Veículo: Gazeta
Data: 07/02/2021
Link: https://www.agazeta.com.br/es/economia/megavazamento-saiba-o-que-fazer-e-como-proteger-seus-dados-pessoais-0221

Cuidado!

Megavazamento: saiba o que fazer e como proteger seus dados pessoais

Origem do vazamento de informações de 223 milhões de pessoas ainda é desconhecida, mas é quase certo que todos os brasileiros tiveram seus dados expostos, segundo especialistas, que alertam que os dados devem estar sendo vendidos na internet

Siumara Gonçalves
sfgoncalves@redegazeta.com.br

Vitória / Rede Gazeta
Publicado em 07/02/2021 às 07h11

Proteção de dados pessoais: megavazamento expôs informações completas sobre 223 milhões de brasileiros. Crédito: Pixabay

O maior vazamento de dados da história do país foi registrado no mês passado. Mais de 223 milhões de CPFs (incluindo de falecidos), 40 milhões de CNPJs e 104 milhões de registros de veículos caíram na internet. Segundo especialistas, é bem provável que essas informações pessoais de todos os brasileiros estejam agora disponíveis à quem quiser pagar o valor cobrado pelo hacker autor do golpe.

Parece sério, e é. Dados como CPF, data de nascimento, endereço, situação fiscal e até informações financeiras podem ser utilizados de formas diversas por pessoas mal intencionadas, seja para aplicar um golpe, pegar um empréstimo e sujar o nome da vítima na praça ou até filiar alguém a um partido político.

Segundo fontes ouvidas por **A Gazeta**, agora que as informações já estão "por aí", há pouco a ser feito para controlar o vazamento. Contudo, há algumas atitudes que podem ser tomadas para se resguardar em caso de mal uso dos seus dados e até para rastrear se o seu CPF está sendo usado sem o seu consentimento.

A origem desse vazamento ainda é desconhecida, mas é quase certo que todos os brasileiros tiveram seus dados expostos. Por meio de uma simples conta é possível verificar que o número de CPFs vazados supera em 11 milhões o contingente da população brasileira, que está estimada em 212 milhões de pessoas.

Dessa forma, segundo o perito em computação forense especializado em Segurança da Informação e comentarista de Tecnologia da Rádio CBN Vitória, Gilberto Sudré, é muito provável que pelo menos o CPF e a data de nascimento de todos os cidadãos brasileiros estejam disponíveis na internet, seja para venda ou gratuitamente.

"Na verdade, quase com certeza, o seu CPF e data de nascimento foram vazados. O risco de que isso não tenha acontecido é muito baixo"

Gilberto Sudré
Perito em computação forense especializado em Segurança da Informação

Veja também

Moraes manda PF investigar venda de dados de ministros do STF

Impactos do megavazamento de dados podem durar anos, diz especialista

Outra certeza é de que pessoas mal intencionadas usarão essas informações pessoais de terceiros para aplicar golpes, aponta o professor da UCL, João Paulo Chamon.

Porém, ele alerta que, embora nesse momento seja grande a curiosidade de saber quais dos nossos dados pessoais vazaram, é preciso ter cuidado. Isso porque sites que supostamente ajudam usuários a identificar essas informações podem, eles mesmos, capturar dados pessoais de quem utiliza.

Como é difícil saber a diferença entre fontes confiáveis ou não, ele orienta que as pessoas não utilizem esses sites de busca por dados vazados.

"É preciso primeiro manter a cabeça fria. Eles (os sites) alegam informar se um determinado CPF está entre as informações vazadas, porém, não se sabe se há segundas intenções por trás disso", explica.

E AGORA? O QUE PODE SER FEITO?

Segundo especialistas, existem poucas maneiras de se proteger contra possíveis golpes no futuro. Uma delas, que leva mais tempo e pode dar trabalho, é fazer um Boletim de Ocorrência.

O professor do curso de Sistemas de informação do campus Cachoeiro de Itapemirim do Ifes, Everson Scherrer Borges, aponta que esse é um meio legal que as pessoas têm de se proteger futuramente.

"O país tem dado os primeiros passos na proteção contra crimes cibernéticos. Já existem delegacias especializadas nesse tipo de golpe e vale a pena procurar uma, até como uma proteção futura. Se você sofrer um roubo de informação e perceber que foi lesado, o máximo de provas que tiver será imprescindível. Vamos supor que, em algum momento ocorra uma investigação e a polícia chegue até você. Com o BO em mãos será possível ter uma prova de que você é uma das vítimas de roubo de dados", explica.

