Sábado, 16 de Agosto de 2025

Ligações excessivas e golpes: por que seus dados podem estar no submundo da internet

Ofertas de produtos e golpes bancários. Quem não lida **cotidianamente** com essas “propostas” do outro lado da linha é porque possivelmente já desistiu de responder aos telefonemas. É o caso do aposentado João Pereira, de 76 anos. “São tantas ligações que, há alguns meses, decidi não atender mais”, relatou, explicando ter bloqueado os números desconhecidos.

Assim como ele, Paula* (nome fictício), de 30 anos, recebe diversas chamadas de empresas e golpistas. Mas, recentemente, a ligação de uma consultoria previdenciária a surpreendeu ainda mais. Na ocasião, a atendente indagou sobre o estado de saúde e ofereceu como serviço dar entrada em um processo de auxílio-saúde por meio do Instituto Nacional do Seguro Social (INSS).

Todavia, Paula não necessitava desse recurso financeiro. Há dois anos, ela se afastou do trabalho por 40 dias, mas não houve razões para estender o prazo. Além da importunação, a questão é: como essa firma detém detalhes que deveriam estar sob sigilo no sistema do órgão?

Já o login e a senha da assinatura de uma plataforma de *streaming*, como a Netflix, são apenas US$ 20, segundo o **índice de preços,** da companhia de segurança da informação Privacy Affairs. O levantamento é realizado todo ano e possui uma tabela com diversos “produtos” comercializados nessa rede secreta.

COMO FUNCIONA O MERCADO ILEGAL DE DADOS

Não se deve afirmar, contudo, ter sido essa a circunstância para a consultoria ter tido acesso ao histórico da Paula, mas a existência desse mercado ilegal é a explicação para a posse de muitos dados não concedidos voluntariamente pelos consumidores, conforme aponta o pesquisador de Segurança Informática da ESET, Daniel Cunha Barbosa.

“Há muitas fontes, mas podemos focar nas duas principais: o vazamento para algum fórum de 'dark web', onde se compra essas informações em lote, ou por uma pessoa dentro da empresa que atua como 'insider' (quem tem acesso à base privilegiada)”, esclarece.

Daniel Cunha Barbosa
Pesquisador de Segurança Informática da ESET

No segundo caso, o próprio consumidor acaba fornecendo o material, mas para outra finalidade. “No caso de idosos, um meio de contato é durante a compra de um medicamento. Aquele cadastro feito na farmácia pode ser passado por um funcionário”, exemplifica.

Outra possibilidade, aponta, é o crime *phishing* (pronunciado *"fishing"*), cuja prática é enviar e-mail ou criar sites falsos para roubar o dinheiro ou a identidade. Uma terceira hipótese é o site dos órgãos e empresas não serem suficientemente seguros contra o ataque de *hackers*.

Barbosa explica que somente quem possui conhecimento técnico consegue identificar se as informações de alguém estão na 'dark web'.A partir dos golpes, afirma, "não é possível inferir sobre a origem dos dados".

Independente da forma de captura, todos os caminhos podem levar esses dados confidenciais ao mercado ilegal de venda no submundo da internet. De acordo com Barbosa, é possível encontrá-los até gratuitamente.

Com essas informações em mãos, os crimes por telefone ficam mais sofisticados, já que é mais fácil se passar por outra pessoa, incluindo políticos, como ocorreu, no início deste mês, com o senador Cid Gomes (PSB).

Recentemente, o "golpe do Nubank" também repercutiu. Os criminosos ligavam supostamente do número do próprio banco para correntistas e informavam haver movimentação financeira suspeita. Temerosos, os consumidores forneciam nome completo, data de nascimento e até o número do cartão de crédito, incluindo o código de segurança.

O membro da Comissão de Defesa do Consumidor da Ordem dos Advogados do Brasil **(OAB-CE)**, Jefferson Cavalcante, reforça que muitos materiais são dados espontaneamente pelos próprios consumidores para quem deveria resguardá-los. Para ele, os vazamentos ocorrem com mais frequência contra servidores públicos, aposentados e pensionistas.

"Quando esse público dá entrada no processo, acaba sendo logo importunado com várias ligações de bancos e financeiras. Segundo o INSS, os dados são mantidos em sigilo, mas, na realidade, a situação é diferente", avalia.

