

Monitoramento e Análise de Canais Eletrônicos em Tempo Real.

INTRODUÇÃO

O Internet Bank e outros canais eletrônicos têm crescido rapidamente no Brasil e no mundo. O Internet Bank em grandes bancos já atinge quase 40% das transações totais, os canais eletrônicos outros 40%, sobrando para as agências tradicionais 20% do movimento.

O assalto a banco tem seguido essa tendência, deslocando-se dos assaltos à mão armada para a muito menos arriscada fraude dos canais eletrônicos, pura e simples.

Não tão simples assim, mas ao alcance daqueles que saibam como explorar as vulnerabilidades desses canais e a ingenuidade das pessoas.

Com a tecnologia passou a ser possível fraudar clientes e bancos em escala industrial. Usando uma mistura de tecnologia e de **Engenharia Social** ⁽¹⁾.

A primeira fase de qualquer fraude é a identificação da vítima, isto é o Banco e o Cliente (a ordem não importa), o que é facilitado pela técnica do **Phishing**, que envolve o envio de centenas de milhares de e-mails (**Spam**) bastante credíveis, seduzindo ou ameaçando os clientes do Banco e pedindo para o cliente atualizar seus dados, “... com a aquisição pelo Banco XYZ do seu novo sistema de segurança que visa coibir fraudes pela internet e evitando que a sua conta seja bloqueada...” “click no link a seguir, vá para o nosso site, e siga as instruções”.

Sedução “... novo sistema de segurança...” e **ameaça** “... a sua conta bloqueada...”, os clientes, na melhor boa fé, clicam no link e caem em um site clone do banco, em que devem informar a sua conta, senha, cartão de débito, data de nascimento, nome da mãe e palavras secretas, etc. ou recebem um **Spyware** ⁽²⁾ que vai enviar para a quadrilha boa parte do que o cliente realiza em seu computador, inclusive senhas.

O esquema para ser bem feito, direciona o cliente para o real site do Banco, através da técnica do **Cross Site Scripting** ⁽³⁾.

De posse dos dados do cliente, fica fácil fazer uma transferência, TED ou DOC para a conta de um laranja.

Alguns esquemas sofisticam a fraude pagando Boletos de Cobrança de Condôminos, Escolas, etc. reais, mas cujas contas no código do Boleto não são as reais das empresas, mas contas de laranjas.

As variações sobre o mesmo tema são inúmeras e só dependem da criatividade dos fraudadores.

Resumindo, a tecnologia empregada passa por **Spam**, **Spyware**, **Cross Site Scripting**, etc. e por boa dose de **Engenharia Social**, em que valem a lábria, a sedução e as ameaças.

Várias medidas podem ser tomadas, appliances e softwares anti-spam, anti-spyware, Firewalls de Aplicação, etc. para proteger o site do banco, mas a melhor maneira de proteger o Banco e seu site é conhecer o comportamento (perfil) de cada cliente e analisar em Tempo Real as suas transações, procurando indícios de anomalia.

Comportamentos e padrões permitem identificar essas transações anômalas em clientes, empregados, canais, pontos de compromisso e contas suspeitas.

A capacidade de entender o comportamento dos clientes, canais, parceiros e empregados e rapidamente investigar quando os mesmos são mudados, é uma importante linha de defesa para Instituições Financeiras.

O **Monitor Internet Plus – Electronic Channel Edition** é um sistema altamente eficaz de detecção em Tempo Real de **transações anômalas**, com um sofisticado sistema de alertas e que pode ser utilizado, em outras versões, para detecção de Lavagem de Dinheiro, Fraudes e Erros, podendo ser



utilizado pelas áreas de Auditoria, Inspeção, Controles Internos, Cash Management e outras em que transações anômalas possam causar prejuízo ao Banco ou a seus clientes.

O **Monitor Internet Plus** passou em testes de laboratório para até 3,3 mil transações por segundo e sete milhões de transações por dia em cliente real.

