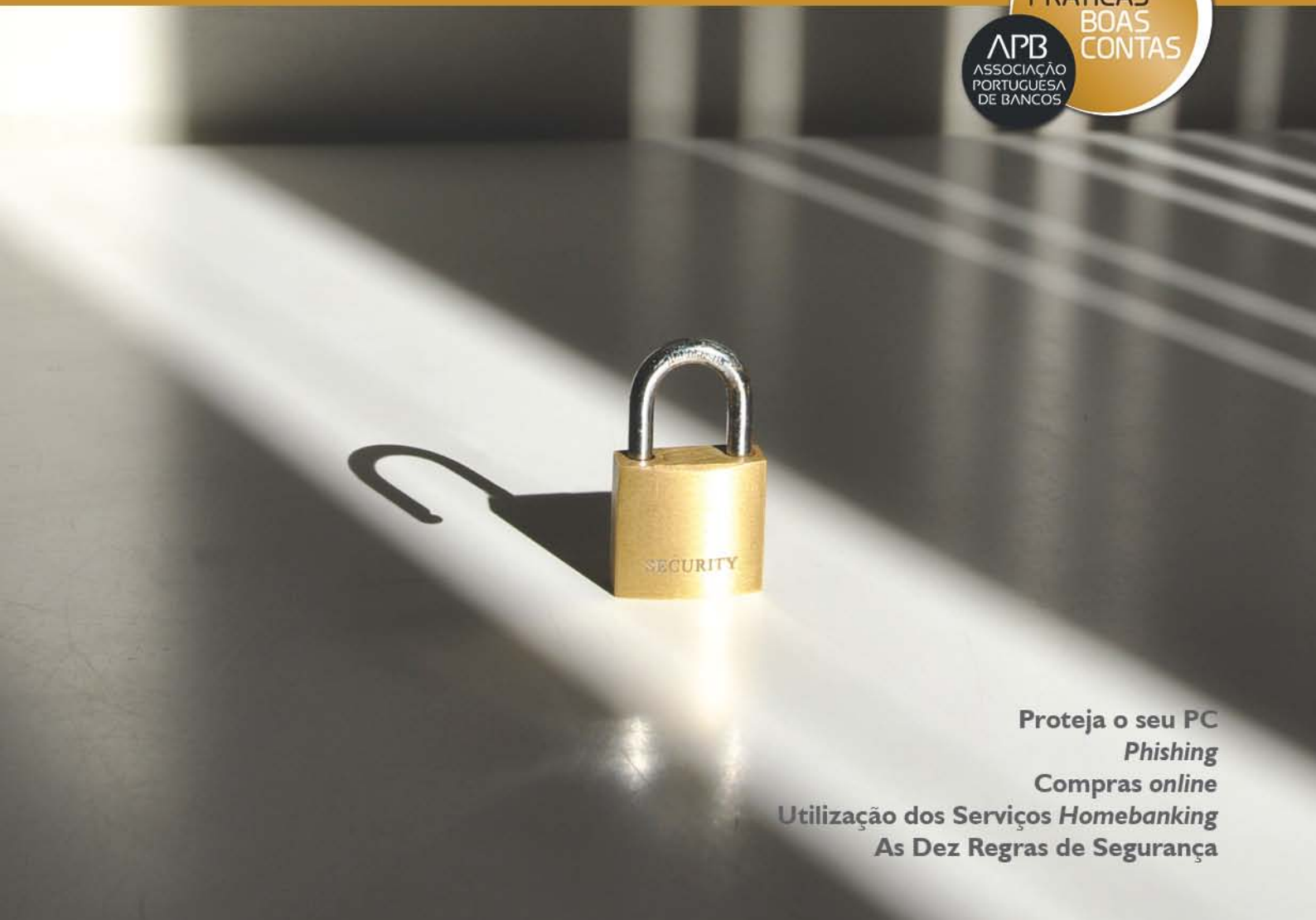
Banca e Internet
Prevenção

Algumas regras para uma utilização segura

BOAS PRÁTICAS BOAS CONTAS

APB ASSOCIAÇÃO PORTUGUESA DE BANCOS



Proteja o seu PC
Phishing
Compras *online*
Utilização dos Serviços *Homebanking*
As Dez Regras de Segurança

Índice

1. Proteja os equipamentos de acesso à internet

A segurança da sua informação, do computador, do *table*t ou *smartfhone* é fundamental e depende muito de si.

