



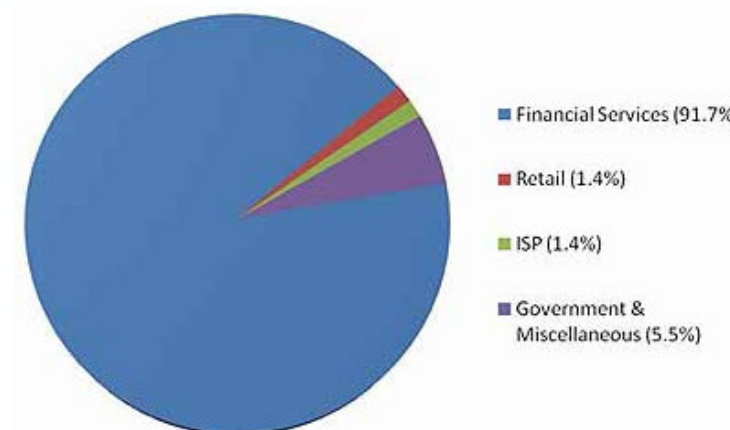
# **Phishing**

## **Definição e Recomendações**

Information Technologies

## Definição de Phishing\*

- Fraude electrónica caracterizada pela tentativa de **obtenção de dados privados** ou **informação sensível** de um utilizador
- Quem pratica este tipo de crime, faz-se passar por uma entidade credível ou de confiança do utilizador, de forma a obter a sua informação
- Esta **personificação** pode ser feita por **e-mail**, **mensagem (chat)** ou através de **outros sites**
- Hoje em dia grande parte dos crimes de phishing ocorre no âmbito de instituições financeiras
- Dados estatísticos de Dez/2007 (IN APWG):



\* O termo “phishing” tem origem na palavra “fishing” e consiste numa alusão aos “iscos” utilizados para capturar informação sensível, cada vez mais sofisticados.

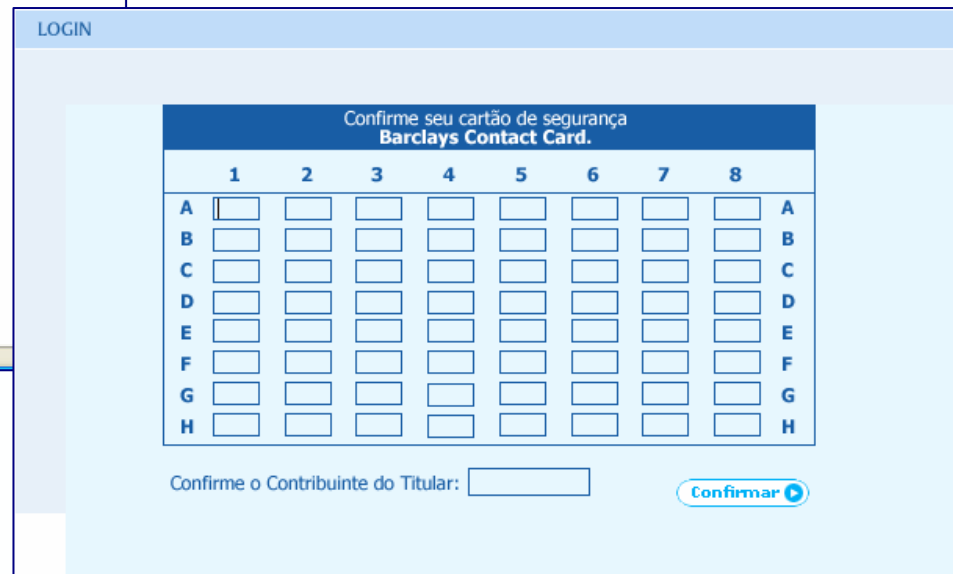
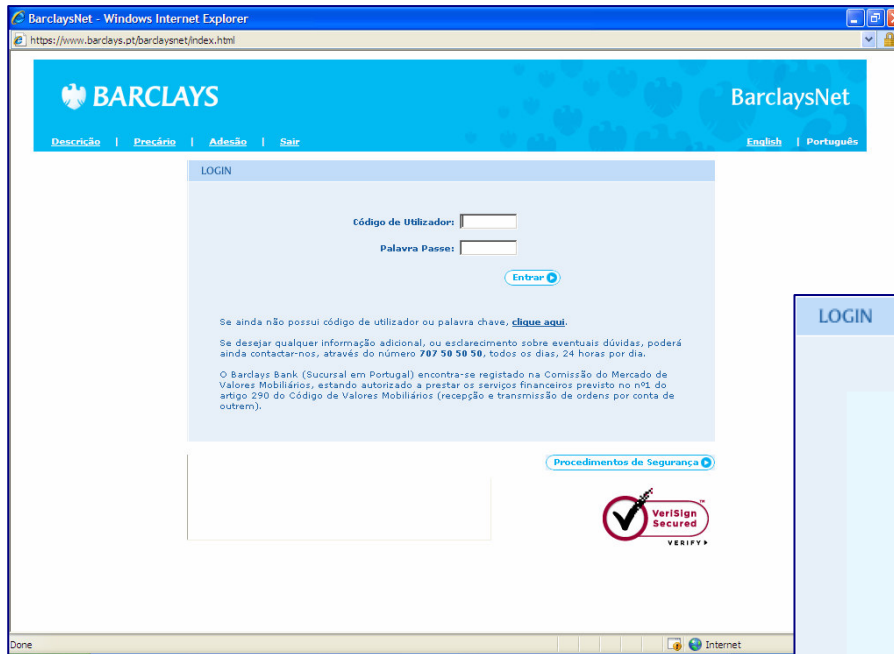


