O CARA DOS SITES

3 CONSEQUÊNCIAS DA
FALTA DE SEGURANÇA DO SITE
+ 2 DICAS PRÁTICAS

Confira 3 consequência da **FALTA DE SEGURANÇA** que o seu site pode trazer

Bem-vindo ao nosso ebook sobre segurança do site! Neste guia, forneceremos 4 dicas importantes para manter o seu site seguro e protegido contra possíveis ameaças.

Como proprietário de um site, você provavelmente já sabe que a segurança é uma preocupação constante. Com o crescente número de *ciberataques*, manter o seu site seguro é mais importante do que nunca. Além disso, a segurança do site é crucial para manter a confiança do cliente e garantir que as informações dos usuários sejam protegidas.

Neste ebook, abordaremos as principais razões pelas quais a segurança do site é importante e forneceremos dicas práticas para garantir que seu site esteja protegido contra possíveis ameaças. De proteger os dados do usuário a evitar penalizações do Google, nosso guia cobrirá todas as informações necessárias para manter o seu site seguro e protegido. Vamos começar!

1# PENALIZAÇÕES DO GOOGLE

O Google é um mecanismo de pesquisa popular e, como tal, tem grande influência sobre o tráfego do seu site. Ele está sempre buscando oferecer aos usuários a melhor experiência possível e, portanto, tem políticas rigorosas em relação à segurança dos sites.

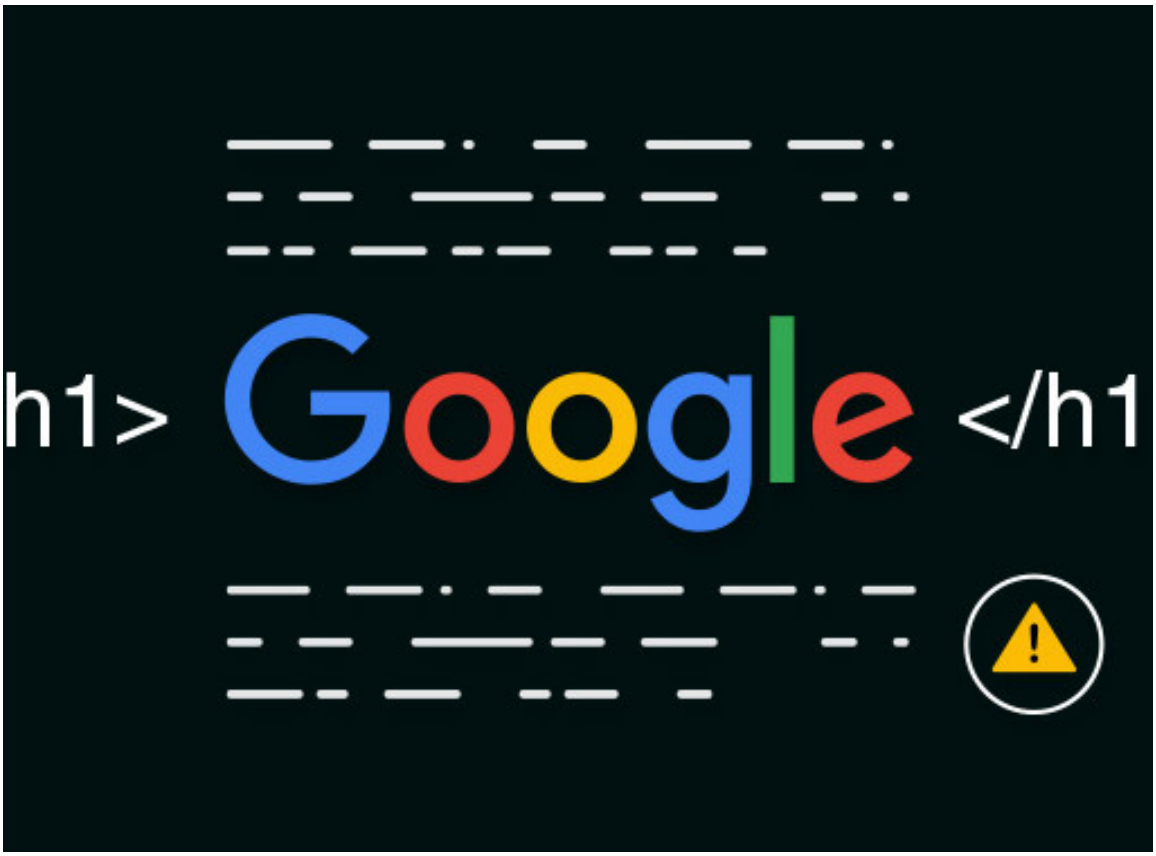
Se o Google determinar que um site é inseguro, ele pode penalizá-lo, o que pode levar a uma queda significativa no tráfego do site e nas classificações de pesquisa. Algumas das penalidades mais comuns que o Google pode impor a um site inseguro incluem:

- Exibir um aviso de segurança: Se o Google detectar que o site é inseguro, ele pode exibir um aviso de segurança para os usuários, alertando-os de que o site pode não ser seguro para navegar.

- Reduzir as classificações de pesquisa: Sites inseguros tendem a ter baixa classificação de pesquisa. Se o Google determinar que um site não é seguro, pode diminuir a posição do site nos resultados da pesquisa, tornando mais difícil para os usuários encontrá-lo.

