RECOMENDAÇÕES DE SEGURANÇA

BFA Net / Net Empresas / APP

MARÇO 2019

DIRECÇÃO DE MARKETING

RECOMENDAÇÕES DE SEGURANÇA

ENQUADRAMENTO

As fraudes bancárias através de emails falsos continuam a afectar muitos clientes. Por isso, é importante passar a mensagem: **O BFA nunca utiliza o correio electrónico, nem qualquer outro meio, para solicitar dados pessoais dos clientes**. Os esquemas de phishing utilizam vários pretextos, mas o objectivo é sempre o mesmo: fazer com que o cliente introduza a sua chave de confirmação na totalidade.

Para garantir que se conhece e se adoptam medidas de protecção adequadas na utilização dos canais transaccionais BFA Net/BFA Net Empresas e APP, apresentamos 5 Regras de Segurança para utilizadores da Internet e dos Serviços de Homebanking:

- Regras de Segurança;
- Utilização dos Serviços Homebanking;
- Utilização do Email;
- Utilização do Computador e Internet;
- Phishing.

RECOMENDAÇÕES DE SEGURANÇA

REGRAS DE SEGURANÇA

O BFA destaca algumas Regras de Segurança para utilizadores da Internet e dos Serviços de Homebanking, que devemos ter sempre em atenção:

- Nunca enviar informação pessoal que 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 seguir as ligações (links) de e-mails suspeitos. Em caso de necessidade, introduzir directamente no browser o endereço da entidade referida no e-mail e navegue a partir daí;
- Em caso de dúvida, contactar a entidade para confirmar a veracidade do email, mas nunca usar os contactos indicados no e-mail;
- Desconfiar 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 , pelo que é difícil conhecerem o nome de antemão.

RECOMENDAÇÕES DE SEGURANÇA

UTILIZAÇÃO DOS SERVIÇOS HOMEBANKING

Regras de segurança a cumprir sempre que se utiliza os Serviços de Homebanking:

CREDÊNCIAS DE ACESSO

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

Não aceder 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 depararmo-nos 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).

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

RECOMENDAÇÕES DE SEGURANÇA

UTILIZAÇÃO DOS SERVIÇOS HOMEBANKING

Regras de segurança a cumprir sempre que se utiliza os Serviços de Homebanking:

SEGURANÇA NO TELEMÓVEL

No acesso ao BFA Net/BFA Net Empresas nunca é solicitada a introdução de informações sobre o telemóvel. Suspeitar sempre que nos deparamos com algum dos seguintes pedidos:

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

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

Suspeitar sempre de mensagens não solicitadas recebidas por SMS, e não aceder aos links nelas contidos.

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

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

RECOMENDAÇÕES DE SEGURANÇA

UTILIZAÇÃO DO E-MAIL

Cuidados a ter para garantir a segurança na utilização do e-mail.

BOAS PRÁTICAS NA UTILIZAÇÃO DO E-MAIL

Estar atento à alguns sinais que poderão ajudar na identificação de 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).

Como nos podemos defender.

- Não abrir, responder ou reencaminhar mensagens de correio electrónico não solicitadas ou sobre as quais existam dúvidas, nomeadamente sobre a sua origem ou o seu conteúdo. Confirmar com a entidade remetente a veracidade do e-mail.
- Nunca fornecer dados pessoais e/ou financeiros em resposta a solicitações via e-mail.

RECOMENDAÇÕES DE SEGURANÇA

UTILIZAÇÃO DO COMPUTADOR E INTERNET

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

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

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.

COMO PROTEGER-SE CONTRA E-MAILS DE PHISHING

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 passar-se 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 do BFA sugerimos sempre que:

COMO PROTEGER-SE CONTRA E-MAILS DE PHISHING

- 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 o email oficial BFA.
- 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".
- 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 directamente 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.

RECOMENDAÇÕES DE SEGURANÇA

PHISHING

EXEMPLO DE EMAIL FRAUDULENTO:

De: "bfa.net@bfanet.ao" <bfa.net@bfanet.ao> → Email falso e não oficial
Data: 25 de fevereiro de 2019, 1:14:29 PM GMT+1
Para: Undisclosed recipients:;
Assunto: Mensagem de atualização importante

Estimado cliente, → Não dirigido ao nome do cliente

Elogio da temporada.
Isto é para informar a todos os clientes que o Banco Nacional de Angola tornou obrigatório que todos os clientes do BFA actualizem o seu registo de conta noutro para regular as novas políticas bancárias e de sistema, conforme discutido na semana passada na reunião realizada em Luan → Erros de português

Como por nossos esforços para melhor atendê-lo, por favor, baixe e atualize o formulário anexado a este e-mail imediatamente. → Link para roubo de informação

É uma obrigação que você preencha seus detalhes corretos para evitar a suspensão.

Nota: A chave de confirmação deve ter 10 dígitos e estar correta. → Pedido de informação pessoal

Begard Regards.
Banco de Fomento Angola

OBRIGADO