RECOMENDAÇÕES DE SEGURANÇA

BFA Net / BFA Net Empresas/ APP

JANEIRO 2020

RECOMENDAÇÕES DE SEGURANÇA

UTILIZAÇÃO DOS SERVIÇOS HOMEBANKING

Conheça as regras de segurança que deve cumprir sempre que utilizar os Serviços de Homebanking:

CREDÊNCIAS DE ACESSO

De forma a proteger os seus dados pessoais, o acesso ao site BFA Net/ BFA Net Empresas deve ser sempre realizado digitando o endereço completo na barra de endereços do seu Browser:

Não aceda aos serviços de Homebanking através de:

- Links existentes em mensagens de e-mail;
- Resultados de pesquisas em motores de pesquisa (Google; Yahoo; Bing; Etc);
- Endereços gravados em Favoritos e/ou Histórico.

O acesso aos serviços de Homebanking por estas vias aumenta o risco de se deparar com páginas falsas, que têm como objectivo capturar informações pessoais e bancárias, para posterior utilização fraudulenta (credenciais de acesso, dados pessoais, confirmação de coordenadas ou informação sobre o telemóvel).

Suspeite sempre que lhe forem solicitadas informações para além das referidas, mesmo que pareça ser um e-mail ou uma página do BFA, ou se notar que a página tem um formato diferente do habitual.

RECOMENDAÇÕES DE SEGURANÇA

UTILIZAÇÃO DOS SERVIÇOS HOMEBANKING

Conheça as regras de segurança que deve cumprir sempre que utilizar os Serviços de Homebanking:

SEGURANÇA DO TELEMOVEL

Ao aceder ao BFA Net/BFA Net Empresas nunca lhe é solicitada a introdução de informações sobre o seu telemóvel. Suspeite sempre que se deparar com algum dos seguintes pedidos:

- Introdução do nº de telemóvel, fabricante/marca e modelo, sistema operativo;
- Download / instalação de software no seu telemóvel, sob qualquer pretexto.

O pedido de introdução destes elementos resulta na instalação de software malicioso no computador que utiliza para aceder ao BFA Net/BFA Net Empresas.

Suspeite sempre de mensagens não solicitadas recebidas por SMS, e não aceda aos links nelas contidos.

Sob o pretexto de activações ou actualizações de segurança, estes pedidos terão como objectivo a infecção do seu telemóvel com software malicioso para posterior uso fraudulento.

O BFA alerta que a introdução da informação sobre o telemóvel pessoal poderá comprometer a sua privacidade e segurança no acesso aos serviços de Homebanking

RECOMENDAÇÕES DE SEGURANÇA

UTILIZAÇÃO DOS SERVIÇOS HOMEBANKING

Conheça os cuidados a ter para garantir a segurança na utilização do e-mail.

BOAS PRATICAS NA UTILIZAÇÃO DO E-MAIL

Esteja atento a alguns sinais que poderão ajudá-lo a identificar um e-mail fraudulento. Estes e-mails:

- Utilizam normalmente expressões genéricas como "Caro Cliente" ou "Prezado Cliente" e não se dirigem aos destinatários pelo nome.
- Muitas vezes contêm erros de ortografia, erros gramaticais e até expressões que habitualmente não são utilizadas na comunicação em língua portuguesa.
- Em grande parte dos casos, são solicitadas informações:
  - Pessoais (números de BI, contribuinte, telemóvel);
  - Financeiras (números de contas, de cartões de débito e de crédito);
  - De acesso a sites diversos, nomeadamente sites bancários (chaves de acessos).

Saiba como se pode defender.

- Não abra, responda ou reencaminhe mensagens de correio electrónico não solicitadas ou sobre as quais tenha dúvidas, nomeadamente sobre a sua origem ou o seu conteúdo. Confirme com a entidade remetente a veracidade do e-mail.
- Nunca forneça dados pessoais e/ou financeiros em resposta a solicitações via e-mail.

RECOMENDAÇÕES DE SEGURANÇA

UTILIZAÇÃO DOS SERVIÇOS HOMEBANKING

Conheça os cuidados a ter para garantir a segurança na utilização do Computador e da Internet.

.

SEGURANÇA DO SEU COMPUTADOR E NA UTILIZAÇÃO DA INTERNET

Para proteger a sua privacidade e garantir a sua segurança na utilização dos serviços de Homebanking é importante garantir a segurança do computador, pelo que o BFA o aconselha a adoptar um conjunto de boas práticas:

- Mantenha actualizado o sistema operativo do seu computador;
- Mantenha cópias de segurança dos seus ficheiros mais importantes;
- Mantenha actualizado(s) o(s) browser(s) com que acede à internet;
- Nunca forneça dados pessoais e/ou confidenciais sem ter a certeza que se encontra num site seguro;
- Não utilize os Favoritos nem siga ligações (links) de outros sites, e-mails ou qualquer outro veículo. Aceda aos sites que pretende visitar introduzindo directamente o endereço na barra de endereços do browser.