1.1 - Proteja o seu PC

O que deve fazer?

Manter o antivírus actualizado

Não manter o antivírus actualizado é quase o mesmo que não o ter! O antivírus protege o computador de ataques maliciosos verificando os programas que instala no computador ou os *e-mails* que recebe na sua caixa de correio.

O antivírus funciona como um protector solar que voltamos a colocar para reforçar a acção protectora.

Utilizar uma *firewall*

Trata-se de um programa, que vem normalmente incluído no sistema operativo dos computadores, permite reduzir o risco de acessos indesejados através de redes ou a partir do exterior por terceiros e/ou vírus. A *firewall* funciona como um chapéu-de-sol que o protege dos raios solares indesejados.

Realizar actualizações de segurança

Para corrigir falhas e vulnerabilidades detectadas nos programas, os fornecedores de *software* disponibilizam actualizações de segurança. Sempre que um fornecedor credível disponibilize actualizações, aplique-as de acordo com as instruções.

As actualizações são como as revisões da sua viatura. Antes de ir férias e sempre que recomendado deve levar a sua viatura à revisão.

Não responder a *e-mails* que não reconheça a origem e o assunto

Não responda a mensagens de correio electrónico de origem desconhecida nem seleccione links incluídos naquelas mensagens.

Não instalar programas

Não instale programas/*softwares* sem que garanta antecipadamente a fiabilidade da sua origem. Nem todos os programas são aquilo que afirmam ser e muitos vão apenas permitir a terceiros o acesso à sua informação.

1.2 - Proteja o seu *tablet* ou *smartphone*

Hoje em dia utiliza-se a internet não só para trabalhar, como também para ocupar os tempos livres e falar com os amigos. Por isso é cada vez é mais importante saber identificar os perigos e salvaguardar a segurança dos equipamentos do acesso por terceiros a dados e informações pessoais.

- **Nem tudo deve ser partilhado**. A utilização de computadores ou *smartphones* no acesso à internet deve ser efectuada de forma responsável, dando particular atenção à informação que se disponibiliza nas redes sociais.

- **Não identifique ou forneça dados pessoais** como o nome completo, moradas, números de telefones ou telemóvel e endereços de e-mail, em redes sociais ou páginas da internet que se apresentem em nome do seu banco;

- **Não confie cegamente nos outros utilizadores das redes sociais** que muitas vezes são simples utilizadores desconhecidos, ou podem ser amigos com contas comprometidas;

- **Tenha em atenção os jogos online** pois, por serem muito apreciados pelos mais novos, alguns deles não são mais do que uma via para obter *passwords* e informações pessoais.

Cuidados genéricos de utilização:

- **Dificulte o acesso ao seu *smartphone*** em caso de perda ou roubo, proteja-o com uma password de acesso. Estes equipamentos podem ser facilmente perdidos ou roubados;

- **Instale as aplicações apenas dos fornecedores confiáveis** (*App Store*, *Google Play*, *WindowsPhone Store*, *BlackBerry World*, *Nokia store*) e confirme sempre quais os níveis de permissão que são pedidos.

- **Defina limites e crie regras de utilização da Internet**. Por exemplo, implemente restrições de acesso de forma a impedir a instalação ou execução de programas que não sejam do seu conhecimento.