## Exemplo de Phishing

- Envio de e-mail, personificando uma entidade bancária, com pedido de **confirmação dos códigos pessoais** do utilizador ou Cliente (username, password, cartão matriz, etc.)
- O cliente **responde directamente ao e-mail, preenche o formulário** enviado, ou **accede ao falso site**, e fornece a sua informação pessoal, acreditando tratar-se de um pedido fidedigno
- “Verifique a sua conta”
  - O banco não solicita qualquer tipo de informação sensível através de e-mail ou contacto telefónico
- “Se não responder no prazo de 48 horas, a conta será encerrada”
  - É inculido um carácter de urgência para que o cliente não tenha tempo para pensar
- “Clique na ligação para aceder à conta”
  - Os links enviados por e-mail podem estar mascarados para abrir ficheiros infectados com vírus, ou aceder a sites fictícios



# Exemplo de Phishing (Barclays 2008)





## Identificar Sites de Phishing

- Podem ser utilizados endereços semelhantes aos originais, para mascarar os sites fictícios
- Exemplo:
  - [www.barclays-pt.com](http://www.barclays-pt.com)
- Links em sites de terceiros podem apontar para sites diferentes dos que anunciam

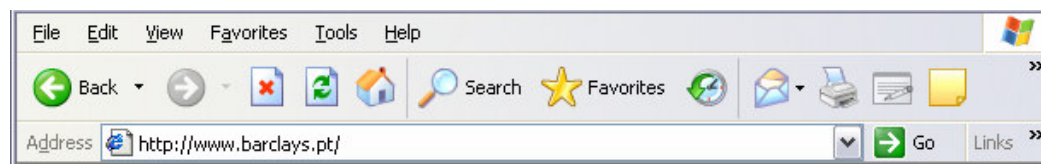


## Recomendações de Segurança

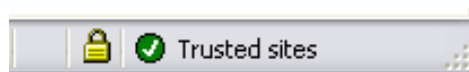
- Verificar o remetente dos e-mails recebidos
- Não fazer download ou executar arquivos não solicitados
- Manter um antivírus actualizado com os últimos updates
- Manter o sistema operativo (ex.: Windows) actualizado com os últimos updates
- Manter uma firewall activa durante a ligação à Internet

## Recomendações Anti Phishing

- Não responder a supostas solicitações de informação pessoal, por e-mail ou telefone
- Aceder ao site de homebanking escrevendo directamente o seu endereço no browser



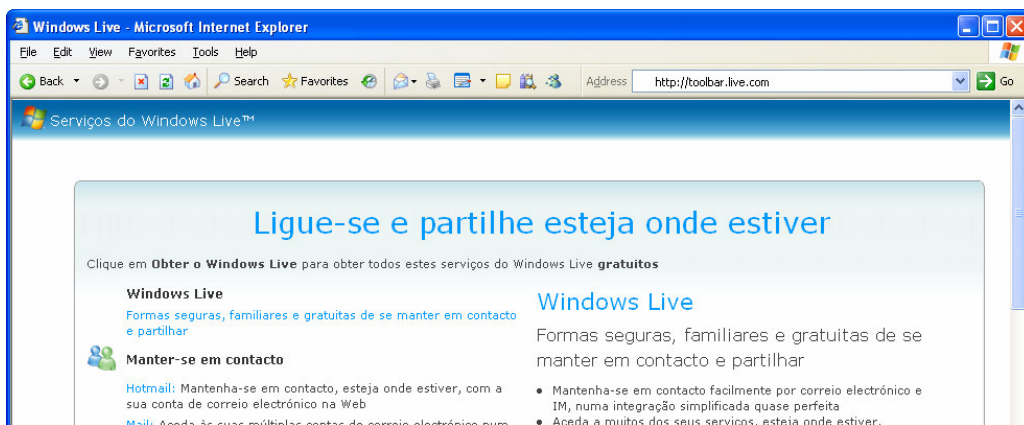
- Verificar se é estabelecida uma sessão segura quando se autentica no site de homebanking



