



PHISHING: FRAUDE NA INTERNET

1. O QUE PRECISA SABER SOBRE O PHISHING:

Cada dia surgem na Internet novas ameaças que fazem com que estejamos actualizados no que respeita a firewalls, vulnerabilidades do sistema, vírus, 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 intenções maliciosas, nem tentam introduzir um vírus que provoca o mau funcionamento do computador. Com um phishing, é o próprio utilizador que envia informação pessoal e confidencial de forma voluntária; isso sim, animado mediante técnicas de persuasão.

2. 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 financeiras, etc.), mas que na realidade estão desenhadas para enganar o destinatário e conseguir que divulgue informação confidencial.

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

3. COMO É QUE FUNCIONA O PHISHING?

Através de um correio electrónico, simulando proceder de uma fonte fiável (por ex: do seu banco), tentam ter acesso aos dados necessários para enganar o utilizador. Na realidade trata-se de mensagens massivos. Os burlões não sabem qual é o banco do utilizador e por isso cria um e-mail com a aparência corporativa da entidade bancária escolhida e é enviado massivamente. A realidade é que essa mensagem acabará por chegar as 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 clicando no link indicado. Ao clicar é reencaminhado a uma página semelhante à 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 esses dados foram recolhidos pelo banco.

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

A surpresa em ambos casos chegará quando o utilizador tem conhecimento que a sua conta se encontra a zeros, e o banco o informa de que foi vítima de um engano denominado Phishing.



3. O QUE PODE FAZER PARA PROTEGER-SE DO PHISHING

A nova estratégia de Phishing adquiriu grande importância a nível 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-vírus, nem nenhum sistema de segurança podem impedir estes fraudes. Se Seguir estes conselhos, irá a ajudar a proteger-se a si e à sua informação:

1. In primo luogo, e forse il più importante, è che dobbiamo ricordare che le Banche o Casse di risparmio si comunicano sempre per corriere tradizionale. Non le chiederanno mai di introdurre dati personali o bancari in una mail.
2. In Spagna stanno cominciando a prodursi questo tipo di casi di truffa in banche spagnoli, però per il momento sono scarsi e le mail che stanno ricevendo l'utenti stanno scritti in inglese. È logico pensare che una Banca spagnola non invierà comunicati in inglese.
3. Ao receber um e-mail desconhecido, é sempre aconselhável avisar imediatamente o seu banco para confirmar a veracidade da mensagem.
4. Observar se a direcção começa com https: em vez de http: (a "S" indica que a página encontra-se num servidor seguro.)

ATENÇÃO: As técnicas de Phishing estão a aprender rapidamente deste tipo de erros e estão a aperfeiçoá-los. Consiste em criar uma janela emergente exactamente 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 supostamente está dirigido à Web da entidade bancária. Se o utilizador clique 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 https:// como se estivesse numa conexão segura. Se ha qualsiasi dubbio, può passare il cursore sopra il link allegato alla mail. Molte volte l'indirizzo non è lo stesso che appare nel messaggio.

5. Se tem alguma dúvida, pode passar o cursor por cima do link anexo à mensagem. Muitas vezes a direcção não é a mesma que aparece na mensagem.
6. Outra forma de reconhecer estas mensagens é que não estão personalizadas. Normalmente começam com: "Estimado cliente...".
7. Tente não aceder as suas Web Sites financeiras de confiança através de link facilitados ou direcções de Internet de origem desconhecida.
8. Também pode confirmar que na parte inferior do navegador aparece um cadeado inteiro (não partido). Este símbolo indica um certificado de autenticidade. Pode comprovar que não está caducado e que o proprietário do mesmo corresponde à página que está a visualizar.



Queremos recordar que o Phishing não é nada novo, já que não se estende unicamente às entidades financeiras. Em geral devemos ser cautelosos e suspeitar de qualquer entidade emergente que nos peça dados bancários. Outros fraudes com mensagens falsas podem prejudicar os utilizadores do Hotmail. Outro dos sectores mais prejudicados são os leilões e as vendas on-line.

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

Name on debit card

Debit card number

Expiration date

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

Area code & phone number Ext

*Your debit card will not be charged.

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 information.



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?](#)

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](#).



