Brasileiros tÃªm prejuÃ-zo de R$ 16 bi com fraude virtual

  Os brasileiros perdem cerca de R$ 16 bilhões por ano em fraudes cibernéticas ou suas consequências, como gastos para conserto de máquinas ou despesas para reaver valores. As redes sociais são um dos principais alvo dos ladrões virtuais. Os dados são da versão 2012 do relatório da empresa de segurança virtual Norton Symantec. Otto Stoeterau, especialista de segurança da Norton, explica que, de acordo com o documento, os internautas brasileiros sabem que podem correr perigo nas redes sociais, mas apenas 44% dos entrevistados dizem se preocupar com soluções específicas para o ambiente. No Brasil, é estimado que mais de mais de 28 milhões de pessoas tenham sido vítimas deste tipo de crime nos últimos 12 meses, sendo que os prejuízos, por vítima, chegam a R$ 562. O relatório tem como base depoimentos pessoais de mais de 13 mil adultos de 24 países. O executivo da Norton afirma que o montante inclui, além de fraudes em contas bancárias, eventuais despesas para reaver o dinheiro roubado, gastos decorrentes de perda ou roubo de equipamentos – usados posteriormente em delitos –, além de desembolsos com consertos necessários por causa das invasões. Stoeterau afirma que muitos internautas abrem uma conta em rede social, como o Facebook, por exemplo, e após a navegação não se desconectam. Isso faz a “seção” ficar permanentemente aberta, o que facilita a ação de cibercriminosos. “O relatório identificou ainda que 36% dos internautas brasileiros aceitam convites ou conexões de pessoas desconhecidas, o que é um perigo”, alerta o executivo da Norton. Segundo ele, é bastante comum o “clique” em links sem que antes o receptor identifique tratar-se ou não de mensagem confiável. “Um hacker mal intencionado pode infectar aquele computador no qual a mensagem foi aberta e, uma vez instalado um vírus, o caminho segue pelas máquinas ou dispositivos móveis dos amigos”, observa o especialista. Stoeterau aponta outro perigo identificado no relatório da Norton: um em cada seis usuários não sabe identificar se seu perfil em uma rede social é aberto ao público em geral ou apenas aos amigos. “Evite dar informações relevantes que permitam identificar ações cotidianas, localização ou patrimônio, o que atrai e facilita a ação dos criminosos.” Almir Meira, professor de redes de computadores da Fiap, reforça as recomendações do executivo da Norton, e sugere que o perfil conte com o mínimo de informações de caráter privado. Meira também pede muita atenção no momento da definição da senha de acesso ao perfil. De acordo com o professor, códigos que tragam a combinação de informações como nome e data de aniversário do usuário são considerados fracos. “São senhas fáceis de descobrir, o que deixa o perfil mais suscetível à ação de fraudadores”, diz. Proteção - Meira sugere que no momento da definição do código, a pessoa escolha um verso de alguma música que ela goste e faça pequenas alterações, como trocar a letra o pelo número zero ou a letra i pelo sinal de exclamação. “É de fácil assimilação pelo usuário e cria grande dificuldade para ser fraudada”, afirma o professor. Leonardo Bonomi, especialista da empresa de segurança virtual Trend Micro, afirma que além dos cuidados com os dados que são informados nas redes, definição de senhas e permissões de acesso, é preciso ter programas antivírus atualizados permanentemente. “As armadilhas usadas pelos criminosos tornam difícil aos usuários identificar quando um link é confiável”, afirma.   Na Revista Cobertura tudo sobre setor de seguros. Acesse o site e fique por dentro!

Sobre o Autor

Agora você vai conhecer um pouco mais sobre a Cobertura Editora. Uma empresa que há 19 anos presta serviços editoriais e promove eventos voltados para o setor de seguros. Sempre presente nos principais eventos de seguradoras, corretores de seguros e de empresas de prestação de serviços ao mercado de seguros, a Cobertura Editora edita a Revista Cobertura - Mercado de Seguros e produz o Clipp-Seg Hoje, newsletter eletrônico com notícias diárias e em duas edições distribuídas através do mailing especializado da SK.