- Rever periodicamente os movimentos da(s) conta(s) e cartões
  - Verificar se todas as transacções são legítimas
- Denunciar qualquer suspeita de tentativa de obtenção de dados pessoais ao banco e às entidades competentes
  - AWPG: [reportphishing@antiphishing.org](mailto:reportphishing@antiphishing.org)

## Filtros de Phishing

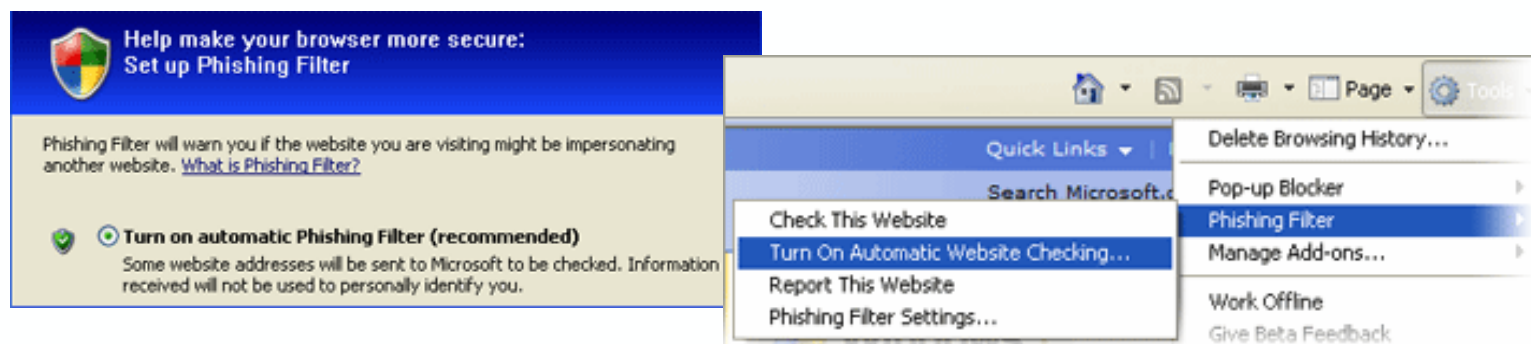
- Filtro incorporado num browser, que verifica os endereços das páginas visitadas, e identifica sites classificados como suspeitos
- Serviço online actualizado, que bloqueia acesso a sites denunciados como phishing
- Sistema que permite a denúncia de sites potencialmente fraudulentos, para verificação e identificação caso seja confirmado
- Para obter um filtro de phishing para o Internet Explorer 6, pode recorrer-se à instalação da barra de ferramentas do Windows Live
  - <http://toolbar.live.com>



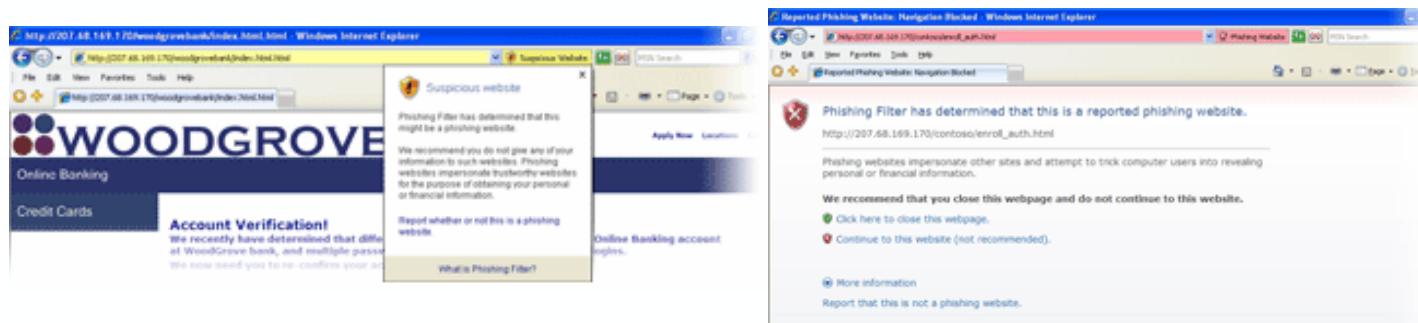
Obter o Windows Live

## Filtros de Phishing (IE7)

- Ao abrir um site de homebanking, pode ser activado o filtro para correr de forma automática
- Esta configuração pode ser feita também posteriormente, no menu Tools/Opções

