SEGURANÇA E FRAUDE
Dicas de segurança

Como Evitar Phishing no Bai Directo: Proteja as Suas Transacções Online

A segurança das nossas transacções financeiras online é de extrema importância nos dias de hoje. O phishing é uma das principais ameaças que enfrentamos ao utilizar serviços de internet banking, como o BAI Directo. Neste blog, iremos discutir como evitar cair em golpes de phishing no BAI Directo e proteger as suas informações pessoais e financeiras.

O que é Phishing?

O phishing é uma forma de fraude online em que os criminosos se fazem passar por uma entidade legítima para obter informações confidenciais, como dados pessoais, números de cartão de crédito e outros dados sensíveis. Os golpistas geralmente utilizam e-mails, mensagens de texto ou até mesmo websites falsos para enganar os utilizadores e levá-los a fornecer essas informações.

Tipos de phishing:

Scam: Os golpes de phishing scam são golpes através dos quais os criminosos tentam induzir as pessoas a fornecer informações pessoais, como números de contas bancárias, credenciais de acesso aos sistemas e números de cartões de crédito, através da abertura de links ou arquivos contaminados.

Blind Phishing: É o mais comum de todos, disparado via e-mail em massa e sem muitas estratégias, que contam apenas com a "sorte" de que algum utilizador distraído caia na armadilha.

Spear phishing: É um ataque contra um grupo específico de utilizadores.
Estes, podem ser executados contra funcionários do governo, clientes de uma empresa específica ou até mesmo uma pessoa específica.

Clone phishing: Este golpe recria um site original para atrair os utilizadores. Geralmente, ao aceder o site falso, a pessoa visada tem que inserir informações num formulário malicioso que transmitirá as informações para os criminosos.

Smishing: É o nome para phishing realizado através de SMS. São mensagens que geralmente constrangem o utilizador como dívidas ou que impulsionam a tomar decisões imediatas pela emoção como sorteio, prêmios ou um valor alto a receber.

Vishing: A letra "p" foi substituída pela "v" porque o vishing utiliza mecanismos de voz para aplicar golpes muitas vezes por meio uma ligação directa para sua casa ou seu telemóvel.

Whaling: O termo vem da palavra whale (baleia, em inglês) e quer dizer caçar baleias. Isso significa que este golpe está ligado ao "tamanho do peixe a ser capturado" e tem como alvo executivos de alto nível de uma empresa.

Como Identificar um Website Falso

Uma das técnicas mais comuns usadas pelos golpistas é criar websites falsos que se assemelham ao Bai Directo ou ao website oficial do Banco BAI. Aqui estão algumas dicas para identificar esses websites falsos:

Verifique atentamente o endereço do website antes de inserir qualquer informação. O website oficial do BAI Directo é https://ib.bancobai.ao/ e o do Banco BAI é https://bancobai.ao/. Certifique-se de que a URL seja exactamente igual, pois pequenas diferenças podem indicar um website falso.

Exemplos de Websites Falsos:

https://baidirecto-angola.com/
https://bancobai-login.net/

Procure pelo símbolo de cadeado de segurança na barra de endereço do navegador. Isso indica que o website utiliza certificado SSL para proteger a comunicação e os dados transmitidos.

Analise o design e a qualidade do website. Websites falsos frequentemente apresentam erros de design, imagens desalinhadas e erros gramaticais. Esteja atento a esses sinais de baixa qualidade, pois podem indicar que está em um website falso.

Esteja alerta para solicitações de informações desnecessárias. o Banco BAI nunca solicitará informações confidenciais, como dados bancários adicionais ou informações pessoais não habituais. Desconfie se um website pedir tais informações.

Fique atento às mensagens:

Sobre ganhos loteria

Muitos atacantes enviam declarações de prêmios, viagens, smartphones e carros. Tudo vem de graça e de forma muito fácil.

Com sentido de urgência

O sentido de urgência é uma característica comum dos criminosos virtuais. Eles pedem que se aja rápido para criar o sentimento de urgência.

Com ameaças

Frases como "o seu serviço será suspenso se..." ou "sua conta foi bloqueada, clique aqui para verificar" são abordagens comuns de phishing. Mais uma vez, verifique directamente com a instituição em questão, seja banco ou órgão do governo (os mais usados), antes de tomar qualquer medida.

Exemplos de Websites Falsos em Nome do Banco BAI:

https://baidirecto-login-angola.com/
https://bai-acesso.net/
https://bancobai-pt.com/
https://ib-bai-directo-ao.com/
https://baidirecto-login.com/

Dicas para Evitar Phishing no BAI Directo

Além de identificar websites falsos, aqui estão algumas dicas importantes para evitar cair em golpes de phishing no BAI Directo:

- O Banco BAI não solicita informações confidenciais, como palavras-passe, por e-mail ou mensagem de texto. Portanto, nunca compartilhe essas informações por esses meios. Os criminosos frequentemente se fazem passar pelo banco para obter acesso às suas contas.

- Digite manualmente o endereço do BAI Directo no navegador. Em vez de clicar em links em e-mails ou mensagens, digite manualmente a URL do BAI Directo no navegador. Isso garante que esteja a aceder o website legítimo e não um falso.

- Mantenha-se actualizado sobre as últimas técnicas de phishing. Esteja ciente das tácticas mais recentes utilizadas pelos golpistas. Mantenha-se informado através de notícias sobre phishing e informações de segurança fornecidas pelo Banco BAI. Quanto mais informado estiver, melhor preparado estará para evitar golpes.

- Utilize soluções de segurança confiáveis. Mantém o seu computador e dispositivos móveis protegidos com software antivírus confiável e mantenha-o actualizado. Isso ajudará a identificar e bloquear possíveis ameaças de phishing.

- Desconfie de solicitações urgentes. Esteja atento a mensagens ou e-mails que exijam uma acção imediata. Os golpistas frequentemente usam a urgência como uma estratégia para pressionar as pessoas a fornecerem informações confidenciais sem pensar.

A segurança das suas transacções online é fundamental. Ao seguir as dicas mencionadas acima, você estará mais preparado para evitar golpes de phishing no BAI Directo. Lembre-se sempre de verificar cuidadosamente os websites, evite compartilhar informações confidenciais por e-mail ou mensagem e mantenha-se actualizado sobre as últimas técnicas de phishing. Com precaução e vigilância, é possível proteger as suas informações pessoais e financeiras ao utilizar o BAI Directo, a solução de internet banking do Banco BAI.