Informática Jurídica – Licenciatura em Direito

PHISHING

Docente: José Manuel E. Valença

Realizado por: Ana Ferreira nº34875
Alexandra Cruz nº31618
Michelle Pinto nº31702

Braga 2005

Resumo

O tema da segurança das transacções não é novo, nem exclusivo de qualquer canal de acesso ou meio de pagamento. Existe nos cheques, nos cartões de crédito, e, pela crescente implantação do Internet *"banking"*,é cada vez mais um desafio também nesta área. Apesar de nenhuma das instituições financeiras portuguesas afirmar que já sofreu ataques, no estrangeiro já são muitos os ataques de "*phishing"* (aglutinação de *"password*") que se tem conhecimento.

Este trabalho tem como objectivo abordar esta questão do *"phishing*", sua problemática e consequências para uma sociedade cada vez mais dependente dos sistemas de informação. Ora, imposta por isso não defraudar as expectativas dos utilizadores destes sistemas procurando medidas "*anti phishing*".

Cada dia surgem na Internat novas ameaças que fazem com que estejamos actualizados no que respeita a *firewalls*, vulnerabilidade do sistema, virus, etc. Mas, a nova moda de delitos na Internet denomina-se Phishing. A grande diferença do anteriormente citado é que desta vez ninguém tenta aceder ao sistema com intençºoes maliciosas, nem tentam introduzir um virus que provoca o mau funcionamento do computador. Com um *phising*, é o próprio utilizador que envia informação pessoal e confidencial de forma voluntária; isso sim, animada mediante tecnicas de persuação

Actualmente, há vários casos que reflectem este problema, mas não há ainda no nosso ordenamento jurídico qualquer sanção prevista

A segurança nos sistemas de informação

" Ataques" a contas bancárias ameaçam dados pessoais"

" O "phishing" é um método utilizado por "hackers" para roubarem informações confidenciais"

Direitos dos cidadãos

Os direitos relativos à utilização da informática estão consagrados na Constituição da Republica Portuguesa (CRP) art.º35º e desenvolvidas na lei de protecção de dados. Os cidadãos têm sempre direito à informação, ao acesso, à rectificação e eliminação e à oposição. No entanto, para se precaver deverá ler sempre com atenção os impressos de dados antes de fornecer os seus dados pessoais e ter cuidado para não fornecer dados que lhe pareçam excessivos ou que violem a sua privacidade. Se de alguma forma lhe for negado o exercício do seu direito ou sempre que considere que os seus direitos não estão garantidos, pode apresentar queixa à Comissão Nacional de protecção de dados (CNPD). Se não entender bem para que serve o questionário, deve solicitar toda a informação necessária sobre a razão das perguntas e se também for o caso sobre quem vai conhecer a resposta. De qualquer maneira, nunca forneça dados pessoais que lhe pareçam excessivos. Em relação ao tratamento dos seus dados pessoais, para efeitos de marketing, caso não queira constar nessas listas, deverá enviar uma carta para a empresa em causa, manifestando o seu direito de oposição a receber mais correspondência, deverá dar-se direito de a empresa o retirar da listagem dos mailings.

A crescente necessidade de partilha de informação entre funcionários e empresas, leva a que, cada vez, mais, a informação se torne acessível para um maior número de pessoas e entidades. A Internet é um universo, cujo, conteúdo facilmente pode ser copiado. A partir de simples "*downloads*", é fácil aceder a pacotes completos de *software*, ou a códigos que permitem trocar e distribuir material informático de forma ilegal. E muitas coisas mais.

De acordo, com o relatório da *Anti- Phishing Working Group*, o número de ataques em Junho de 2004 ascendeu a 1422, sendo o principal país de origem os EUA, com 27%. Normalmente, os ataques são efectuados através do correio electrónico e a média de vida dos falsos sites é de 2,25 dias. No entanto, a forma como os piratas atacam é inovadora. Isto porque, não atingem as estruturas informáticas dos bancos, mas sim, os clientes. Utilizando bases de dados de "spam" (endereços de e-mails roubados), o "*phishing*" é vinculado, pelo envio de e-mails a clientes de "home-banking". Desta forma, ao abrirem a mensagem e o respectivo anexo, os clientes entram numa falsa página de Internet do banco e sem saberem introduzem a sua "*password*" ,fornecendo aos 'piratas' os dados de acesso às suas contas.