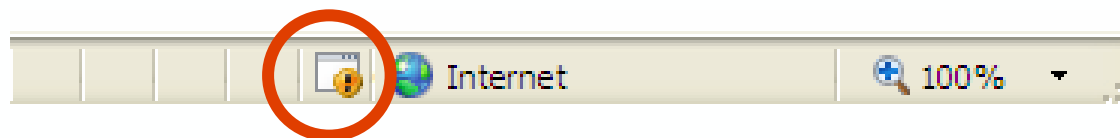


- O filtro de phishing identifica sites suspeitos (amarelo, com mensagem alerta) e sites conhecidos (vermelho, com página de alerta)
- Se o site for conhecido, o acesso é bloqueado



## Filtros de Phishing (IE7)

- O cliente pode sempre invocar manualmente a validação de um site, utilizando o ícone exibido na parte inferior da janela do browser



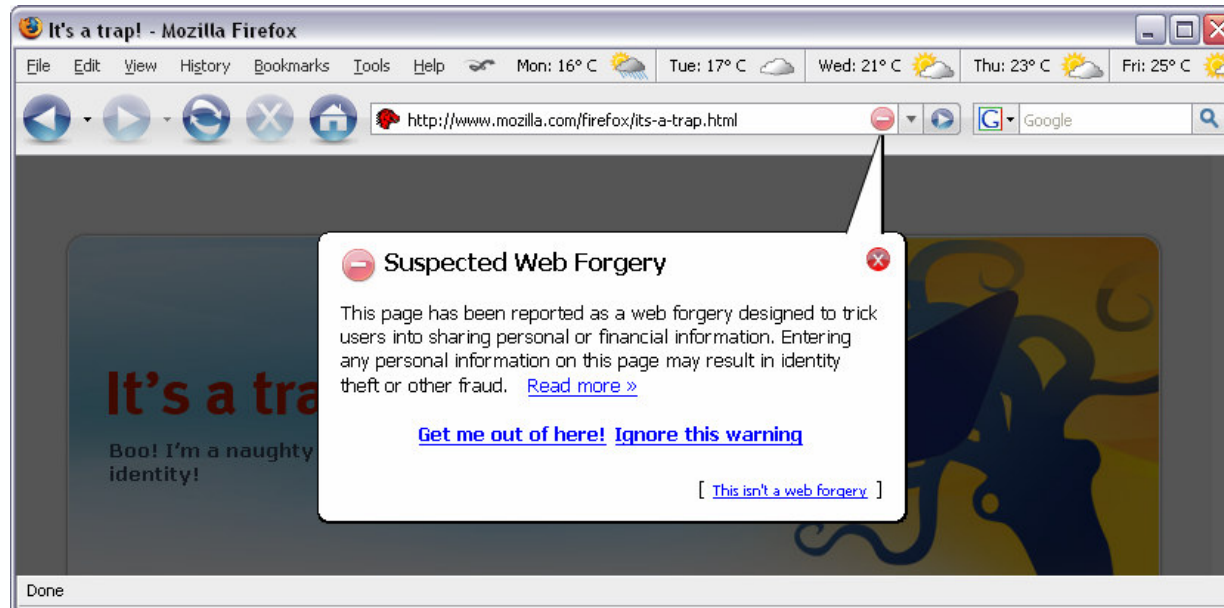
## Filtros de Phishing (Firefox 2)

- Potenciais sites de phishing são bloqueados por definição, mas o filtro pode ser configurado:
  - Tools > Options > Security



## Filtros de Phishing (Firefox 2)

- O filtro embutido no Firefox identifica os sites de phishing e emite um alerta para o cliente





## Links de Referência

- Wikipedia:
  - <http://pt.wikipedia.org/wiki/Phishing>
- AWPG:
  - <http://www.antiphishing.org>
- Microsoft:
  - <http://www.microsoft.com/protect/yourself/phishing/identify.mspix>
- Symantec:
  - [http://www.symantec.com/pt/br/norton/security\\_response/phishing.jsp](http://www.symantec.com/pt/br/norton/security_response/phishing.jsp)