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*

Proteja o seu PC

A segurança da sua informação e do computador é fundamental e depende muito de si.

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 *emails* 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 *emails* 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.

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.

Comprar *online*? Sim, mas 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 site 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 sites** 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 site 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 *emails*** 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 ***emails* 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 *email*** 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.

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 *emails*, SMS ou outras mensagens electrónicas a solicitar dados pessoais e confidenciais dos Clientes;
- ✓ NUNCA enviam *emails*, 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 *email* 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.