O que é o "phishing"?

O *Phishing*, não é mais, que a suplantação de web sites. Trata-se, de correios electrónicos enganosos e páginas web fraudulentas, que aparentam proceder de instituições de confiança (bancos, entidades finaceiras, etc.), mas, que na realidade estão desenhadas para enganar o destinário e conseguir que divulgue *informação confidencial.*

O termo *phishing* significa «pescar» em inglês, já na realidade tem semelhanças com pesca. Lançam um isco e esperam que alguém morda o anzol. A recompensa não pode ser mais saborosa: dados pessoais e códigos de acesso ás contas bancárias dos utilizadores.

Como é que funciona o Phising?

Através de um correio electrónico, simulando proceder de uma fonte fiável (por exemplo: do seu banco), tentam ter acesso aos dados necessários para enganar o utilizador. Na realidade, trata-se de mensagens massivas. Os burlões, não sabem qual é o banco do utilizador e ,por isso, criam um e-mail com aparência corporativa da entidade bancária escolhida e é enviado massivamente. A realidade, é que, esta mensagem acabará por chegar ás mãos de alguém que pertence a esse banco.

Trata-se, normalmente de mensagens com textos como: «por motivos de segurança...», ou «a sua conta deve ser confirmada....», ou «utilizadores do banco advertem»..., indicando ao utilizador que se estão a realizar mudanças e que por segurança deve introduzir os seus dados pessoais e códigos bancários e clicar no link indicado. Ao clicar é reencaminhado a uma página semelhante á do banco em causa. A verdade, é que essa página pertence ao burlão, que não tem mais, que copiar os dados fornecidos pelo utilizador. Ao finalizar é confirmada a operação e ficamos tranquilos e a pensar que eses dados foram recolhidos pelo banco.

Outras vezes, o mesmo e-mail pede ao utilizador que preencha com os seus dados um formuário e que clique em «enviar», sem necessidade de ser reencaminhado a outra página.

A supresa em ambos casos chegará quando o utilizadr tem conhecimento que a sua conta se encontra a zero, e o banco, o informa de que é vitima de um engano denominado "***Phishing"***.

Como se proteger do "Phishing"

A nova estrategia do *Phishing* adquiriu grande importancia a nivel mundial, no que respeita a utilizadores e a empresas, incluindo os próprios bancos, que não podem fazer nada pelos seus clientes que estão a ser enganados.

Actualmente, a única forma de evitar este tipo de fraudes consiste em estar informados. Infelizmente, nenhum anti-virus, nem nenhum sistema de segurança podem impedir estas fraudes. Seguindo estes conselhos, podemos proteger o utilizador:

(1) Ao receber um e-mail desconhecido, ao avisar o banco e confirmar a vericidade da mensagem.

(2) Tendo-se dúvidas o melhor é passar o cursor por cima do link em anexo á mensagem, muitas das vezes a direcção não é a mesma que aparece na mensagem;

(3) Estas mensagens, normalmente, não costumam estar personalizadas. Começam por «Estimado Cliente.»

(4) Também se pode confirmar que na parte inferior do navegador aparece um cadeado inteiro (não partido). Este simbolo, indica um Certificado de Autentacidade. Pode comprovar que não está caducado e que o proprietário do mesmo corresponde á página que está a visualizar.

No entanto, as técnicas de *Phishing* estão a aprender rápidamente este tipo de erros e estão a aperfeiçoa-los. Consiste em criar uma janela emergente exatamente na posição da URL na barra de direcções da Internet explorer, de forma que se sobrepõe e oculta a direcção real do servidor web,onde se encontra o utilizador, mostrando no seu lugar a URL da entidade bancária. A mensagem inclui um link que supostamnente está dirigido á Web da entidade bancária. Se o utilizador clicar no link, pode observar como aparece a Web da entidade e na barra de direcções do Internet Explorer aparece a URL correcta, incluindo o prefixo *http://* como se estivesse numa conexão segura