- **Instale um Antivírus para os *smartphones*.** Já existem soluções disponíveis para alguns tipos de *smartphones* sendo algumas gratuitas**;**

- **Actualize sempre o sistema operativo e as aplicações instaladas.** Caso não proceda às actualizações está a aumentar o risco de ataques virtuais ou instalação de aplicativos maliciosos;

- **Aceda apenas a Redes Wi-Fi conhecidas.**

- **Evite clicar em *links* ou fazer download** de aplicativos de fontes desconhecidas.

- **Evite ainda fazer clique em mensagens, imagens ou outros conteúdos publicitários de aspecto ou origem duvidosa.**

2. PHISHING

O que é?

Se recebeu uma mensagem de correio electrónico que não reconhece a origem nem o assunto da mesma, que contém *links* e/ou ficheiros em anexo e em cujo texto lhe são solicitadas informações de carácter privado e/ou confidencial, ou em que incluem ofertas de trabalho demasiadamente atractivas, DESCONFIE de imediato.

Alguém, provavelmente, o está a tentar enganar pelo que se deve precaver. Estará perante aquilo que se denomina, de uma forma geral, como *Phishing*.

Os ataques de *Phishing* têm evoluído rapidamente adaptando-se à realidade actual. Os mais recentes prendem-se, sobretudo, com programas maliciosos que se instalam quando acede a *links* ou abre anexos em emails.

Não se deixe "pescar". Para isso recomendamos que nestas situações:

- **não clique no *link***;

- **não forneça elementos** que lhe são solicitados e nunca abra o ficheiro que se encontra em anexo. Abrir o ficheiro poderá significar instalar um Vírus (código malicioso) e, por essa via, ficar com o seu computador comprometido que poderá ser utilizado futuramente para fins ilícitos por terceiros.

- **Não aceite ofertas de trabalho** que parecem excelentes oportunidades de ganhar dinheiro sem esforço. Normalmente o que é pedido aos "candidatos" é que tenham contas em Bancos nacionais para que sirvam de intermediários em transferências de dinheiro para países estrangeiros cuja origem é ilegal e lesa terceiros.

Como proteger-se destes ataques:

- **Nunca facultar a terceiros dados sensíveis**, como os seus **códigos** ou **outra informação** que permita o acesso às suas contas bancárias *online***.**

- Deve **instalar** no computador um **programa de antivírus**, mantendo-o actualizado. Não actualizar este programa é quase igual a não o ter;

- Ter uma *firewall* instalada permiti-lhe filtrar o tráfego que entra e sai do seu computador;

- O *software* instalado no seu computador, como por exemplo: sistema operativo e *browser* de acesso à Internet, devem também ser actualizados;

- Os Bancos **NUNCA** solicitam informações pessoais e/ou confidenciais através de mensagens de correio electrónico e SMS.

- O ambiente seguro no acesso ao site está sempre associado a um endereço que começa por https:// e a página possui um cadeado na barra inferior ou superior do seu *browser*.

3. Compras *online* com Segurança!

Efectuar compras pela Internet é um hábito cada vez mais comum entre os cibernautas e, se outro motivo não existisse, a simples comodidade do acto justifica a crescente adesão a este tipo de serviço.

Fazer as compras no conforto do lar permite-nos realizar uma análise mais detalhada e, por isso, uma compra mais adequada às nossas necessidades. Contudo, tal como fazemos numa loja ou num hipermercado, deveremos tomar algumas medidas para evitar surpresas desagradáveis.

Quando efectuar compras na Internet deverá ter em atenção o seguinte:

- Antes de efectuar a compra

Procure informações sobre a entidade na Internet - Para confirmar a veracidade da empresa pesquise-a pelo nome através de motores de busca;

