Treasury and Trade Solutions

As Melhores Práticas de Segurança no CitiDirect BE℠

No Citi, a segurança de nossos clientes é muito importante. Nesse sentido, já que existem indivíduos que continuam tentando obter acesso não autorizado à informação, gostaríamos de destacar algumas das melhores práticas recomendadas para seu uso, ajudando a garantir que você esteja seguro.

Para manter o mais alto nível de segurança, é essencial que seus controles sejam periodicamente revisados:

- O CitiDirect BE contém até nove níveis de aprovação. Recomenda-se fortemente que sua organização configure um ou mais níveis de aprovação;
- Garanta que as transações de alto risco ou de alto valor passem pela maior quantidade de processos de aprovação;
- Aproveite a funcionalidade de pré-formato do CitiDirect BE para garantir que você esteja pagando beneficiários conhecidos ou pré-aprovados;
- Supervisione a atividade de contas de alto risco, tais como tentativas de modificar os detalhes da conta bancária do beneficiário. Estas tentativas fraudulentas, quando bem-sucedidas, podem resultar na perda de recursos.

Se for necessário ajuda para implementar as práticas anteriormente mencionadas, utilize o módulo de capacitação do *"Client Academy"* ou entre em contato com o seu representante de Serviço ao Cliente do Citi.

Tenha cuidado com os ataques de Engenharia Social

A Engenharia Social envolve a atuação de criminosos que obtêm acesso não autorizado às informações e/ou contas, através da manipulação e do engano dos usuários.

O objetivo da Engenharia Social é permitir que um usuário não autorizado cometa fraude, espionagem industrial ou roubo de identidade ou que, simplesmente, entre à força a uma rede para poder modificar os sistemas e aplicativos.

Em vez de hackear sistemas, os engenheiros sociais tentam obter informações por meio de golpes aos usuários. Para isso, se utilizam da psicologia como forma de conseguir o que desejam, tais como, o desejo de ajudar, a tendência de confiar nas pessoas e o medo de arriscar. Os engenheiros sociais utilizam uma série de métodos para enganar os usuários, o que torna essencial que você tenha ciência dos mesmos.

O Citi recebeu relatórios de inteligência empresarial advertindo que houve alguns incidentes onde os engenheiros sociais se fizeram passar por funcionários do banco, representantes da área de atendimento ao cliente. **Por favor, tenha em mente que o Citi jamais liga para os clientes solicitando seus dados de acesso ao internet banking, incluindo os dados de identificação pessoal (login), senhas ou qualquer outra informação de segurança desse tipo.** Se você receber qualquer ligação suspeita (não solicitada ou inesperada, na qual a pessoa que liga solicita informação), por favor, entre imediatamente em contato com seu Usuário Master ou com a área de Serviço ao Cliente do Citi.

Aproveite o CitiDirect BE℠ Mobile

Você pode utilizar o CitiDirect BE Mobile para aprovar pagamentos e acompanhar seus saldos diários, quando não estiver no escritório. Alertas também podem ser configurados para transações de valor elevado ou quando os limites de saldo são atingidos.

Nunca compartilhe seu Token

O Token não deve ser compartilhado. Compartilha-lo aumenta o risco de fraude. O mecanismo de segurança do CitiDirect BE foi estabelecido para diferenciar a pessoa que inclui uma transação e o autorizador da mesma. Caso os tokens sejam compartilhados, torna-se mais fácil que um indivíduo crie e aprove uma transação.

Mantenha sua Senha de Acesso em Sigilo

Do mesmo modo que ocorre com o Token, é muito importante manter sua senha de acesso em sigilo. Sua senha é a primeira linha de defesa contra alguém que esteja utilizando seu token para acessar ou para autorizar uma transação em seu nome. Trate sua senha da mesma maneira que trataria a senha da sua própria conta bancária, e não a guarde em uma localização visível. Saiba que a senha do seu token pode ser alterada, e o Citi recomenda que os usuários modifiquem a mesma periodicamente.

Exclua ex-funcionários

Garanta que, quando um funcionário deixar a empresa ou mudar de posição, seu perfil seja atualizado no sistema e seu token excluído. É importante que os tokens não sejam novamente atribuídos a novos usuários. Também leve em consideração que os perfis dos usuários podem ser programados para expirar automaticamente, garantindo que esses tokens não sejam usados de modo inadequado.

Revisão de perfis de acesso

Execute revisões periódicas de usuários e perfis no sistema, para garantir que o acesso seja atualizado e alinhado com a segregação de funções. Recomenda-se fortemente que as atividades de gerenciamento de usuários, inclusão de transações, autorização e controle não sejam realizados pela mesma pessoa. Garanta que o usuário do CitiDirect tenha recebido tanto seu token, como sua senha de acesso, antes de habilitá-lo no sistema. Os usuários que estiverem fora do escritório por períodos prolongados (por exemplo, férias, licenças estendidas, etc.) devem estar desabilitados até que voltem ao escritório.

Outras Dicas

Você pode configurar a opção de "Entrega Automatizada de Arquivos e Relatórios" (AFRD) para receber os mesmos diariamente e poder gerenciar a inclusão de transações.

As melhores práticas no seu PC

- Instale somente aplicativos e software de companhias reconhecidas nos quais você confie;
- Instale software de antivírus, anti-spyware e de detecção de malware – uma maneira de defender-se contra os ataques ao seu computador é utilizar software preventivo. É necessário atualizar os softwares periodicamente, para proteger-se contra novos riscos, assim é recomendável configurar o software para ser atualizado de forma automática;
- Utilize um bloqueador de pop-ups – configure as preferências de seu navegador para que bloqueie pop-ups. Além de incomodar os usuários, esses pop-ups podem conter conteúdos inapropriados ou com intenções maliciosas;
- Feche a sessão de internet – certifique-se de fechar a sessão de internet e de sair do navegador, ou de fechar a janela do seu navegador sempre que terminar de utilizar o CitiDirect BE;
- Atualize – mantenha seu navegador e o plug-in de Java atualizados em suas versões mais recentes;
- Proteja-se com uma senha – Certifique-se de que seus dispositivos (computadores pessoais, desktops, laptops, etc.) utilizados para acessar o CitiDirect BE estejam protegidos por uma senha.

Além disso, é provável que você precise de seu departamento de TI para assessorá-lo com as melhores práticas em relação ao seu PC e que realizem avaliações periódicas em relação aos riscos.

Entre imediatamente em contato com seu representante do Citi, caso note alguma atividade suspeita na sua conta, experimente incidentes relacionados com a segurança da informação, ou se tiver alguma dúvida sobre a segurança no Citi.

1461607 GTS26303 08/16