Orientações Sobre Como Combater a Fraude

Sinais de alerta

Para e-mails, correspondências, ligações telefônicas, transações e sistemas de comunicação

Como saber se o e-mail, telefonema ou correspondência que você recebeu solicitando informações ou dando instruções para uma transação não são fraudulentos? Pegadinhas que utilizam a psicologia humana e outras táticas elaboradas de engenharia social são aliadas de peso na tentativa de cometer fraudes. Esteja atento: reconhecer falas e perguntas é a forma mais efetiva para combater as fraudes.

Percebeu algum desses sinais?

- Conversas alarmistas ou também exageradamente bajuladoras;
- Solicitações de transação abusivas ou agressivas;
- Mudanças no tom ou no comportamento usual do cliente;
- Sugestões de perda de dinheiro se você não agir;
- Mencionar funcionários de alta hierarquia para acelerar a transação;

- Erros gramaticais, de sintaxe ou ortográficos;
- Instruções falsas enviadas por e-mail, fax ou papel timbrado;
- Contatos ou detalhes que não coincidem com os do banco;
- Variações no endereço de email ou mudanças no nome do domínio;

- Ligação do cliente/fornecedor antes do seu retorno ser realizado;
- Mudanças no número habitual de retorno da ligação do cliente/fornecedor;
- O cliente/fornecedor raramente está disponível através dos canais oficiais;
- O cliente/fornecedor parece ansioso para realizar a transação;

- Os detalhes de contato do cliente/fornecedor não estão em arquivo;
- Fornecedores desconhecidos ou detalhes da transação alterados;
- Passos adicionais no acesso a sistemas ou transações;
- Instruções do sistema que "aparecem" misteriosamente.

Estão solicitando que você realize algumas destas ações?

- Receber ligações não solicitadas de contatos desconhecidos;
- Contatar supostos clientes em números não habituais;
- Fornecer uma senha em um lugar que você não conhece;
- Aceitar detalhes de contato inclusos ou não confirmados;
- Receber ou agir sob instruções não solicitadas;
- Clicar em links inesperados, desconhecidos ou falsos;

- Evitar procedimentos com razões convincentes;
- Tratar com um beneficiário pela primeira vez ou desconhecido;
- Oferecer informação de pagamentos SWIFT por e-mail;
- Realizar instruções depois de uma mudança de perfil;
- Realizar mudanças nos pagamentos de maneira imediata e urgente;
- Extrair quase todo o saldo da conta;

- Aprovar uma transação desconhecida ou pouco habitual;
- Transferir recursos por causa de, ou antes, de férias prolongadas;
- Transferir recursos a um conhecido em paraísos fiscais;
- Transferir uma pequena soma, seguida de uma grande soma, a um beneficiário;
- Transferir recursos a uma jurisdição alternativa;

O que fazer e o que não fazer?

Para dispositivos (smartphones, tablets, laptops e PCs)

Para adotar as práticas aqui recomendadas, você poderá ter a necessidade de envolvimento de seu departamento de TI. Isto pode exigir a realização de uma avaliação dos riscos, em conformidade com os próprios controles e avaliações da sua empresa.

O que se deve fazer...

- ✓ Utilizar software de antivírus, spyware ou malware que seja atualizado automaticamente;
- ✓ Instalar aplicativos ou software de fornecedores credenciados, nos quais você sabe que pode confiar;
- ✓ Habilitar o bloqueador de pop-ups do seu servidor, para evitar ataques de softwares maliciosos;
- ✓ Cada vez que terminar de usar o CitiDirect BE, encerrar a sessão e fechar o navegador;
- ✓ Manter seu plug-in de Java sempre atualizado, de modo que seu software seja executado sem problemas e tal como o esperado;
- ✓ Proteger com senhas qualquer dispositivo que você utiliza para acessar a plataforma CitiDirect BE;
- ✓ Suspeitar de toda ligação telefônica não solicitada de qualquer pessoa desconhecida;
- ✓ Desligar se tiver dúvidas sobre a mesma, depois ligue ou envie um email ao seu contato conhecido no Citi.