5. REPERCUSSÕES DO PHISHING

Actualmente, os casos mais graves relacionados com o Phishing foram produzidos nos Estados Unidos, no entanto as "máfias" deram conta do seu enorme potencial, por isso a sua expansão está a produzir-se a nível mundial, principalmente em países anglófonos onde está cada dia mais concentrado.

A empresa Gartner analisou o problema do Phishing e realizou um interessante estudo sobre este fenómeno nos Estados Unidos. De seguida vamos expor as conclusões mais relevantes.

I tentativi di frode contro i consumatori in Internet, meglio conosciuti come phishing, sono diventati così comuni che si stima che 57 milioni di statunitensi hanno ricevuto qualsiasi tipo di messaggio elettronico fraudolento, d'accordo con un nuovo studio presentato da Gartner. Le perdite dirette del frode d'identità contro queste vittime riguardanti questo tipo di attacchi di phishing, costarono alle Banche e Compagnie de credito circa 1,200 milioni di dollari l'anno scorso.

Basati in una inchiesta applicata a 5,000 adulti che usano Internet, gli analisti di Gartner stimano che approssimativamente 30 milioni di adulti utenti della Web credono che hanno sofferto un attacco di phishing, mentre che altri 27 milioni credono che è stato un tentativo di frode.

I tentativi di attacchi phishing non sono nuovi, però sono diventati più comuni nei ultimi 12 mesi. D'accordo con l'inchiesta della ditta consulente, il 76% dei attacchi sospettosi accaddero nei ultimi sei mesi (da ottobre del 2003), e altro 16% successe sei mesi fa o prima. Quindi, i risoltati combinati suggeriscono che il 92% dei tentativi di frode si sono prodotti nell'ultimo anno.

"Le istituzioni finanziarie, fornitori di servizi di Internet e altri fornitori di servizi devono considerare seriamente questi tipi di frodi", disse Avivah Litan, vicepresidente e direttore di investigazione della ditta. "Questi fornitori di servizio devono agire e applicare soluzioni che minimizzino o evitino il rischio, sebbene i fornitori dei servizi non siano vittime dirette.

Eventualmente, tutti quelli utenti della posta elettronica si vedranno affettati per una mancanza di fiducia del consumatore nelle sue transazioni si i frodi non sono ridotti in maniera significativa dai livelli in cui attualmente si trovano.

L'attacco di Phishing accade quando un "ciberpirata" invia un messaggio che contiene un link a un sito di rete fraudolento dove si sollecita all'utente di fornire informazioni sul suo conto personale. Il messaggio e il sito web si trovano tipicamente mascherati simulando essere il sito di un fornitore di fiducia, istituzione finanziaria o di commercio on line degli utenti.

L'inchiesta di Gartner, conclusa in Aprile, mostrò un alto grado di successo da parte dei truffatori. Basandosi nei risoltati dell'inchiesta, Gartner stima che circa il 19% dei attaccati o quasi 11 milioni di statunitensi adulti che usano Internet, hanno cliccato in un messaggio di tentativo di frode. Peggio ancora, il 3% dei attaccati, uno stimato di 1.78 milioni di adulti affermano aver dato ai truffatori le sue informazioni finanziaria o personale.



I dati indicano che "le vittime di frodi tipo phishing sono quasi tre volte tanto propense a identificare un fraude, come possono esserlo altri consumatori on line", menzionò Litan. "In qualsiasi modo che si veda, i ladroni stanno ottenendo i loro obiettivi fraudolenti. I fornitori di servizi non hanno altra scelta che combattere detti messaggi, se vogliono che la computazione on line ritorni a essere sicura come un canale per le transazioni on line con i clienti".

Le soluzioni contro le frodi tipo phishing, da messaggi con firma elettronica digitale fino a servizi anti-phishing amministrati, sono alcune delle tecnologie che discuteranno nelle ricerche future da Gartner.

6. LUTANDO CONTRA O PHISHING

6.1 ANTI-PHISHING WORKING GROUP" (APWG)

A rápida proliferação deste novo fraude converteu-se nas principais causas de luta das empresas contra os delitos on-line. Nos Estados Unidos criou-se "Anti-Phishing Working Group"(APWG). Trata-se de uma associação de indústrias cujo o principal objectivo é acabar com este novo esquema de furto de identidade. Se deseja mais informação sobre esta organização, pode visitar o seguinte site: <http://www.antiphishing.org>; no caso que detecte um fraude sobre do phishing, pode denunciá-lo enviando um e-mail a: reportphishing@antiphishing.org.

