Compugraf
Soluções Avançadas para Comunicação Empresarial

É possível pagar contas pela internet com segurança?

O Tony Silva é uma pessoa comum nascida nos anos 80. Ele tem boa formação e emprego fixo como Gerente Administrativo de uma multinacional de bebidas. Tony viu o início da era digital e está usufruindo muito bem dela – tem cartão de crédito, conta bancária e, como todas as pessoas, muitas contas para pagar.

Ele se adaptou muito bem às novas tecnologias. Quase não pega filas nos bancos, resolve tudo pela internet usando seu computador ou smartphone. Normalmente resolve essas questões antes de começar o seu expediente. Sempre que as contas estão prestes a vencer, acessa seu internet *banking* e paga, em poucos minutos, os boletos, contas de serviços e assinaturas . Nada de perder tempo nas filas, trânsito ou transporte público.

Tony era uma pessoa feliz até 8 de maio de 2015. Naquela manhã ele observou que algo errado acontecera. Ao acessar sua conta bancária, para pagar suas contas, uma mensagem estranha apareceu. Informava que não havia saldo disponível! Checou seu extrato. Viu que no dia anterior seu salário havia sido depositado. Também viu que todo o valor havia sido transferido para outra conta – que ele não conhecia. Ainda era muito cedo e não dava para ligar para o gerente do seu banco. Então resolveu conferir suas aplicações. Entrou em choque quando percebeu que o saldo dos investimentos era o mesmo de sua conta corrente - R$ 0,00! Seu coração disparou e ele começou a suar frio!

A essa altura ele já estava sem saber o que fazer. Avisou seu chefe que precisava sair e foi direto ao banco. Na conversa com o gerente, descobriu que todas as transações, pelo menos perante o banco, haviam sido feitas por ele próprio. Seu salário havia sido transferido para outra conta usando as credenciais e senha dele. Os investimentos de toda sua vida estavam naquele banco e também haviam sido retirados "por ele" no dia anterior. Ouviu que nada poderia ser feito. Como era de se esperar, ele ficou furioso! Afirmou que não tinha feito nada daquilo e que queria seu dinheiro de volta. Procurou uma delegacia, registrou uma ocorrência e foi orientado a aguardar a investigação.

As contas do mês não puderam nem poderão ser pagas, Tony não sabe se conseguirá fazer suas compras rotineiras e necessárias, porque teve que cancelar seus cartões.

E quanto às demais pessoas da sua empresa? Lá a vida continuava normalmente, cada um fazendo seu trabalho, salvo um comentário ou outro de quem sabia o que tinha ocorrido com o Tony. Todos os dias, no final da manhã, o pessoal do departamento financeiro faz o pagamento das contas da empresa. Os fornecedores enviam boletos por e-mail e esses são impressos e enviados ao banco para serem pagos no caixa, com cheques. O que o pessoal ainda não sabia era que o mesmo vírus que havia infectado o computador do Tony, já havia se espalhado pelos computadores de vários funcionários.

Esse vírus tinha várias capacidades. Primeiro, quando uma pessoa acessa sua conta a partir de um computador infectado, o vírus captura os dados da conta e a senha e

depois transmite para o criminoso (em algum lugar na internet). Segundo, ele altera o código de barras de qualquer boleto impresso no computador infectado – quando o boleto é pago o dinheiro vai para a conta do criminoso. Os vírus, em geral, são conhecidos tecnicamente como *malware* e esse, que atacou o Tony e sua empresa, está numa categoria chamada, pelos especialistas, de *Ameaça Avançada*. São assim conhecidas pois elas têm a capacidade de se esquivar dos sistemas de antivírus. São como um vírus mutante.

Várias pessoas e empresas são vítimas destes *malwares*. Infelizmente, mesmo as pessoas que tomam muitos cuidados com seus dispositivos também são alvos de crimes como esses, difíceis de serem evitados.

Algumas companhias se especializaram em ajudar outras empresas e pessoas a se protegerem de ameaças como essas. Novas tecnologias permitem analisar o comportamento dos arquivos recebidos por e-mail e baixados da internet. Podem identificar se há alguma ameaça oculta em arquivos trabalhando enquanto visualizamos seu conteúdo. Podem inspecionar arquivos de textos PDF ou DOC, planilhas XLS, apresentações PPT, dentre outros. Se o arquivo estiver comprometido, o *malware* será removido e o destinatário receberá uma versão segura do arquivo. Com uma solução dessas, a empresa do Tony teria seu ambiente protegido contra esse e outros tipos de ameaça.

A Compugraf é uma companhia que pode proteger sua empresa, seu dinheiro e sua imagem. Implementamos soluções de proteção Antifraude, Ameaças Avançadas, *Anti-Bot* e *Anti-Malware*, dentre outras, para resolver as questões de segurança das pessoas, das empresas e dos bancos. Elas permitem mitigar os riscos e aumentar a segurança no mundo digital. Assim cada um pode se preocupar apenas com seu negócio, sabendo que o seu ambiente está seguro.

Apesar de não ter controle sobre o computador dos seus correntistas, o banco é responsável por prover um acesso seguro. Para aceitar as transações pela internet, deve prover meios de validar a identidade das pessoas, fazendo uso de tecnologias para detectar acessos suspeitos às transações, para proteger as senhas dos clientes enquanto eles as digitam, para bloquear alterações nas páginas dos sites, dentre outros recursos.

E o Tony? Perdeu tudo mesmo? Não! Para proteger a imagem da marca, o banco assumiu o prejuízo e devolveu o seu dinheiro. Agora ele sempre se certifica que sua empresa tem as ferramentas de segurança digital adequadas. Conversa frequentemente com o Gerente de TI para saber se estão atualizadas e continua usando a tecnologia a seu favor.

José Ricardo Batista
Business Development Manager