Conforme Cavalcante, as instituições financeiras só podem ligar para quem já possui cadastro. Caso o consumidor receba ligações de outro banco com ofertas e dados informações não concedidas, deve denunciar à ouvidoria da Previdência Social.

O advogado também recomenda recorrer ao Programa Municipal de Defesa do Consumidor **(Procon)**. É importante solicitar o nome do atendente, da empresa e tirar um registro de tela ('print') das ligações, sobretudo quando são excessivas, para comprovar a importunação.

"Deve-se informar que está sendo importunado, mas também falar sobre a situação do vazamento de dados. Essas práticas continuam ocorrendo porque poucas pessoas denunciam", orienta. Para se ter ideia, no Procon Fortaleza, não há nenhuma denúncia.

Jefferson Cavalcante
Membro da Comissão de Defesa do Consumidor da Ordem dos Advogados do Brasil

Sobre o problema, a Federação Brasileira de Bancos (Febraban) disse não compactuar com fraudes e eventuais falsificações são reportadas às autoridades *(leia nota completa no fim deste texto)*. Já o Banco Central (BC), que regula ou supervisiona as instituições financeiras, não respondeu aos questionamentos, até esta publicação.

Como denunciar:

- O Procon recebe denúncias pelo telefone 151, das 8h às 17h, de segunda a sexta-feira, bem como de forma virtual, em qualquer dia e horário da semana, no portal da Prefeitura de Fortaleza; e ainda pelo aplicativo Procon Fortaleza;
- Ligue para ouvidoria do INSS, no número 135. Se for outro órgão, procure o contato da ouvidoria;
- Para não receber mais ligações de determinada empresa, se cadastre no site Não Me Perturbe

CONSUMIDOR TEM O DIREITO DE PEDIR EXCLUSÃO DOS DADOS DE EMPRESA; VEJA COMO PROCEDER

A presidente do Procon Fortaleza, Eneylândia Rabelo, explica que a Lei Geral de Proteção de Dados **(LGPD)** prevê a exclusão de detalhes pessoais após o fim da relação com as empresas. Por exemplo, se houver o encerramento de uma conta bancária, o consumidor pode exigir o apagamento no sistema.

Em caso de suspeita de fraude bancária, o ideal é entrar em contato imediatamente com a instituição financeira e registrar uma reclamação formal, solicitando o bloqueio da conta e/ou cartão bancário.

Além disso, é necessário registrar um Boletim de Ocorrência (B.O) para auxiliar nas investigações policiais. De acordo com o Procon, se a instituição financeira não resolver o problema ou se recusar a prestar assistência, é possível recorrer aos órgãos de defesa do consumidor, como o Procon.

“Tanto o Código de Defesa do Consumidor como a LGPD são ferramentas importantíssimas para garantir a segurança dos dados pessoais e a proteção dos consumidores em caso de fraude”, aponta.

Para Rabelo, é fundamental o conhecimento sobre os direitos para saber como proceder diante de fraude bancária. Deve-se:

- Informar imediatamente a instituição financeira;
- Buscar os órgãos de defesa do consumidor;
- Ou acionar o Poder Judiciário, a depender da circunstância.

COMO FICAM OS DADOS EM POSSE DOS ÓRGÃOS?

Segundo o advogado Jefferson Cavalcante, no caso da Paula, citada no início da reportagem, cujos dados estão sob a tutela de um órgão público, não há possibilidade de exclusão por se tratar de uma relação contínua. Entretanto, a instituição pública deve tratar as informações conforme a LGPD.

“O INSS é uma autarquia federal que trata dados pessoais de seus servidores, assim como dos aposentados e pensionistas, como nome, telefone e e-mail para fins de gestão de pessoas”, destaca.

“Se uma entidade financeira privada solicita ao setor de recursos humanos dessa autarquia os contato dos servidores para oferecer empréstimo consignado, O pedido deve ser negado pela autoridade competente, com base em análise técnica e jurídica”, enfatiza.

Conforme os artigos 26 e 27 da LGPD, os dados só poderão ser concedidos entre entes públicos e privados em algumas hipóteses. São elas:

- Casos de execução descentralizada da atividade pública que exija a transferência, exclusivamente para esse fim específico e determinado
- Casos de dados acessíveis publicamente
- Quando houver previsão legal ou a transferência for respaldada em contratos e instrumentos congêneres
- Ou na hipótese de a transferência objetivar exclusivamente a prevenção de fraudes e irregularidades, ou proteger e resguardar a segurança e a integridade do titular dos dados, desde que vedado o tratamento para outras finalidades.