Esta organização realiza um relatório mensal analisando todos os ataques de phishing denunciados à APWG. O último relatório publicado corresponde a Julio de 2004 e podemos encontrá-lo na sua Web Site (em inglês). A seguir destacamos os dados mais relevantes do relatório.

Anti-Phishing Working Group
APWG
register

Anti-Phishing Working Group

Committed to wiping out Internet scams and fraud

[report phishing - click here](#)

- [Home](#)
- [Phishing Archive](#)
- [Report Phishing](#)
- [Events](#)
- [APWG News](#)
- [Resources](#)
- [Membership](#)
- [APWG Member Site](#)
- [Contact Us](#)
- [JOIN THE APWG](#)

PARTNER EVENT:

Spam Compliance

inbox EAST
THE EMAIL EVENT

What is Phishing?

Phishing attacks use 'spoofed' e-mails and fraudulent websites designed to fool recipients into divulging personal financial data such as credit card numbers, account usernames and passwords, social security numbers, etc. By hijacking the trusted brands of well-known banks, online retailers and credit card companies, phishers are able to convince up to 5% of recipients to respond to them.

Date	Cumulative Phishing Attacks	Weekly Phishing Attacks
5/1/2004	215	279
5/8/2004	441	268
5/15/2004	748	321
5/22/2004	1056	310
5/29/2004	1274	224
6/5/2004	1588	315
6/12/2004	1928	339
6/19/2004	2231	303
6/26/2004	2558	324
7/3/2004	2976	424
7/10/2004	3387	418
7/17/2004	3816	419
7/24/2004	4241	385
7/31/2004	4745	504

News and Events:

- 30-Aug-04 - New Phishing Trends Report Available!
[Phishing Attack Trends Report - July 2004](#)

Anti-Phishing Working Group
The Anti-Phishing Working Group (APWG) is an industry association focused on eliminating the identit and fraud that result from the grov problem of phishing and email spc

APWG Members

- Over 636 members
- Over 407 companies
- 8 of the top 10 US banks
- 4 of the top 5 US ISPs
- Over 100 technology vendors
- Law enforcement from Australia, Canada, UK, USA

APWG Working Groups

- Best Practices
- Education
- Future Threat Models
- Phishing Repository
- Sizing the Problem
- Solution Evaluation/Trial
- Law Enforcement

APWG SPONSORS:



6.2 DADOS

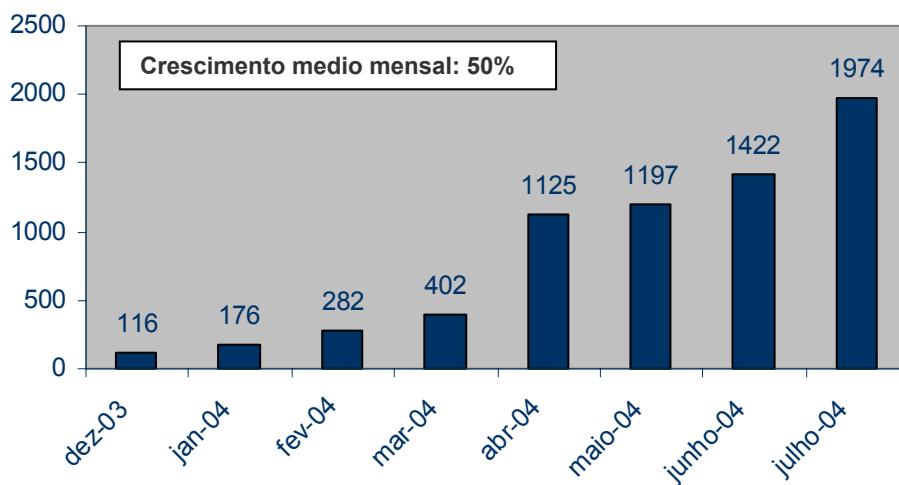
- ▶ Número de ataques únicos de phishing* reportados durante Julho: **1974 ataques**
- ▶ Media mensal do ratio do crescimento: **50%**
- ▶ Organização mais prejudicada durante Julho: **Citibank (682)**
- ▶ País com maior número de Web Sites alojadas de phishing: **USA (35%)**

*Um "ataque único de phishing" define-se neste análise como um envio massivo de correios electrónicos enviados de uma vez só, destinados a uma companhia ou organização, e escritos na mesma linha de texto.