O que não se deve fazer...

- x Utilizar seu computador sem antivírus, anti-spyware ou software de detecção de malware;
- x Instalar aplicativos ou software de fontes ou companhias desconhecidas nas quais você não confia;
- x Utilizar tecnologia sem um bloqueador de pop-ups nativos ou de terceiros para defender-se contra malware;
- x Deixar a janela aberta de seu servidor, em dispositivos, depois de ter finalizado a sessão no CitiDirect BE;
- x Utilizar um dispositivo ou computador sem a versão mais atualizada ou recente do plug-in de Java;
- x Acessar o CitiDirect BE em qualquer dispositivo ou tecnologia que não estiver protegida por senha;
- x Compartilhar sua senha com qualquer pessoa (o Citi não lhe pedirá que compartilhe esta informação);
- x Clicar em qualquer link suspeito em um e-mail;
- x Compartilhar telas de PC com pessoas não autorizadas.

Riscos e controles

Para solicitações de modificações por parte dos beneficiários

Reconhecer o problema é fundamental para aplicar as melhores soluções. Estes conselhos, quando aplicados juntamente com seus próprios processos de controle interno, reduzirão os riscos associados à modificação dos detalhes de pagamento de beneficiários.

Os problemas com os fraudadores são que eles...

- Operam em todos os mercados, setores e regiões;
- Trabalham de maneira criativa e sofisticada;
- Realizam tentativas para redirecionar pagamentos;
- Procuram modificar os detalhes bancários dos beneficiários;
- Esperam que você aceite logotipos falsificados;
- Tentam avisá-lo de novas modificações bancárias;
- Tentam se passar por novos gerentes de conta/técnicos do banco;
- Hackeiam contas de emails de pessoal sênior para solicitar um pagamento.

As maneiras de reduzir o risco de fraude são...

- Criar seu próprio perfil de cliente/fornecedor/pagador;
- Validar de modo independente todas as solicitações de alteração que receber;
- Confirmar acordos por escrito com contatos conhecidos;
- Nunca tratar com acordos de solicitantes desconhecidos;
- Validar somente através de canais e contatos aprovados;
- Certificar-se de que os procedimentos de pagamento do beneficiário sejam robustos;
- Estar sempre atento a solicitações não usuais ou que contenham sinais de alerta.

As melhores práticas

Ações para proteger sua organização

- **EXECUTAR** controles para reduzir o risco de fraude.
  - » Valide instruções de pagamento para qualquer contraparte nova, e a mesma autenticação deve ser aplicada a qualquer solicitação de alteração seguinte recebida;
- **GERENCIAR** transações de alto valor e risco
  - » Estabeleça níveis de aprovação adicionais no processo de feito/conferido no CitiDirect BE;
- **REDUZIR** o risco de transação em todo o negócio.
  - » Separe as obrigações das atividades sensíveis ou de alto risco;
- **COMPREENDER** melhor a engenharia social.
  - » Promova treinamentos sobre as ameaças cibernéticas/fraudes;
- **VERIFICAR** a atividade dos usuários
  - » Revise periodicamente os relatórios de transações e realize auditorias frequentes nos usuários;
- Complete a capacitação sobre a "Consciência de Fraude de Engenharia Social" do Citi em **http://www.citibank.com/tts/sa/emea_marketing/training/index.html**

SE VOCÊ FOR VÍTIMA DE UM ATAQUE, ENTRE EM CONTATO COM SEU ADMINISTRADOR DE USUÁRIOS E SEU CONTATO NO CITI.
O CITI POSSUI UM SERVIÇO DE INVESTIGAÇÃO DE FRAUDE QUE ESTÁ COMPLETAMENTE CAPACITADO PARA INVESTIGAR E TRATAR ATAQUES DE FRAUDE.

1461600 08/16