- Obtenha referências de amigos e familiares que possam já ter efectuado compras junto dessa entidade ou pesquise, por exemplo, em fóruns de discussão, confirmando se existem reclamações sobre a empresa;
- Verifique o endereço físico do fornecedor, ou seja, se existem contactos de telefone, *e-mail*, fax, etc.;
- Tenha **cuidado com os sites** que apresentam apenas **contactos de telemóveis**;
- V**erifique que o contacto corresponde à entidade** em questão e qual a sua política de funcionamento.
- Confirme os procedimentos para **reclamação, devolução, garantia e outras** informações de protecção ao consumidor;
- **Verifique as medidas de segurança que o website adoptou para garantir a privacidade dos seus dados**, principalmente nos casos em que tenha de introduzir dados pessoais e/ou confidenciais;
- Verifique a **reputação do vendedor em websites** de leilões em que normalmente os valores dos produtos são mais baixos. Veja os comentários feitos por outros utilizadores e os produtos que este vendedor já vendeu/promoveu, e desconfie sempre que os valores estejam muito abaixo dos de mercado;

- **Verifique sempre que o website em questão utiliza SSL**, um certificado de segurança onde os dados enviados pelo seu computador até ao servidor da entidade são encriptados (codificados). Para efectuar esta verificação confirme que o endereço inicia com https:// em vez de http://.

- No acto da Compra

- **Não faculte** dados que não sejam essenciais à compra que está a realizar;
- **Desconfie** se lhe forem pedidos dados que nada tenham a ver com a compra em questão.
- **Guarde o comprovativo da** sua compra bem como o nome do site e a referência da mesma para que a possa indicar em caso de necessidade/reclamação;
- **Guarde *e-mails*** e/ou mensagens **que tenha trocado com o fornecedor** no âmbito da compra ou onde tenham sido discutidas as condições;
- **Confirme a existência de despesas adicionais** como taxas ou custos de envio, assim como os prazos de entrega ou de execução dos serviços adquiridos;
- **Exija facturas**, sempre que possível, para comprovar que o produto é fidedigno e não foi roubado. Este documento serve muitas vezes de garantia do produto, caso seja necessário a troca ou devolução por defeitos de fabrico, por exemplo;

- Pela sua Segurança

- **Desconfie** sempre que receber ***e-mails* que solicitem a confirmação dos seus dados sem motivo aparente ou por supostas verificações de segurança**.
- Não faculte os seus dados de registo a terceiros, mesmo que se apresentem como funcionários de entidades fidedignas;
- **Utilize *passwords* complexas**. Não utilize datas de nascimento ou outras referências pessoais já que essas são as primeiras que terceiros, com intenções maliciosas, tentam utilizar;
- **Não use computadores públicos** (como os cibercafés) para efectuar compras *online*, já que estes equipamentos podem estar infectados com vírus ou estar a ser alvo de vigilância por terceiros.

- **Se desconfia que o computador pode estar infectado com vírus não efectue compras *online*** já que ao realizar a transacção necessitará de introduzir dados confidenciais;
- **Evite as compras através de mensagens de *e-mail*** com promoções fantásticas. Tenha em atenção que os endereços ou anexos incluídos na mensagem podem levar a páginas falsas cujo objectivo é a obtenção dos seus dados pessoais e confidenciais (acções de *Phishing*).

- Pagamentos

- **Opte por meios seguros de pagamento** ao realizar as suas compras *online* como o pagamento à cobrança ou, por exemplo, o serviço Mbnet onde os dados do seu cartão nunca são facultados aos fornecedores.
- **Tenha especial atenção aos produtos mais procurados e valorizados nas vendas *online*** como, por exemplo, MP3, Consolas de Jogos, Telemóveis, entre outros. Estes produtos são os mais utilizados nas tentativas de fraude *online.*
- **Desconfie sempre de ofertas espectaculares**, promoções imperdíveis e valores muito abaixo do mercado, sobretudo em situações em que entidade não lhe seja familiar.

