

28 de janeiro: Dia Internacional da Proteção de Dados



Mas o que é o Dia Internacional da **Proteção de Dados**?

No dia 28/1, é comemorado o Dia Internacional da Proteção de Dados. A iniciativa global tem o objetivo de promover, anualmente, o conhecimento sobre a **Lei Geral de Proteção de Dados (LGPD)**, por meio da criação de conteúdos explicativos sobre o tema, a fim de reforçar a importância da criação de uma cultura de proteção de dados e estimular as empresas a serem mais responsáveis sobre esse tema.

O objetivo da LGPD é garantir segurança, privacidade e transparência para as pessoas físicas ao cederem dados para companhias.

E o que você pode fazer para proteger suas informações pessoais **online**?

De acordo com números da Surfshark, de janeiro a novembro de 2021, 24,2 milhões de perfis de brasileiros tiveram suas informações expostas na internet a partir de ataques ou brechas em sistemas. Com isso, o **Brasil assumiu o 6º lugar no ranking de países com mais vazamentos de dados no mundo**. Além disso, o País também registrou um aumento nos casos de golpes contra pessoas jurídicas. (FONTE: [Isto é Dinheiro](#)).



Portanto, é fundamental que todos tenham o acesso e conhecimento a estratégias que auxiliem na proteção de seus dados pessoais. **Aqui estão alguns exemplos:**



1 - Limpe seus cookies: todos nós clicamos em ‘aceitar cookies’ sem realmente saber o que isso significa. Limpar regularmente os cookies de seu navegador removerá certas informações que foram colocadas em seu dispositivo, muitas vezes para fins publicitários. No entanto, os cookies também podem representar um risco de segurança, pois esses arquivos podem ser facilmente sequestrados por hackers.



DICA: Limpe, sempre que possível, o histórico de navegação sobre os sites visitados.

Para auxiliar os Participantes e empregados da Fundação, a PREVIRB montou o seguinte material: **Instruções para limpeza de cache** – [CLIQUE AQUI](#) para acessá-lo.

2 - Faça uso de navegadores que protegem a privacidade: muitos navegadores estão descontinuando cookies de terceiros e têm configurações de privacidade fortes por padrão. Mudar de navegador é uma mudança simples que pode auxiliar na proteção da sua privacidade. Dito isso, opte por fazer uso de navegadores mais conhecidos como: Google Chrome, Mozilla Firefox e Microsoft Edge.

3 - Utilize senhas fortes: Sabemos que é difícil lembrar todas as senhas que utilizamos no dia a dia e que fazer uso de senhas apenas com números pode ser mais fácil, mas essa NÃO é uma prática segura. Para maior segurança, o ideal é fazer uso de senhas alfanuméricas, ou seja, que contenham combinação aleatórias de letras minúsculas e maiúsculas, números e símbolos, além de evitar a repetição dessas senhas.



DICA: se lembrar de todas essas senhas complexas parece ser uma dor de cabeça, experimente fazer uso de um gerenciador de senhas confiável. Ele permite não apenas criar senhas fortes e únicas, mas também armazená-las, facilitando a consulta quando necessário.

4 - Reforce a segurança habilitando a autenticação de dois fatores: essa autenticação impede que outras pessoas acessem aplicativos e sites apenas com a sua senha, pedindo uma segunda verificação que pode ser via SMS, e-mail, WhatsApp etc.

5 - Mantenha o antivírus sempre atualizado: é essencial utilizar um aplicativo/programa confiável de antivírus que identifique e exclua qualquer programa que possa capturar dados sensíveis da sua máquina.

6 - Mantenha sua conexão Wi-Fi mais segura: não deixe o nome de fábrica, troque; desative a conexão automática, porque assim você não corre o risco de ser conectado automaticamente a redes abertas desconhecidas e potencialmente perigosas.

7 - Utilize apenas o seu computador ou celular de uso pessoal para acessar aplicativos de banco e/ou serviços financeiros: evite abrir esses tipos de aplicativos em equipamentos do trabalho ou de outras pessoas. É importante ter certeza que o computador/celular está protegido contra vírus que podem roubar seus dados.



DICA: não deixe seu celular, notebook ou computador ser acessado por pessoas estranhas. Encerre a sessão sempre que sair do e-mail, de redes sociais e demais áreas de acesso restrito.

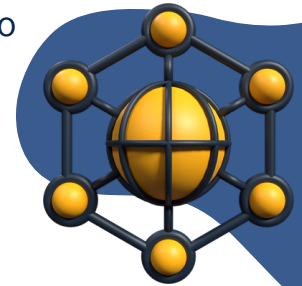
8 - Não compartilhe dados confidenciais por mensagens, e-mails ou telefone: Enviar senhas pessoais, número de cartão de crédito e outros dados sensíveis por mensagens pode ser um risco. Mesmo quando a pessoa do outro lado é confiável, não é possível garantir que ela não terá o celular roubado ou o aplicativo invadido.

9 - Desconfie de mensagens e sites desconhecidos: caso receba solicitações, de pessoas ou números desconhecidos, para enviar dados ou até valores, desconfie na hora.



DICA: evite clicar em links que vieram de fontes desconhecidas.

No caso de e-mails, sempre verifique o remetente, principalmente, nos e-mails de banco. Vale também ficar atento ao uso do português, muitas mensagens falsas apresentam pequenos erros de escrita.



10 - Conheça seus direitos de privacidade: muitas das leis de privacidade, como a LGPD, oferecem aos usuários um conjunto de direitos para ajudá-los a controlar como seus dados pessoais serão utilizados pelas empresas/instituições e fundações. Estes direitos podem variar de acordo com o País em que se encontra, portanto vale a pena conhecer quais direitos se aplicam a você e como você pode exercê-los.

A PREVIRB possui sua própria Política de Privacidade em conformidade com as exigências previstas na LGPD e que fica disponível, para acesso do público em geral, no site da Fundação. Portanto, que tal aproveitar a data para conhecer ou relembra-la? [**CLIQUE AQUI**](#) e acesse a Política de Privacidade da PREVIRB.

Esperamos que esse material possa auxiliar na proteção de seus dados pessoais!