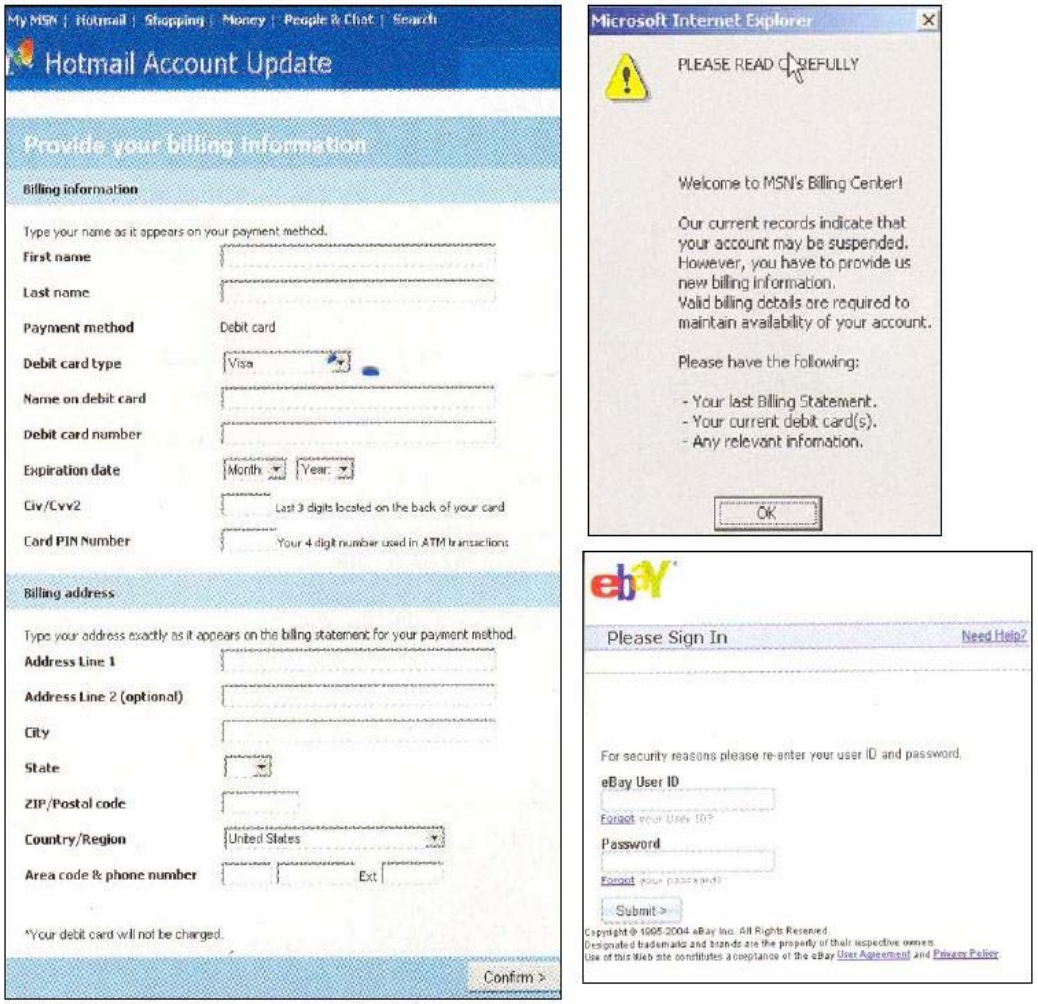
My MSN | Hotmail | Shopping | Money | People & Chat | Search
Hotmail Account Update
Provide your billing information
Billing information
Type your name as it appears on your payment method.
First name
Last name
Payment method
Debit card
Debit card type
Visa
Name on debit card
Debit card number
Expiration date
Month
Year
Civ/Cvv2
Last 3 digits located on the back of your card
Card PIN Number
Your 4 digit number used in ATM transactions
Billing address
Type your address exactly as it appears on the billing statement for your payment method.
Address Line 1
Address Line 2 (optional)
City
State
ZIP/Postal code
Country/Region
United States
Area code & phone number
Ext
*Your debit card will not be charged.
Confirm >
Microsoft Internet Explorer
PLEASE READ CAREFULLY
Welcome to MSN's Billing Center!
Our current records indicate that your account may be suspended. However, you have to provide us new billing information.
Valid billing details are required to maintain availability of your account.
Please have the following:
- Your last Billing Statement.
- Your current debit card(s).
- Any relevant infomation.
OK
ebay
Please Sign In
Need Help?
For security reasons please re-enter your user ID and password.
eBay User ID
Forgot your User ID?
Password
Forgot your password?
Submit >
Copyright © 1995-2004 eBay Inc. All Rights Reserved.
Designated trademarks and brands are the property of their respective owners.
Use of this Web site constitutes acceptance of the eBay User Agreement and Privacy Policy.