Através da parametrização adequada, o **Monitor Internet Plus** pode alertar, investigar, armazenar dados, executar workflows e fazer relatórios, por exemplo, sobre os seguintes eventos:

- Desvios significativos e injustificados no comportamento histórico de cada cliente;
- Aumentos consideráveis no volume movimentado, especialmente em transferências feitas em um curto espaço de tempo;
- Pagamento de boletos bancários “novos”, nunca antes acontecidos;
- Compra de “traveler Checks”, ou transferências com grandes montantes em espécie, sem uma lógica aparente;
- Movimentos de dinheiro para locais geograficamente suspeitos;
- Somatória da movimentação de um cliente, em varias contas, mostrando uma disparidade entre sua capacidade econômica e a movimentação financeira;
- Movimentações “abruptas” em contas historicamente inativas;
- Fluxo financeiro incompatível com os dados cadastrais do cliente;
- Uso atípico de linhas de crédito automáticas;
- Cancelamento ou antecipação de liquidação de contratos de empréstimo, CDC, Leasing, CDBs.

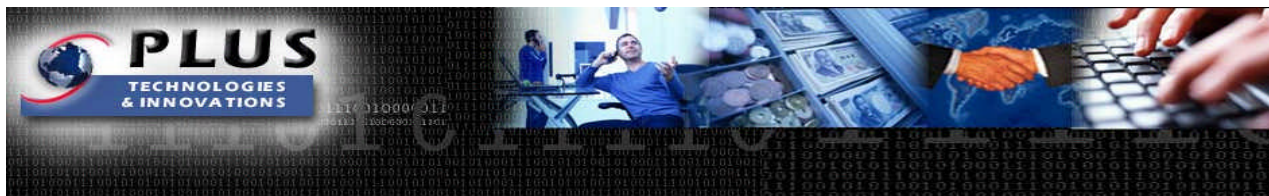
Estes são apenas alguns dos controles que cada instituição financeira tem a liberdade de definir para seu próprio uso e defesa.

De modo geral, o **Monitor Internet Plus** é uma solução de software que já trata de atividades de controle de Fraude e Lavagem de Dinheiro em mais de 60 instituições financeiras, em vários países.

A PlusTI tem larga experiência nas diversas formas de fraude bancária, de cartões de crédito e cartões de débito em diversos países das três Américas, conhecendo mais de uma centena de casos diferentes de fraudes.

Através do treinamento fornecido pela PlusTI as áreas de “controle de fraudes”, “reação a incidentes” e o “call center” ficam aptas a utilizar-se plenamente das capacidades do Monitor Plus.





RESUMO EXECUTIVO

Funcionalidades que diferenciam o **Monitor Plus**

- **Módulo Tempo Real (Modulo Interativo)**
 - **Análise e Alerta** de Transações em **Tempo Real** – Uma “cópia” de cada transação realizada no Internet Bank ou em outros canais eletrônicos deve ser enviada ao **Monitor Internet Plus** que efetuará a análise da transação em função do contexto, comportamento do cliente e das regras de negócio pré-estabelecidas, que poderá enviar um Alerta a uma ou várias pessoas da organização.
 - Análise, **Bloqueio** e Alerta de Transações em **Tempo Real** – Cada transação iniciada no Canal é interceptada, analisada pelo **Monitor Plus**, liberada ou bloqueada automaticamente ou transferida para decisão por operador humano (Call Center, Gerente da Conta, Grupo de Resposta Imediata, etc.). É necessário o **Módulo Monitor Interativo** e algumas modificações no Internet Bank ou em outros sistemas.
 - **Análise** de Transações ou **Cientes** em Tempo Real – Um usuário, com os poderes adequados, pode inquirir o Data Warehouse do **Monitor Internet Plus** sobre operações, clientes, convênios pagos, beneficiários e em segundos obter respostas satisfatórias. É necessário o **Módulo Datawarehouse**.
- **Módulo Workflow**
 - O Workflow é uma importante ferramenta de compliance, que pode controlar desde a investigação de casos de Lavagem de Dinheiro, Fraudes, Erros, até os processos, melhorando a aderência da empresa às suas normas internas, normas do Banco Central e à legislação.
 - Como o Monitor está integrado às operações do Internet Bank, o Workflow permite controlar a velocidade e as decisões do Grupo de Resposta a Incidentes, do Call Center, do Gerente da Conta, podendo enviar as requisições em paralelo e escalar rapidamente no caso de atrasos na decisão.
 - Permite controlar a produtividade e o tempo de resposta dos Investigadores, alimentando e controlando automaticamente as filas de transações a serem investigadas.
 - É bastante flexível, com um número ilimitado de nós (instancias), possibilidades de ser programado no tempo e aceitar paralelismos quando necessário.
- **Módulo de Alertas**
 - É um módulo bastante completo, que envia alertas através de
 - Telas das estações de trabalho (para o Call Center, por exemplo)
 - E-Mail, através de servidores SMTP (Gerente de Conta)
 - Telefones, através de uma URA - Unidade de Resposta Audível
 - SMS (Mensagens de Celulares), Pagers ou Bips
 - Impressoras conectadas diretamente à rede
 - Os usuários receptores de alerta, podem, em função dos poderes outorgados, aprovar operações na hora e pelo meio em que receberam o alerta. Podem autorizar pelo celular, por telefone, por e-mail, pela tela da estação, etc.



