Proteger o Dinheiro

Home banking
Conselhos aos Utilizadores

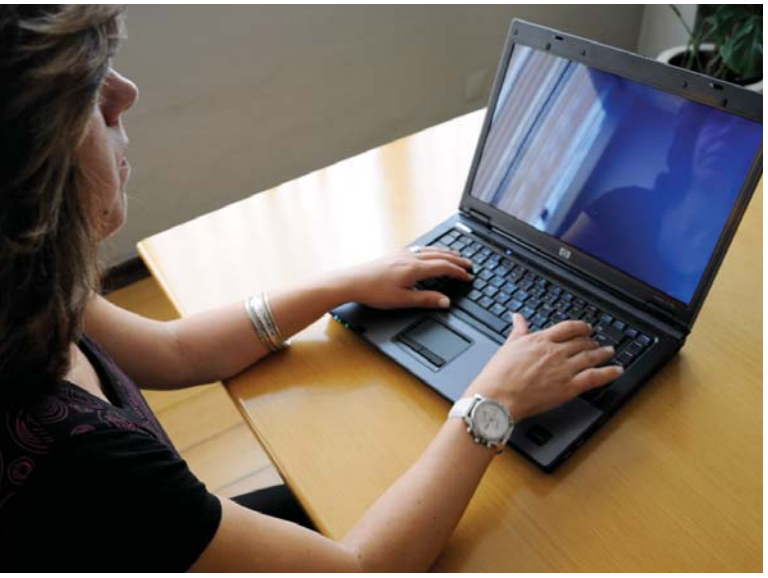
Francisco Luís*

Ir ao Banco a Qualquer Hora e em Qualquer Lugar. Mas com Precaução!

O termo *phishing* provém da palavra inglesa *fishing*, que significa pescar, fazendo alusão à tentativa de que as vítimas "mordam o anzol" e caiam no esquema.

Em termos genéricos, *phishing* é um método ilícito de capturar credenciais que ilude de tal forma o utilizador que o leva a revelar informação pessoal ou financeira (dados pessoais). Cibercriminosos enviam mensagens de correio electrónico aparentemente provenientes de instituições fidedignas, como é o caso das instituições bancárias, organismos públicos, forças de segurança, grandes operadores de comunicações, etc. Este tipo de mensagem apela a uma acção urgente por parte do utilizador, sob o risco de uma sanção, em regra de inibição do acesso às contas.

As mensagens de *phishing* são divulgadas massivamente (*spam*) e direccionam a vítima para páginas criadas pelos cibercriminosos, onde se é levado, de forma enganosa, a fornecer as credenciais ou a executar um *software* malicioso (*malware*). Caso o utilizador execute o *malware*, irá infectar o seu computador e, desta forma, o atacante poderá direccioná-lo para uma página muito idêntica à da instituição em causa ou capturar ilicitamente toda a informação digitada (*keylogging*) pelo mesmo.



Embora alguns ataques sejam grosseiros e fáceis de identificar, por utilização de expressões ou palavras pouco usadas ou inexistentes no nosso léxico, muitos são sofisticados e bem elaborados, fazendo uso de vulnerabilidades técnicas muito recentes e usando a imagem institucional do *site* legítimo.

Os criminosos vão sempre atrás do dinheiro. Se cada vez mais pessoas são clientes de sistemas de *home banking*, é aí que eles vão focar a sua atenção. Ainda para mais, a transnacionalidade desta actividade dificulta em muito a investigação destes ilícitos.

Os ataques de *phishing* e o *malware* usados são cada vez mais sofisticados e difíceis de detectar, mesmo para utilizadores alertados para a temática da segurança. Com a massificação do acesso à Internet, muitas pessoas estão pela primeira vez a ter contacto com sistemas de correio electrónico e *browsers* e, consequentemente, alguns utilizadores de sistemas de banca electrónica são ludibriados, fornecendo inadvertidamente os seus dados de acesso e autenticação desses sistemas em resposta a mensagens de *phishing*.

Proteger o seu Computador

A responsabilidade de proteger o computador é do seu utilizador e, como tal, o primeiro passo para manter o computador protegido requer o uso de *software* genuíno, realizando regularmente a actualização do sistema operativo e das aplicações usadas, nomeadamente do seu *browser*, no *site* do fabricante. Active a funcionalidade de actualizações automáticas, seguindo as recomendações ou documentação do fornecedor.