Veja também

Empresa na Serra espionava Google Drive de concorrente para fraudar licitação

Google lista 5 dicas para evitar espionagem no drive

Outra forma de proteção, nesse caso financeira, é monitorar o seu CPF e tentar identificar movimentações suspeitas. Uma das formas de fazer isso é no Registrato, que é um sistema do Banco Central.

Nele você consegue consultar de forma gratuita relatórios de chaves Pix, de empréstimos, de financiamentos, de contas em banco e outros que foram feitos usando os seus dados. Se você não reconhecer algum deles, já é um sinal de alerta.

Também há meios de saber toda vez que o seu CPF for usado para fazer algum cadastro. Porém, esse monitoramento mais detalhado é pago. Uma empresa nacional que fornecesse esse tipo de serviço, por exemplo, cobra R$ 170 por ano.

INFORMAÇÕES DE CRÉDITO E ATÉ FOTOS ESTÃO NO VAZAMENTO

De acordo com a empresa de segurança Syhunt, que analisou alguns dos arquivos disponibilizados pelo hacker em fóruns on-line, as informações de 39.645 brasileiros (entre pessoas vivas e falecidas) e 22.983 empresas nacionais já circulam livremente e gratuitamente na internet. Embora a maior parte das informações estejam à venda na Dark Web, o golpista tornou pública uma pequena parte dos arquivos, como um "teaser".

Ao jornal Estadão, a empresa informou que, no total, estima que o hacker tenha em mãos quase 1 terabyte (TB) de informação. Um dos dados mais preocupantes entre todos os vazados é o pacote com fotos com o rosto de pessoas. Ele tem cerca de 16 GB e, para a Syhunt, isso equivale a imagens de 1,1 milhão de pessoas.

A lista de dados vazados é grande. Os dois vazamentos (de empresas e pessoas físicas) juntos continham:

- Dados básicos relativos ao CPF - nome, data de nascimento e endereço;
- Sexo;
- Endereços;
- Fotos do rosto das pessoas;
- Score de crédito - responsável por indicar se você é um bom pagador -, além da renda, cheques sem fundo e outras informações financeiras;
- Imposto de Renda (IR) de pessoas físicas;
- Dados cadastrais de serviços de telefonia;
- Grau de escolaridade;
- Benefícios do Instituto Nacional do Seguro Social (INSS);
- Programas sociais, como Bolsa Família;
- Dados relacionados a servidores públicos;
- Informações do LinkedIn.

CRIE BARREIRAS DE PROTEÇÃO

Ainda que não seja mais possível "recuperar" as informações que já vazaram, continua sendo muito importante se proteger contra outras investidas contra seus dados pessoais. Para isso, é preciso criar um muro e várias camadas de segurança.

Imagine da seguinte forma, o primeiro passo para usar uma conta, seja em uma rede social ou até uma carteira digital, é ter um login e senha. Normalmente o login é o seu e-mail. De posse dele, os criminosos vão precisar descobrir a sua senha, o que pode ser feito de duas formas, usando um programa que quebra a senha ou tentando "adivinhar".

A primeira camada de proteção está no grau de complexidade da sua senha. O professor do curso de Sistemas de informação do Ifes de Cachoeiro Everson Scherrer Borges, aconselha a, sempre que possível, escolher um código grande que inclua caracteres especiais - como @, #, $, %, & e ! -, letras maiúsculas e números.

"Uma boa forma de você construir uma senha é se apoiar em uma frase ou letra de música marcante. Com base nela você pode pegar a primeira ou última letra de cada palavra e formar uma senha aleatória. Mas é claro, sempre se preocupando com o nível de complexidade: caractere especial, maiúsculos e números para dificultar varredores de senha", comenta.

Veja também

Vazamento pode ter exposto 220 milhões de dados pessoais de brasileiros

Pix vira canal de paquera e Banco Central alerta sobre exposição de dados

Suponhamos que você é um fã de Luiz Gonzaga e que sua música favorita seja "Asa Branca". Usando a primeira letra de cada palavra do primeiro verso: "Quando olhei a terra ardendo/ Com a fogueira de São João", senha ficaria: **quatacafdsj**. Agora, troque as letras A por @ e/ou o S por $: **qo@t@c@fd$j**. E, para tornar ela ainda mais difícil, seria possível substituir a letra O pelo número 0 e colocar algumas delas em maiúsculo: **Q0@t@c@fd$J**.