4. Utilização dos Serviços Homebanking

Consulte sempre os alertas de segurança para conhecer as últimas

Tentativas de Fraude

As instituições financeiras:

- ✓ NUNCA solicitam o número de telemóvel para aceder aos serviços *homebanking*;
- ✓ NUNCA enviam *e-mails*, SMS ou outras mensagens electrónicas a solicitar dados pessoais e confidenciais dos Clientes;
- ✓ NUNCA enviam *e-mails*, SMS ou outras mensagens electrónicas a solicitar o download de aplicações.
- ✓ NUNCA enviam por SMS actualizações para o seu telemóvel ou *Smartphone*.

Utilizadores – Boas Práticas

- ✓ NUNCA utilize ou aceda aos serviços *homebanking* através de links contidos em mensagens de *e-mail* ou SMS;
- ✓ Verifique se alguma parte do site não lhe parece autêntica, se a linguagem utilizada é adequada e se são solicitados os dados de acesso habituais;
- ✓ Verifique SEMPRE se a mensagem é personalizada (Exemplo: "Exmo. Senhor Pedro Alves") e não é enviada de forma geral (Exemplo: “Estimado Cliente” ou “Exmo. Senhor”);
- ✓ Utilize um antivírus e mantenha SEMPRE o seu sistema operativo e o seu *browser* actualizados.

5. As Dez Regras de Segurança

A protecção do seu computador depende de si!

Quando navega na Internet, deve estar atento a acções que têm como objectivo obter os seus dados ou informações pessoais, pelo que o acesso deve ser feito em segurança e com regras!

A internet para além de ser um espaço de verdadeiro entretenimento e lazer, é cada vez mais utlizada para aceder a websites bancários, sem necessidade de se deslocar a uma Sucursal/Agência.

No entanto, é muito importante ficar a salvo de vírus e outros programas maliciosos que possibilitam que terceiros obtenham códigos de acesso/*passwords*, sem que o utilizador tenha conhecimento.

Para que não tenha surpresas, disponibilizamos "dez regras" que podem ajudar a manter o acesso *online* seguro:

1. Nunca aceda a websites, através de *links,* com informação pessoal ou confidencial/sensível, ou que lhe permitem realizar operações bancárias. Digite sempre o endereço completo do site a que pretende aceder na respectiva barra;
2. Não utilize códigos de acesso/*passwords* óbvios (12345, 111111, data de nascimento, etc.) para o acesso a sites bancários. Periodicamente, deverá alterar os seus códigos;
3. Os Códigos de Acesso/*Passwords* são Pessoais e Intransmissíveis, pelo que não deverão ser transmitidos/disponibilizados a terceiros, nem mesmo, a outro(s) titular(es) da(s) conta(s);
4. Instale um antivírus e mantenha-o permanentemente actualizado. Não actualizar o antivírus é quase o mesmo que o não ter. Utilize uma *firewall* para que possa filtrar o tráfego da Internet que entra e sai do seu computador;
5. Esteja atento às actualizações de segurança que os fornecedores credíveis de *software* disponibilizam e aplique-as de acordo com as instruções que são fornecidas;
6. Os Bancos NUNCA solicitam informações pessoais e/ou confidenciais por contacto telefónico, mensagens de correio electrónico ou por SMS;

7. Sempre que aceder a websites bancários, verifique se o endereço se inicia por https:// e que, no final do endereço ou barra inferior da janela, se encontra um cadeado;
8. Esteja alerta para mensagens de correio electrónico com promessas de dinheiro fácil ou negócios que parecem demasiado aliciantes, estas ofertas podem ter o objectivo de utilizar a sua conta para fins ilícitos.
9. Caso duvide do conteúdo de uma mensagem de correio electrónico com uma oferta expressa, sugerimos que, utilize um motor de busca, pesquisando os dados da entidade (nome, morada, etc.). Muitas vezes estas já estão identificadas em websites ou blogues como entidades fraudulentas;
10. Contacte o seu banco caso verifique que os dados solicitados na página de acesso ao serviço *homebanking* foram alterados, sem comunicação prévia.

Associação Portuguesa de Bancos
Av. República, 35 – 5º, 1050-186 Lisboa
www.apb.pt
www.boaspraticaboascontas.pt