fig: 1

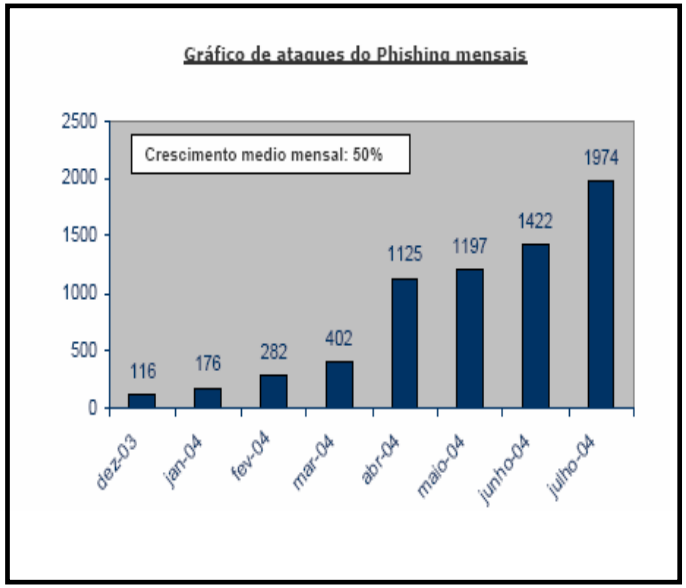
Gráfico de ataques do Phishing mensais
Crescimento medio mensal: 50%
2500
2000
1500
1000
500
0
116
176
282
402
1125
1197
1422
1974
dez-03
jan-04
fev-04
mar-04
abr-04
maio-04
junho-04
julho-04

fig: 2

Quais as organizações ou companhias mais atacadas pelo Phishing:

Quando falamos das organizações mais atacadas, fazemos referência aos correios elctrónicos fraudulentos, que parecem ser uma organização correcta. Obviamente, os mais atacados e realmente prejudicados são os utilizadores e os clientes dessa organização.

Empresa "Blanco"	Jul-04	Jun-04	Maio-04	Abr-04	Mar-04	Fev-04	Jan-04
Citibank	682	492	370	475	98	58	34
U.S.Bank	622	251	167	62	4	0	2
eBay	255	285	293	221	110	104	51
Paypal	147	163	149	135	63	42	10
AOL	41	14	17	9	10	10	35
Suntrust	25	4	1	5	1	0	0
Lloyds	23	24	17	15	4	0	1
Fleet	20	55	33	28	23	9	2
Barclays	17	19	15	31	11	6	1
Earthlink	15	7	6	18	5	8	9

fig: 3

Países com maior número de Web Stes alojados de Phishing:

Os EUA é mais uma vez o «lider» em número de alojamentos de Web Sites com *Phishing*. Outros países, incluindo a Russia, o Reino Unido e o México mostram um crescimento significativo de ter estas páginas.