"A cada dia que passa acredito que as senhas pedidas na hora de fazer um cadastro serão mais complexas para dificultar a ação de criminosos. Elas são como portões, cercas elétricas e grades da casa que é o mundo virtual"

Everson Scherrer Borges
professor do curso de Sistemas de informação do Ifes Campus Cachoeiro

Mas não adianta criar e usar a mesma senha em todas as mídias sociais, aplicativos e instituições financeiras. É preciso variar para que, caso alguém descubra uma delas, não consiga utilizar todas as contas que você possui na internet. Além disso, outra dica é trocar periodicamente de senha.

Outra barreira extra de proteção é a chamada autenticação em dois fatores ou verificação em duas etapas. Em muitos locais, como bancos e redes sociais, ela já está disponível e basta ativar. Ela te protege em caso de tentativa de clonagem do Whatsapp, roubo de e-mail e Instagram, uso indevido de contas bancárias, por exemplo.

LIMITE A QUANTIDADE DE DADOS QUE VOCÊ COLOCA NA INTERNET

Muito antes do megavazamento de dados do mês passado, uma série de informações pessoais já estavam disponíveis de graça na internet. Nome completo, data de nascimento, cidade onde reside e data de aniversário, por exemplo, são dados que as próprias pessoas costumam publicar voluntariamente nas redes sociais.

João Paulo Chamon aconselha que as pessoas prezem mais por essas informações. "Limite quem tem acesso às suas informações. Quanto mais pessoas puderem ter contato com seus dados, maiores serão as chances deles serem usados da forma errada", comenta o especialista em segurança.

Chamon lembra ainda que funcionários públicos e políticos têm a maior parte das suas informações pessoais divulgadas de forma pública em portais de transparência, ou na Justiça Eleitoral. Dessa forma, por meio do portal da transparência ou do Tribunal Eleitoral é possível consultar diversos dados, desde os da merendeira da escola até os do presidente da República.

VEJA 20 DICAS DE COMO PROTEGER SEUS DADOS

Com as senhas

1. Faça a mudança de senha frequentemente em todas as suas contas on-line;
2. Escolha diferentes senhas para e-mail, aplicativos e contas bancárias;
3. Escolha senhas difíceis, aleatórias e não óbvias como número do telefone, nome completo ou data de aniversário;
4. Tenha mais de um e-mail, para caso precise recuperar a senha do outro se ele for perdido ou roubado;
5. Não forneça suas senhas para ninguém. Bancos, por exemplo, nunca pedem a senha do usuário. Caso liguem pedindo, é um golpe;

Nas mídias sociais, sites e aplicativos

1. Assuma o controle das suas informações nas redes sociais. Leia e modifique as autorizações de privacidade e compartilhamento de dados;
2. Não disponibilize muitas informações pessoais nas suas redes. Quanto menos dados e preferências ficarem disponíveis, mais protegidos eles estarão;
3. Configure o perfil para que as publicações só sejam vistas por quem você realmente conhece;
4. Escolha a autenticação em dos fatores. Com ela fica mais difícil, caso você perca o celular ou tenha seus dados roubados, do invasor ter acesso às suas contas.
5. Ative os avisos de segurança nas contas bancárias, e-mail e redes sociais. Dessa forma, caso alguém faça um acesso não autorizado você saberá na hora;

No dia a dia

1. Não use qualquer computador para entrar nas suas redes sociais, muito menos em bancos e e-mails. Eles podem conter programas instalados para capturar informações;
2. Não use redes de internet abertas para se conectar as suas redes sociais, muito menos em bancos e e-mails. Elas também podem conter programas instalados para capturar informações;
3. Não clique em links desconhecidos ou promoções que cheguem por e-mail, mensagem de texto ou WhatsApp. Eles podem conter vírus para infectar o seu dispositivo e capturar informações;
4. Esteja ciente dos sites e e-mails de phishing e utilize soluções de segurança com função anti-phishing;
5. Não esqueça de ter o antivírus sempre atualizado. Isso vale para qualquer dispositivo, tanto celulares, quanto computadores;
6. Acompanhe regularmente a fatura e o extrato bancário;
7. Utilize sempre cartões virtuais para compras on-line, ele estará disponível no app do seu banco;
8. Faça o acompanhamento do seu CPF no Registrato, sistema do Banco Central. Por meio dele você pode consultar gratuitamente os relatórios de chaves Pix, de empréstimos, de financiamentos, de contas em banco e outros;