COMO EVITAR GOLPES E TER DADOS VAZADOS

Conforme o pesquisador de Segurança Informática da ESET, Daniel Cunha Barbosa, é necessário haver maior consciência por parte dos usuários da internet sobre os riscos.

“É preciso ter atenção onde os dados serão inseridos, não ter senso de urgência para aproveitar um benefício, pequeno desconto que qualquer empresa pedir, pois nem todas se preocupam com a segurança”, alerta.

Ao fazer o cadastro em uma companhia, portanto, vale redobrar a atenção. Já as empresas devem buscar ferramentas eficazes para proteger as informações dos clientes.

“Existem camadas extremamente técnicas, mas as corporações devem basicamente proteger todos os dispositivos com as melhores formas e sempre atualizadas”, frisa, acrescentando ser fundamental mitigar as vulnerabilidades para impedir o acesso de criminosos.

Veja algumas dicas elaboradas pela ESET:

- Utilize um equipamento confiável. Dê preferência para dispositivos próprios ou até mesmo de acesso público em vez de usar de terceiros. Além de se colocar na posição de controle dos seus dados, será mais fácil para identificar quando ocorrer alguma atividade suspeita;
- Não utilize qualquer rede Wi-Fi. Não são todas as conexões que oferecem um grau de segurança recomendável, principalmente em espaços públicos. Preferencialmente, use uma rede 3G ou 4G. Caso não tenha essa opção, busque utilizar uma rede privada virtual (VPN), que permitirá a criptografia das informações;
- Instale as últimas atualizações. Sistemas desatualizados servem como porta de entrada para criminosos conseguirem acessar dados e também infectarem dispositivos. Muitos sistemas operacionais e aplicativos contam com a atualização automática;
- Crie senhas seguras. Utilize caracteres especiais, letras maiúsculas e minúsculas, dando prioridade para uma senha exclusiva ao serviço bancário;
- Use dupla autenticação. Habilite o segundo fator de autenticação no seu dispositivo, caso este seja um recurso oferecido pelo seu banco;
- Desconfie de e-mails e ligações para confirmação de dados. Os criminosos podem se passar por funcionários de bancos e, dessa forma, conseguir que você passe informações como números de cartões e senhas de contas. Em caso de dúvida, o ideal é sempre ligar para os números oficiais ou ir presencialmente à agência;
- Use o botão “desconectar” ao terminar de realizar as transações em sua conta, desconecte-se da sessão, isto pode dificultar o acesso de cibercriminosos à sua conta online.

VEJA O QUE DISSE A FEBRABAN

"Desde janeiro de 2020 está em vigor a Autorregulação do Consignado, iniciativa criada em parceria com a Associação Brasileira de Bancos (ABBC), que visa eliminar do sistema as más práticas relacionadas à

oferta e contratação dessa modalidade de crédito.

Pela autorregulação, é considerada falta grave qualquer forma de captação ou tratamento inadequado ou ilícito dos dados pessoais dos consumidores sem sua autorização e todos os bancos que participam da autorregulação assumem o compromisso de adotar as melhores práticas relativas à proteção e ao tratamento de dados pessoais dos clientes e o combate a fraudes.

Desde o início das regras, em 2020, até março de 2024, 1.331 medidas administrativas foram aplicadas a correspondentes bancários, dos quais 53 perderam o direito de exercer a atividade em definitivo e estão impedidos de prestar serviços aos bancos.

Os bancos que não aplicarem as sanções a correspondentes podem ser multados pelo Sistema de Autorregulação por conduta omissiva, cujos valores variam de R$ 45 mil até R$ 1 milhão.

Para coibir as ligações telefônicas indesejadas e o assédio comercial, por exemplo, os bancos participantes não remuneram os correspondentes em caso de novas operações em nome de consumidores que estão registrados ou desbloquearam seu número de telefone no "Não me Perturbe" há menos de 180 dias.

O fortalecimento da autorregulação conta ainda com o apoio de normas estatais, como a Instrução Normativa 138 do INSS, que estabelece que as instituições participantes do convênio devem aderir e respeitar as regras do Não me Perturbe, previstas na Autorregulação do Crédito Consignado.".

Fonte diariodonordeste