Copyright © 2011 by IFB/APB, Lisbon

"Os ataques de *phishing* e o *malware* usados são cada vez mais sofisticados e difíceis de detectar, mesmo para utilizadores alertados para a temática da segurança."

Para realizar actualizações, recorra sempre ao *site* do fabricante. Não siga *links* para *download* nem realize actualizações com base em pesquisas que realizou na Internet.

O uso de *software* antivírus ajuda a proteger o seu computador contra programas maliciosos. Deve instalar este tipo de aplicação e mantê-la actualizada numa base diária (actualizações automáticas são recomendadas). Ter um antivírus desactualizado é quase o mesmo que não ter antivírus. Não instale no seu computador *software* antivírus ou outros que tenham proveniência desconhecida, uma vez que pode estar a instalar uma aplicação falsa denominada *rogue security software* ou *scareware*.

Faça uma verificação regular do conteúdo dos dispositivos de armazenamento de dados do seu computador, fazendo uso do seu antivírus, com vista a detectar eventuais infecções por *software* malicioso.

Instale ou configure uma *firewall* pessoal. Esta aplicação visa impedir acessos remotos e não autorizados a dados ou recursos do seu computador quando está ligado à Internet.

Sem este tipo de protecção, o computador fica vulnerável a ataques.

A fim de evitar que as suas credenciais de acesso a um sistema de *home banking*, *webmail*, redes sociais ou outros sejam capturadas, evite a utilização de computadores e/ /ou redes públicas, nomeadamente redes *wireless* abertas e sem encriptação ou encriptação fraca, para aceder a estes serviços.

Importante reter:

- Usar *software* genuíno;
- Actualizar o *software* do seu computador com regularidade no *site* do fabricante;
- Instalar um antivírus e mantê-lo actualizado;
- Instalar uma *firewall*;
- Evitar a utilização de computadores públicos para aceder a serviços de *home banking*.

Como Detectar um Esquema de *Phishing*

Nenhuma instituição, nomeadamente um banco, solicita aos clientes a confirmação/validação das credenciais de acesso e/ou validação, seja em páginas na Internet, por correio electrónico, por SMS ou por outra qualquer forma.

Mensagens de correio electrónico que solicitam informações confidenciais devem ser vistas como potenciais ameaças. O utilizador deve abster-se de clicar em *links* que vêm com a mensagem ou de responder ao solicitado, podendo sempre entrar em contacto com a instituição através dos canais apropriados, da forma que costuma fazer habitualmente, a fim de aferir da veracidade do pedido.

Quando estiver a usar o seu sistema de *home banking*, e caso lhe seja exibida uma página para preencher números respeitantes a dados de validação de operações (algumas coordenadas ou a totalidade do cartão matriz), isso significa que o seu sistema informático foi comprometido. Aparentemente "está" no *site* do seu banco, mas, provavelmente, tal não corresponderá à verdade. Nunca deve fornecer dados de validação de operações a não ser que tenha efectivamente agendado ou realizado uma.

Se for vítima de uma situação idêntica, entre de imediato em contacto com o seu banco e solicite o cancelamento do seu contrato de adesão ao sistema de *home banking*, devendo o computador ser alvo de uma intervenção técnica a fim de eliminar o *software* malicioso que nele se encontra instalado.

Como medida de segurança adicional, altere a sua *password* regularmente. Não use *passwords* óbvias e tenha diferentes *passwords* para aceder a diferentes serviços como sistema de *home banking*, *webmail*, redes sociais ou outros. Não registe os seus códigos de acesso ou validação de forma a poderem ser consultados por terceiros (incluindo digitalização ou armazenamento no seu computador). Não deve enviar os códigos de acesso por correio electrónico.

Um utilizador deve ainda verificar regularmente as contas pessoais ou bancárias e comunicar qualquer alteração ou situação suspeita à entidade que administra a mesma.

Dê conhecimento às autoridades competentes para a investigação de processos deste tipo se for vítima de um esquema desta natureza. Preserve o computador a fim de serem recolhidas provas para o eventual processo-crime a ser instaurado.

As sessões de acesso a *sites* que envolvam autenticação devem sempre ser terminadas através da opção de sair (*logout* ou terminar sessão).