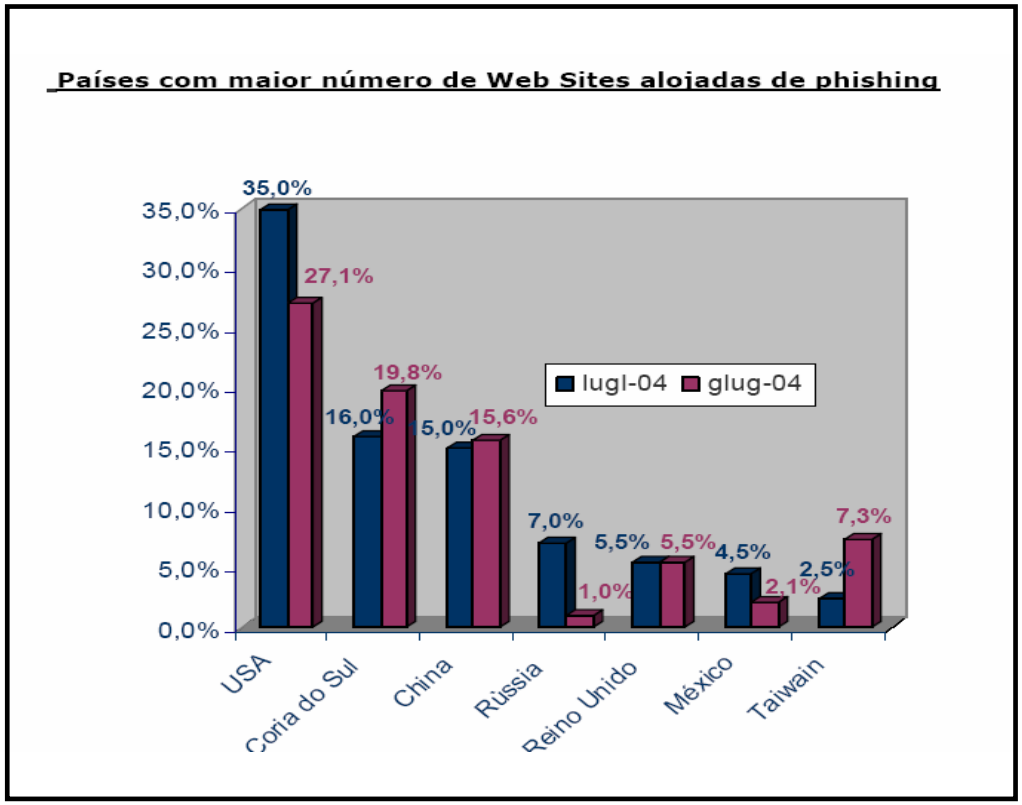
Países com maior número de Web Sites alojadas de phishing
35,0%
30,0%
25,0%
20,0%
15,0%
10,0%
5,0%
0,0%
lugl-04
glug-04
35,0%
27,1%
16,0%
19,8%
15,0%
15,6%
7,0%
1,0%
5,5%
5,5%
4,5%
2,1%
2,5%
7,3%
USA
Coria do Sul
China
Russia
Reino Unido
México
Taiwain

fig: 4

Da mesma forma que a segurança da nossa casa não está dependente da espessura da porta,como também, não nos esquecemos de a trancar ao sair, ou de não entregarmos a chave a desconhecidos, também, a segurança do *Internet banking* depende tanto do utilizador como do banco. O banco deve assegurar a utilização de tecnologias e procedimentos seguros, enquanto, que o cliente, deve, em comtrapartida, assegurar a confidencialidade dos seus dados de acesso, não os divulgando a terceiros, protegendo o seu computador contra programas maliciosos que possam, se alguma forma fraudulenta, captar essa informaão. A defesa em relação a programas maliciosos deve ser assegurada através, nomeadamente, da actualização frequente do sistema operativo e utilização de programas «*anti-spyware*». No caso de outras tipologias de ataque, como o «*Phishing*» é fundamental estar alerta para algumas regras básicas de segurança.

No entanto, todos os cuidados são poucos. Os utilizadores do «Home-banking» devem sempre, verificar os Certificados Digitais que asseguram a codificação de toda a informação reservada entre cliente e banco. Em alguns bancos, como no Millennium bcp, é solicitado ao cliente que introduza dois digitos do Bilhete de Identidade ou o *NIF*. O BESnetb é baseado numa plataforma segura, utilizando encriptação da informação através de SSl de 128 bits. Também, o sistema de códigos de acesso utilizado com inserção do PIN através de teclado virtual e obrigatoriedade de confirmação de transacções com um código de segurança de 2º nivel variável, corresponde ás melhores práticas de controlo do risco de fraude. Estas e outras práticas de utilização segura, são frequentemente comunicadas aos clientes, quer no momento de adesão ao serviço, quer, em mensagens de serviço disponibilidade através do próprio «*Internet Bankinhg*».

