Recomendações de segurança para clientes

Senhas

A ActivTrades recomenda seus usuários a:

- Manter a confidencialidade de sua senha, não informando-a a terceiros e memorizando-a, evitando anotar a senha em papéis ou cartões;
- Alterar a senha sempre que houver suspeita do comprometimento da mesma;
- Usar senhas fortes, evitando sequencias facilmente presumíveis (data de nascimento, placa do carro, etc.).

Soluções contra Vírus e malwares

A ActivTrades recomenda seus usuários a:

- Manter solução de antivírus instalada e atualizada no computador utilizado para acesso dos serviços da ActivTrades;
- Utilizar somente sistemas operacionais e programas originais e de fontes confiáveis.

Prevenção de Fraudes em meio digital e engenharia social

As atuais práticas fraudulentas em geral possuem em alguma medida técnicas de engenharia social.

Para realizar a prática, primeiramente o criminoso obtém informações sobre a vítima, desde através de formas ilícitas (documentos furtados, vazamento de dados) e até por meio da observação em redes sociais (identificação dos nomes de cônjuges, parentes e amigos).

As informações que podem ser utilizadas para se praticar engenharia social são variadas e podem ser desde o simples endereço de e-mail (para envio de e-mail malicioso) até nomes completos de parentes ou dados de documentos.

De posse destas informações o criminoso comete a fraude induzindo a vítima em engano, fazendo se passar por familiar, amigo ou empresa com a qual a vítima possui relacionamento, como bancos ou lojas.

Abaixo se relaciona algumas das fraudes mais comuns com dicas de prevenção:

Pharming

O pharming acontece quando a vítima tem a sua navegação na internet redirecionada para sites falsos, que pode ter como consequência o vazamento de dados pessoais com possível perda financeira.

<u>Dicas de prevenção</u>

- Escolher um provedor de internet confiável;
- Verificar se há erros no endereço do site que se pretende acessar;
- Ao desconfiar de um site, inclusive de um banco, realizar login com uma senha errada. Como um site falso não tem como conferir a sua senha, a próxima tela mostrará que é golpe.

Phishing

O criminoso envia um link ou e-mail com vírus que direcionam as vítimas a sites falsos, em geral solicitando a atualização de dados juntos a instituições financeiras ou administradoras de cartão de crédito.

Dicas de prevenção

- Desconfiar de mensagens com conteúdo financeiro;
- Não acessar sites, links duvidosos ou e-mails suspeitos;
- Procurar o banco ou administradora do cartão de crédito para confirmar qualquer contato via mensagem de texto ou ligação telefônica;
- Manter o antivírus e firewall atualizados.

Ofertas e Boletos falsos

O criminoso consegue a informação de que a vítima paga determinada dívida através de boleto bancário e emite um falso com dados que não correspondem aos do real destinatário, mas de um falsário. O criminoso pode realizar a cobrança fraudulenta também através da oferta falsa de produto ou vantagem mediante pagamento.

Dicas de prevenção

- **A ActivTrades não emite cobranças nem recebe depósitos via boleto bancário;**
- **A ActivTrades não oferece empréstimos;**
- Sempre emitir os boletos no site oficial da empresa ou do banco que está fazendo a cobrança;
- Não acessar sites de recálculo de boleto atrasado, em geral são falsos;
- Não acessar links duvidosos ou e-mails suspeitos;
- Antes de efetuar o pagamento, verificar se os três primeiros números da sequência correspondem ao código do banco que emitiu o boleto;
- Conferir se os dados do beneficiário ou da pessoa que vai receber o dinheiro estão corretos;
- Verificar se o código de barras que fica na região superior do documento é idêntico ao que aparece na parte inferior.