vishing

O Manuel recebeu um e-mail do banco através da qual investe na Bolsa. O banco pede-lhe que telefone para o número indicado, para efeitos de actualização da base de dados da sua carteira de clientes GOLD.
Ao ligar Manuel é atendido por um atendedor automático que lhe solicita dados pessoais para efeitos de 'verificação de segurança'; após fornecimento dos dados a 'máquina' agradece e a chamada termina.
No dia seguinte Manuel tenta pagar uma conta com o seu cartão de crédito e a operação não é autorizada.
Ao contactar com o seu gerente de conta compreende que foi vítima de phishing, na sua vertente vishing.
O telefonema que efectuou 'para o seu banco' não foi mais do que uma técnica de phishing para lhe roubar informações pessoais que posteriormente foram utilizados de forma fraudulenta, tendo-lhe sido retirado o dinheiro da conta por alguém que possuía os seus códigos pessoais.

A DG Consumidor informa:

Phishing é o método utilizado para roubar a identidade de um cibernauta. As técnicas de phishing podem utilizar malware ou spam e podem ser de diferentes tipos:
- 'SMiShing': os utilizadores de telemóveis recebem uma mensagem (SMS) confirmando a sua ligação a uma empresa de serviços e informando que esta cobrará uma determinada quantia diária se o dono do telemóvel não anular a sua ligação no site da empresa. O site, contudo, não é mais do que o meio utilizado para roubar dados pessoais ao utilizador (através de malware).
- 'Vishing': a técnica de VoIP (Voice over Internet Protocol) utiliza o telefone para roubar informações pessoais. É enviada um e-mail que aparenta ser proveniente de uma instituição legítima e que convida o receptor a telefonar para um determinado número. Quando as vítimas telefonam (pensando que irão falar com alguém da instituição que enviou o e-mail) são atendidas por um atendedor automático que solicita dados pessoais para efeitos de 'verificação de segurança'. Há situações em que os interessados prescindem do envio de e-mail e telefonam directamente às vítimas para recolher os seus dados pessoais.
-'Spear-phishing': consiste em enviar um e-mail que parece ser de um colega, chefe ou amigo e que consegue levar o receptor a divulgar dados pessoais e ainda pode permitir o controlo de todo o sistema informático da organização visada.

A DG Consumidor recomenda:

1. Nunca responda a um e-mail que lhe solicite PIN e passwords ou outros dados pessoais.
2. Invista através da Internet só em fornecedores de serviços financeiros licenciados (pesquise, informe-se e desconfie antes de iniciar uma relação comercial/financeira com a entidade em causa).
3. Desconfie de e-mails cujo tema é preocupante ou excitante (a escolha dos assuntos é feita de forma a chamar a atenção e levar as pessoas a reagir imediatamente, antes de se aperceberem da possível intenção fraudulenta).
4. Não clique em links que vêm em mensagens de e-mail ou em chats se suspeitar que a mensagem não é autêntica ou se não conhecer o emissor.

Em caso de dúvida contacte a Direcção-Geral do Consumidor ou o Centro Europeu do Consumidor – CEC e as autoridades policiais.

Amanhã leia mais sobre outras modalidades de PHISHING

Dia 10 de Abril no TagusPark, das 14h 30m às 18h 30m.
Esquemas e Fraudes na Net. Protecção dos Consumidores.
Inscrições: fraudenanet@dg.consumidor.pt

www.consumidor.pt

Model of the action

- Consumer Directorate (guide presentation and more)
- Gambling legal supervisor (lotteries and gambling)
- Bank Institution (Phishing and more)
- Instituto Superior Técnico - IST(Spyware, Malware and others)
- ITU / FIINA (Internet Dumping and Video Codecs)
- Criminal Police (Tips about informatics crime)
- Microsoft Internet safety division (how to protect personal computers)
- CEC (how to buy a car safely on the Net)
- CEC (presentation of “Howard” shop assistant tool)

- More : experts, press and media members.

Future developments/perspectives

- **Follow up of FraudenaNet project (development of an "E-Fraud Center" involving the competent authorities)**
- **More frequent internet sweeps, and reinforcement of the follow-up enforcement actions**
- **Maintenance of the "Investigations On the Web" EU project**
- **Broaden the collaboration with FCCN (domains register), ANACOM (Communications regulator), Criminal police and ISP's**
- **Gathering synergies to promote an "Internet Lab" targeting consumer protection, in order to support initiatives related to:**
- Information
- Training and education
- Assessment of Complaints
- Enforcement of legislation

We hope this Workshop will lead to new opportunities / new projects !

Thank You.

José Faisca, Manuel Tão

DIRECÇÃO-GERAL
CONSUMIDOR