Reflexo desta Problemática…

Raras são as Instituições Bancárias que assumem ser alvo de fraude na Internet, isto porque, levaria à falta de confiança dos seus clientes *on-line*, o que faria com que houvesse o perigo de perda da carteira de clientes. No entanto, no passado dia 27 de Abril uma instituição bancária Caixa Geral de Depósitos assumiu tal facto. Informaram os seus clientes da banca electrónica da existência de um “clone” da página da “Caixa”, que tem por objectivo, obter os códigos de acesso utilizados pelos clientes do site do banco, solicitando aos utilizadores a inserção dos códigos de acesso às contas bancárias, a fim de proceder a um suposto teste de segurança.

Para confirmar o que atrás foi dito a CGD não adianta qualquer número acerca dos casos de *Phishing* ,por isso, desconhece-se se alguém terá “caído” na burla, bem como os montantes que possam ter sido desviados. Ainda assim, o banco lembra, que nos casos de páginas falsas, pouco pode fazer, além de informar as autoridades e alertar os utilizadores para que nunca forneçam os seus códigos acesso a ninguém.

Apesar de ser uma cópia, a página criada pelos burlões apresenta alguns traços que permitem distingui-la da original: é o caso do domínio cgdi.pt e alguns erros ortográficos.Do que se trata afinal é da análise do conceito de confidencialidade neste tipo de relações on- line.

A definição clássica de confidencialidade é a garantia do segredo de informações dadas pessoalmente em confiança e a protecção contra a sua revelação não autorizada. Actualmente, a confidencialidade é considerada como o dever de guardar todas as informações que dizem respeito a uma pessoa, isto é, a sua privacidade. A confidencialidade é o dever que inclui a preservação das informações privadas.

O objectivo do processo de identificação é a garantia de direitos do identificado, e para tal, podem existir duas abordagens distintas a esse problema: por um lado temos a identificação por atributos em que a segurança se identifica com a incapacidade pelo identificado de repúdio da personalidade; por outro lado temos a identificação por acto de vontade, em que a segurança se identifica com a incapacidade por qualquer outro agente (incluindo o identificador) da assunção de personalidade alheia. No nosso ensaio, é abordada a identificação por acto de vontade, que tem como forma mais comum a revelação controlada de um segredo que assume a forma do chamado protocolo login- password. No entanto, este protocolo apresenta problemas: se a sua comunicação for via canal público, qualquer agente com acesso ao canal pode assumir a sua personalidade; e se o identificador for um agente eventualmente hostil ao identificado pode usar o " segredo" para assumir a personalidade do identificado perante terceiros. Então, qualquer pessoa pode ter acesso a este segredo quando o canal é público, pelo que este protocolo só é recomendado quando a comunicação é feita sobre canal confidencial e quando o identificador é um "agente amigo". A este protocolo existe uma alternativa que passa pelo ***protocolo desafio – resposta****, que na prática é o mesmo que dizer, que, só se acederá a determinadas informações confidenciais se se souber a resposta àquele desafio. Todavia, este é um protocolo computacionalmente mais complexo e não acessível a qualquer utilizador dos sistemas de informação. Assim, como nenhum dos dois ultrapassa estas dificuldades, uma solução mediadora seria a que conseguisse conciliar vantagens de um e de outro, ou seja, optar pela identificação por representante. O telemóvel poderia concretizar esta solução na medida em que funciona num canal privado e o sujeito tem a sua posse, pelo que este não irá agir de modo hostil.*

Actualmente, não temos no nosso Ordenamento Jurídico qualquer solução para estes casos, ao contrário do que se passa com países como os EUA e o Brasil. Na prática, a responsabilidade (por estes casos de burla pela Internet) é repartida entre a instituição bancária e o seu cliente, mas, não o sabemos em termos rigorosos, pois, como já o dissemos, por um lado, as instituições de crédito não assumem tais hipóteses e por outro, não temos relatos de clientes defraudados.

Bibliografia:

Internet:

- www.hispasec.com/unaaldia/2163
- www.vnunet.es/actualidad/noticias/seguridade/privacidade/20040927017
- www.el-mundo.es/navegante/2004/09/27/seguridad/1096287700.html
- http://www.antiphishing.org/