▶ NÚMERO DE ATAQUES ÚNICOS DE PHISHING

Em Julho, produziram-se 1974 novos e únicos ataques de phishing denunciados à APWG. Isto significa um aumento de um 39% sobre o número de ataques registrados no mês de Junho (1422). A média de números de ataques diários registrados em Julho foi de 63.7 (dado muito significativo considerando que em Junho a média foi de 47.6). Só na última semana desse mesmo mês registaram-se cerca de 500 ataques.

Gráfico de ataques do Phishing mensais



Fonte: Anti-Phishing Working Group



► **QUAIS SÃO AS ORGANIZAÇÕES OU COMPANHIAS MAIS ATACADAS PELO PHISHING?**

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

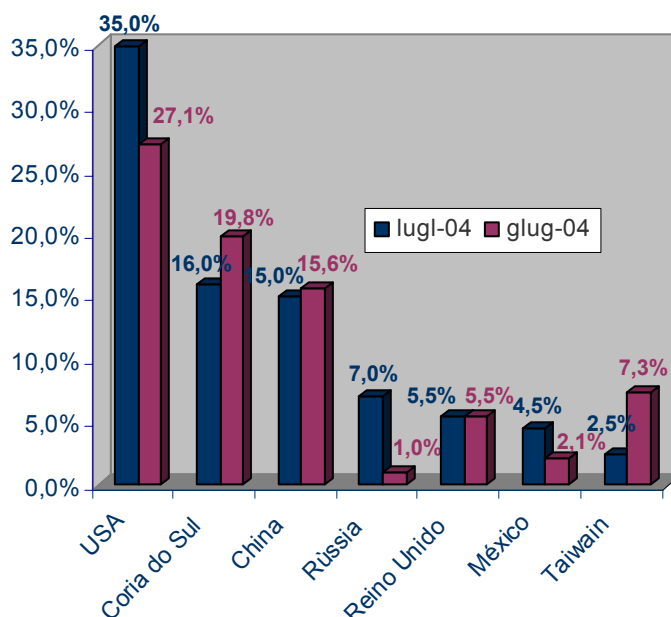
Empresa "Blanco"	Jul-04	Jun-04	Mai-04	Abr-04	Mar-04	Fev-04	Jan-04
Citibank	682	492	370	475	98	58	34
U.S.Bank	622	251	167	62	4	0	2
eBay	255	285	293	221	110	104	51
Paypal	147	163	149	135	63	42	10
AOL	41	14	17	9	10	10	35
Suntrust	25	4	1	5	1	0	0
Lloyds	23	24	17	15	4	0	1
Fleet	20	55	33	28	23	9	2
Barclays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

Fonte: Anti-Phishing Working Group

► **PAÍSES COM MAIOR NÚMERO DE WEB SITES ALOJADAS DE PHISHING**

Estados Unidos uma vez mais é o país "líder" em número de alojamentos de web Sites com phishing. Outros países, incluindo Rússia, Reino Unido e México mostraram um crescimento significativo no alojamento de estas páginas.

Países com maior número de Web Sites alojadas de phishing



Fonte: Anti-Phishing Working Group



6.3 CICLO DE VIDA DE WEBS PHISHING

A média de “vida” de este tipo de Webs fraudulentas é de 6.1 dias. Até à data, a Web Phishing que permaneceu activa durante mais tempo teve uma duração de 31 dias (funcionou durante um mês completo).

BIBLIOGRAFIA

Jornais:

- ▶ Personal Computer: Ottobre 2004. Nº 21
- ▶ PC Pro: Nº 51 2004

Internet:

- ▶ www.hispasec.com/unaaldia/2163
- ▶ [www.vnunet.es/Actualidad/Noticias/ Seguridad/Privacidad/20040927017](http://www.vnunet.es/Actualidad/Noticias/Seguridad/Privacidad/20040927017)
- ▶ [www.el-mundo.es/navegante/ 2004/09/27/seguridad/1096287700.html](http://www.el-mundo.es/navegante/2004/09/27/seguridad/1096287700.html)
- ▶ <http://www.antiphishing.org/>

Relatòrios:

- ▶ Anti-Phishing Working Group. “Phishing Attack Trends Report - July 2004.” Julio 2004