RECOMENDAÇÕES DE SEGURANÇA

REGRAS DE SEGURANÇA

Para garantir que conhece e adopta medidas de protecção adequadas, o BFA destaca algumas Regras de Segurança para utilizadores da Internet e dos Serviços de Homebanking, que deverá ter sempre em atenção:

- Nunca envie informação pessoal que lhe seja solicitada por e-mail tal como: n.º do cartão de crédito/pré-pago/multicaixa, nº de adesão, código secreto, nomes, nº telefone;
- Não siga as ligações (links) de e-mails suspeitos. Caso queira aceder, introduza directamente no browser o endereço da entidade referida no e-mail e navegue a partir daí;
- Em caso de dúvida, contacte a entidade para confirmar a veracidade do email, mas nunca use os contactos indicados no e-mail;
- Desconfie de e-mails impessoais que se dizem de uma entidade com a qual mantém relações, seja um site de e-commerce ou uma instituição financeira. Normalmente os e-mails destas entidades dirigem-se ao Cliente pelo nome, como "Exmo. Sr. José Silva" e não por "Caro cliente".
- O objectivo dos e-mails fraudulentos é precisamente obter informação pessoal sobre si, pelo que é difícil conhecerem o seu nome de antemão.

RECOMENDAÇÕES DE SEGURANÇA

PHISHING

O Phishing consiste no tipo de fraude através da qual um pirata informático (hacker) tenta obter dados pessoais e financeiros de um utilizador, pela utilização combinada de meios técnicos e engenharia social.
A engenharia social consiste num conjunto de práticas que são utilizadas com o objectivo de persuadir o utilizador a realizar acções que favoreçam o atacante. Sendo este um ataque que é conduzido a nível psicológico, não há aplicativos que possam impedi-lo.

- Com base na engenharia social o phishing utiliza-se da confiança que os utilizadores têm nas organizações ou indivíduos genuínos para convencê-los a disponibilizar informações confidenciais ou efectuar instalação de softwares maliciosos. Os utilizadores acreditam estar a obter vantagens com tais acções quando na verdade estão a ser "pescados" numa fraude.
- O phishing ocorre por meio do envio de mensagens electrónicas que:
- Tentam fazer-se passar pela comunicação oficial de uma instituição conhecida, como um banco, uma empresa ou um site popular;
- Procuram atrair a atenção do utilizador, seja por curiosidade, por caridade ou pela possibilidade de obter alguma vantagem financeira;
- Tentam induzir o utilizador a fornecer dados pessoais e financeiros, por meio do acesso a páginas falsas, que tentam se passar pela página oficial da instituição;
- Tentam induzir o utilizador a instalar programas maliciosos, projectados para recolher informações confidenciais.

RECOMENDAÇÕES DE SEGURANÇA

PHISHING

Os e-mails de phishing apresentam características que, por norma, permitem diferenciá-los da comunicação oficial da entidade visada no e-mail. Assim ao receber um e-mail o BFA sugere sempre que:

- Verifique o endereço de e-mail do remetente. Habitualmente os e-mails de phishing são remetidos a partir de endereços de e-mail que não estão relacionados com a entidade visada no e-mail.
- Verificar se o e-mail lhe é dirigido (se está personalizado). Por norma os e-mails de phishing são enviados de forma massiva para os utilizadores da Internet que podem ou não ser utilizadores da instituição visada no e-mail. Assim e de forma a não levantar qualquer suspeita iniciam-se por expressões genéricas como por exemplo "Caro Cliente", "Prezado Cliente" ou "Caro Utilizador".

COMO PROTEGER-SE CONTRA E-MAILS DE PHISHING

- Nunca envie informação pessoal que lhe seja solicitada por e-mail tal como: n.º do cartão de crédito, username, password, nomes, informações sobre o telemóvel pessoal (Fabricante, Modelo, Nº Telemóvel);
- Não siga as ligações (links) de e-mails suspeitos. Caso queira aceder, introduza diretamente no browser o endereço da entidade referida no e-mail e navegue a partir daí;
- Desconfie de e-mails impessoais que se dizem de uma entidade com a qual mantém relações, seja um site de e-commerce ou uma instituição financeira. Normalmente os e-mails destas entidades dirigem-se ao Cliente pelo nome, como "Exmo. Sr. José Silva" e não por "Caro cliente".
- O objectivo dos e-mails fraudulentos é precisamente obter informação pessoal sobre si, pelo que é difícil conhecerem o seu nome de antemão.