- Remover o site dos resultados da pesquisa: Em casos extremos, o Google pode remover completamente o site dos resultados da pesquisa, o que pode ser devastador para o tráfego do site e para o sucesso dos negócios.

Portanto, manter o site seguro é crucial para manter a reputação positiva do site e para evitar penalizações do Google que possam afetar negativamente o tráfego do site. É importante implementar medidas de segurança sólidas, como um certificado SSL e senhas fortes, para garantir que o site seja seguro e protegido contra possíveis ameaças.



2# PROTEÇÃO DE DADOS DO USUÁRIO

Quando os usuários acessam um site, eles geralmente fornecem informações pessoais, como nome, endereço, e-mail e até mesmo informações financeiras. Mesmo que o usuário não preencha nenhum formulário o seu site captura informações valiosas através dos famosos Cookies. Esses dados são valiosos para os hackers, que podem usá-los para cometer crimes financeiros, como roubo de identidade, ou para vender esses dados na dark web.

Ao manter o site seguro, você pode proteger esses dados valiosos dos usuários e evitar que eles caiam nas mãos erradas. Algumas medidas que você pode tomar para proteger os dados dos usuários incluem:

- Usar um certificado SSL: um certificado SSL criptografa os dados do usuário, tornando-os ilegíveis para hackers. Isso garante que as informações confidenciais dos usuários, como senhas e números de cartão de crédito, não sejam interceptadas por terceiros mal-intencionados.

- Senhas fortes: as senhas são a primeira linha de defesa contra hackers. É importante que os usuários criem senhas fortes que incluem letras, números e caracteres especiais. Além disso, as senhas devem ser atualizadas regularmente e nunca devem ser compartilhadas entre diferentes sites.

- Inserção e configuração do *Captcha*: é um tipo de medida de segurança conhecido como autenticação por desafio e resposta. O CAPTCHA protege contra spam e descriptografia de senhas com um teste simples que prova que você é um ser humano, não um computador tentando invadir uma conta protegida por senha.

3# RESPONSABILIDADE LEGAL PELA SEGURANÇA DO SITE

Uma das principais leis que regem a segurança do site é a Lei Geral de Proteção de Dados (LGPD), no Brasil. Essa lei estabelece os direitos dos usuários em relação aos seus dados pessoais e impõe responsabilidades aos controladores e operadores de dados. Em caso de violação de dados, a LGPD prevê sanções administrativas, como multas e advertências, e também responsabilidade civil e criminal.

Outra lei importante é a Lei de Proteção de Dados Pessoais dos Estados Unidos (GDPR). Esta lei impõe responsabilidades semelhantes aos proprietários de sites em relação aos dados dos usuários, independentemente de onde eles estejam localizados no mundo. O GDPR também estabelece sanções significativas em caso de violação de dados.

Além das leis de proteção de dados, os proprietários de sites também podem enfrentar ações judiciais por negligência na segurança do site. Se um usuário sofrer danos ou perdas financeiras como resultado de um ataque cibernético em seu site, eles podem entrar com uma ação contra você alegando negligência na segurança.

Portanto, é importante entender a responsabilidade legal pela segurança do site e tomar medidas para garantir que seu site esteja adequadamente protegido contra ameaças cibernéticas. Certifique-se de seguir as leis de proteção de dados em vigor em sua região e implementar as melhores práticas de segurança cibernética para manter seu site e seus usuários seguros.

Muito bem, agora que você conheceu 3 consequências que um site sem segurança pode trazer, talvez você esteja se perguntando: *"tá, mas o que eu posso fazer AGORA para ter certeza de que estou seguro?"*

Não se preocupe, na próxima página eu separei 2 dicas que você pode aplicar hoje mesmo.

CONFIRA 2 DICAS PRÁTICAS PARA FAZER AINDA HOJE:

1 - Tome cuidado com os e-mails que recebe

Apesar de parecer óbvio mas ainda muitos usuários de e-mail clicam em qualquer link que recebem. Uma dica é sempre verificar a autenticidade do endereço de e-mail é simples perceber se um endereço de e-mail é confiável ou suspeito.

Outro ponto referente aos e-mails é sempre utilizar senhas fortes, nada de Senha123 ou Empresa123. Mescle números com letras e caracteres especiais como @, *, / e etc.

2 - Mantenha seu site e banco de dados sempre atualizados

Tudo o que um invasor precisa é de uma brecha aberta e sites desatualizados são ótimos lugares para que eles invadam e roube informações importantes que ali constam.

Aqui também vale manter as senhas de acessos bem fortes, mais até que as dos e-mails. Caso o seu site tenha sido desenvolvido em cima de um CMS, principalmente em casos com *WordPress* é imprescindível que ele esteja sempre em sua ultima versão.

Portanto, é importante entender a responsabilidade legal pela segurança do site e tomar medidas para garantir que seu site esteja adequadamente protegido contra ameaças cibernéticas. Certifique-se de seguir as leis de proteção de dados em vigor em sua região e implementar as melhores práticas de segurança cibernética para manter seu site e seus usuários seguros.

Espero que esse e-book tenha clareado suas dúvidas sobre a importancia do seu site estar sempre bem seguro.

E depois de todo esse conteúdo eu te pergunto: como está a segurança do seu website?

Entre em contato e agende uma avaliação gratuita!