- **Módulo Data Warehouse**
 - O Data Warehouse armazena dados sobre transações e clientes. Permite a execução de análises instantâneas sobre essas operações ou clientes;
 - Armazena o comportamento identificado (perfil) de cada cliente; de cada canal (Caixas Eletrônicos, etc.); de cada empregado, etc.
- **Ambiente de Autorização**
 - Com o Módulo Interativo (Tempo Real), o Modulo de Alertas e o Módulo WorkFlow, o Banco passa a dispor de um completo **Ambiente de Autorização** , capaz de monitorar e bloquear as transações em Tempo Real, submetendo-as a uma **instancia superior** para autorização via sistema, e-mail, telefone, celular, SMS, Pager, etc.
- **Ambiente de Investigação**
 - Com o Módulo Data Warehouse e o Módulo WorkFlow o Banco passa a automatizar e aumentar a eficácia das investigações de operações suspeitas.
 - O Monitor Internet Plus pode enviar por e-mail, formulários HTML ou PDF para o Cliente, Gerente de Contas, Gerente da Agencia, solicitando informações sobre determinada operação feita pelo cliente. Estas solicitações tem prazo de resposta esperado e ao fim deste prazo, sem receber a resposta, o Monitor pode escalar a demanda para o superior hierárquico, conforme definido no WorkFlow. Em paralelo pode enviar copia da demanda ao Responsável por Lavagem de Dinheiro, à Inspeção, ou a qualquer área definida no WorkFlow.
 - O Data Warehouse possibilita aos investigadores terem todas as informações necessárias, em Tempo Real, sobre o cliente, sobre a agencia, sobre o caixa, sobre o canal utilizado, para tomarem as decisões adequadas, registrando os resultados no próprio Data Warehouse.
- **Ambiente de Controle do Risco Operacional (Basiléia II)**
 - Com o monitoramento contínuo das transações, o Monitor pode localizar Pontos de Compromisso, identificar transações com erros, transações suspeitas, resultados de Investigação e armazena-las no Data Warehouse para uso futuro e comprovação junto ao Banco Central e outra autoridade de Tutela.
- **Ambiente de Suporte a Línguas Nacionais**
 - O Monitor suporta atualmente Inglês e Espanhol e está previsto o Português (do Brasil).
 - Com esse ambiente é possível enviar **o mesmo alerta, em diferentes idiomas para diferentes destinatários** (e-mail, Pager, telefone, celular, etc.)

Distribuidor Exclusivo no Brasil

CLM

Distribuidor Exclusivo das mais Avançadas Tecnologias

11-21CLMCLM

clm@clm.com.br

WWW.CLM.COM.BR