 Copyright © 2011 by IFB/APB, Lisbon

"Os bancos actualmente estão a migrar para sistemas de autenticação de dois factores que combinam algo que o utilizador sabe ... com algo que tem ..., a fim de verificarem e validarem uma identificação ou operação."

Importante reter:

- Os bancos **nunca** pedem informação sobre os dados de autenticação de um cliente;
- Nunca envie informação pessoal que lhe seja solicitada por e-mail ou em páginas Web;
- Não siga os *links* dos e-mails suspeitos;
- Aceda ao *site* digitando o endereço da instituição. Não use *links* dos favoritos ou resultados de pesquisa em motores de busca;
- Desconfie de e-mails impessoais;
- Em caso de dúvida, contacte a entidade para confirmar a veracidade da mensagem (nunca utilize contactos referidos na mensagem ou em páginas suspeitas);
- Certifique-se que o *site* é seguro (cadeado ao lado do endereço ou no canto inferior direito do *browser* ou pelo endereço, que deve começar por "https://");
- Active os filtros de *phishing* no seu *browser*;
- Altere a sua *password* regularmente.

E quando o *Phishing* É Bem Sucedido?

Quando o esquema de *phishing* é bem sucedido, os cibercriminosos têm a possibilidade de transferir dinheiro das contas das vítimas. Nesse caso, vão precisar de ter disponíveis contas bancárias para onde vão transferir montantes de forma ilegítima.

Estas contas são disponibilizadas por indivíduos recrutados através de empresas multinacionais fictícias que oferecem "empregos" bem remunerados, cuja função final é receber dinheiro transferido por alegados clientes da empresa e remetê-lo, a troco de uma comissão, para um país estrangeiro, onde a empresa diz ter sede ou representação, tipicamente um país de Leste.

Recomenda-se que não responda a ofertas de emprego desta natureza, ou seja, que envolvam a solicitação de preenchimento de *curriculum vitae* e que incluam a menção do número da conta bancária.

Qualquer pedido de cedência, empréstimo ou abertura de conta bancária solicitada por terceiros, em regra pertencentes a círculos de pessoas próximas ou conhecidas, para recepção de quantias monetárias, a troco de uma eventual comissão, pode levar o respectivo titular da conta a incorrer num crime, devendo, nestes casos, consultar o seu banco sobre a legitimidade da operação financeira em causa.

Em caso de qualquer dúvida, deve consultar o seu banco.

Importante reter:

- Nunca responda a ofertas de emprego deste tipo;
- Não ceda, empreste ou abra uma conta para receber quantias monetárias cuja proveniência desconhece;
- Nunca transfira dinheiro, por qualquer meio, para um destinatário que não conheça.

Sistemas de Autenticação Multi-Factor

Os bancos actualmente estão a migrar para sistemas de autenticação de dois factores que combinam algo que o utilizador sabe (como um *username* e uma *password*) com algo que tem (*smart card*, *token* ou telemóvel), a fim de verificarem e validarem uma identificação ou operação.

Uma das soluções adoptadas para o mercado bancário tem sido o denominado "SMS token" (mensagem enviada com um código que validará a operação cujos dados constam da SMS). Nestes casos, o utilizador deve sempre confirmar os dados da operação, nomeadamente a conta de destino e o montante. Não deve ainda fornecer, independentemente da forma de solicitação, algum código que tenha recebido e que não tenha tido origem numa operação por ele realizada naquele momento. Deve ainda comunicar à sua operadora de comunicações móveis alguma anomalia, como informação que o cartão GSM que está a usar não é válido na rede, uma vez que o mesmo poderá ter sido clonado ou emitida uma segunda via, de forma ilícita.

Existem outras soluções comerciais que poderiam igualmente ser adoptadas, como a virtualização da execução do *browser*, que acede exclusivamente ao sistema de *home banking*, para evitar alguns dos ataques mais comuns.

No entanto, independentemente das medidas tecnológicas adoptadas, o *phishing* é um fenómeno que "veio para ficar", pois o foco do ataque e as principais falhas estão do lado do utilizador. Assim, este deverá adoptar comportamentos que o protejam destas situações, seguindo na íntegra as recomendações da sua instituição bancária e as boas práticas de segurança. ■

*Inspector da Polícia Judiciária
Secção de Investigação de Criminalidade Informática e Tecnológica da Directoria de Lisboa e Vale do Tejo.

Copyright © 2011 by IFB/APB, Lisbon