
20 Dicas para se proteger na Internet
E-Book Gratuito
@kye3.sec
SECURITY
php
git
node

Role para baixo para ler o conteúdo

INTRODUÇÃO

Atualmente, a internet é amplamente utilizada por grande parte da população mundial e é considerada uma ferramenta indispensável para muitas atividades. No entanto, mesmo oferecendo muitas vantagens, ela também apresenta riscos consideráveis.

Com a evolução da tecnologia, os golpistas e cibercriminosos têm criado novas maneiras de acessar informações pessoais de usuários de redes sociais e outras plataformas online, causando prejuízos significativos. Por isso, é importante estar sempre atento e adotar medidas de segurança ao navegar na internet.

Para ajudar nessa tarefa, compilei uma lista com as 20 principais dicas para evitar os golpes em redes sociais e vazamentos de dados. Ao seguir esses passos, você estará aumentando significativamente sua segurança online. Além disso, é importante lembrar que a segurança na internet é uma responsabilidade compartilhada entre os usuários e as empresas. É fundamental que as empresas ofereçam medidas de segurança robustas e eficazes para proteger seus usuários, bem como educar a população sobre como se proteger de ameaças online.

1 - Use Senhas Fortes

Sempre use senhas fortes e únicas para cada conta que você tiver. Uma boa senha deve ser longa e complexa, com uma combinação de letras, números e caracteres especiais.

Como montar a sua senha forte:

- **No mínimo 27 caracteres;**
- **Letras maiúsculas e minúsculas;**
- **Símbolos e caracteres especiais: ! @ # $ % ¨ & * ? / ^ ~ ´ \;**
- **Evitar uso de datas conhecidas por várias pessoas, nomes de parentes, ruas e animais.**

Exemplo de Senha Forte (NÃO UTILIZE ESSA SENHA):
Uki%37sA1#Yh1>Ru5N&ä&a/?a4f0pLwq@

2 - Ative a Autenticação em Duas Etapas

A autenticação em dois fatores (2FA) é uma camada adicional de segurança que protege suas contas contra invasores. Quando você ativa a 2FA, precisa inserir um código único que é enviado ao seu telefone ou outro dispositivo de confiança, além de sua senha, para fazer login na sua conta.

Passo a passo (Habilitando a 2FA):

- **Passo 1: Instale um aplicativo de autenticação em seu smartphone**

Existem diversos aplicativos de autenticação que podem ser utilizados, como o Google Authenticator, o Microsoft Authenticator ou o Authy. Esses aplicativos podem ser baixados gratuitamente nas lojas de aplicativos para iOS e Android.

- **Passo 2: Acesse as configurações de segurança do serviço que você deseja proteger**

Vá até o site ou aplicativo que você deseja proteger e acesse as configurações de segurança. Procure pela opção "Autenticação em duas etapas" ou algo semelhante.

- **Passo 3: Escolha a opção de autenticação em duas etapas por aplicativo**

Na seção de autenticação em duas etapas, selecione a opção para utilizar um aplicativo de autenticação em vez de receber um código por SMS ou e-mail.

- **Passo 4: Configure o aplicativo de autenticação**

O serviço que você está protegendo deve apresentar um código QR ou uma chave secreta que deverá ser escaneado ou inserido no aplicativo de autenticação. Abra o aplicativo de autenticação que você instalou anteriormente e selecione a opção para adicionar uma nova conta. Em seguida, escaneie o código QR ou insira a chave secreta fornecida pelo serviço.

- **Passo 5: Verifique a autenticação em duas etapas**

Após a configuração do aplicativo de autenticação, você será solicitado a fornecer um código gerado pelo aplicativo ao fazer login no serviço. O aplicativo de autenticação gera um novo código a cada 30 segundos, portanto, certifique-se de inserir o código correto e válido antes que ele expire. Depois de inserir o código corretamente, você terá acesso à sua conta.

@kye3.sec

3 - Mantenha o Software Atualizado

Mantenha o software do seu computador, smartphone e outros dispositivos sempre atualizado. As atualizações incluem correções de segurança importantes que podem proteger seus dados pessoais.

Além dessas funcionalidades, as atualizações podem adicionar novas interações do suporte e da equipe de segurança com os usuários.

@kye3.sec

4 - Evite Links Suspeitos

Não clique em links suspeitos em emails ou mensagens de texto. Eles podem levar você a sites maliciosos que roubam suas informações pessoais.

- **Exemplo de link suspeito:**

  "https://www.maisbolosecia.com.login-attempt98765.xyz"

  Este link parece ser de uma empresa fictícia, mas contém um domínio suspeito e não oficial. Se um usuário clicar neste link e inserir suas informações de login, elas podem ser roubadas por um golpista.

- **Exemplo de link real:**

  "https://www.maisbolosecia.com/"

  Este é o link oficial de uma empresa fictícia, e é seguro clicar nele e inserir suas informações de login. Ele contém o domínio confiável e reconhecido dessa empresa.

@kye3.sec

5 - Use um Antivírus

O software antivírus é uma ferramenta importante para proteger seu dispositivo contra malwares e outras ameaças. Certifique-se de usar um software antivírus confiável e mantenha-o atualizado.

Recomendações: Avast, Kaspersky e McAfee.

@kye3.sec

6 - Não Compartilhe Informações Pessoais

Não compartilhe informações pessoais, como seu número de CPF, endereços, endereço de e-mail, ou informações bancárias, em redes sociais ou outros sites. Os golpistas podem usar essas informações para roubar sua identidade.

@kye3.sec

7 - Não Use Senhas Fáceis de Adivinhar

As senhas fáceis de adivinhar, como "123456" ou "senha", são fáceis de serem quebradas pelos golpistas. Use senhas fortes e únicas para cada conta e evite reutilizar senhas antigas.

Se você suspeita que sua conta foi vazada pelo motivo de usar uma senha fácil, consulte o site "https://haveibeenpwned.com/" e escreva o seu número de telefone/ e-mail e espere até o algoritmo terminar de fazer uma varredura pela web.

@kye3.sec

8 - Verifique as Configurações de Privacidade

Verifique as configurações de privacidade em suas contas de redes sociais e certifique-se de que apenas as pessoas que você confia possam ver suas informações pessoais.

Exemplos de opções de privacidade:

- **Somente seus amigos ou seguidores podem ver quem você segue/ o que você curte;**
- **Somente as pessoas que você segue podem te mencionar em stories e publicações;**
- **Somente seus amigos ou seguidores podem visualizar as fotos e informações do seu perfil.**

@kye3.sec

9 - Não Clique em Anexos Suspeitos

Os golpistas muitas vezes usam anexos maliciosos para infectar seu dispositivo com malware ou roubar suas informações. Evite clicar em anexos suspeitos e sempre verifique se o remetente é confiável antes de baixar qualquer anexo.

***Lembre-se*: Antes de clicar em um anexo, verifique se conhece o remetente e, se possível, confirme com ele que enviou o anexo. Se não tiver certeza, exclua o e-mail ou mensagem.**

Passo a passo:

- **Passo 1: Abra seu navegador de internet e acesse o site do VirusTotal em https://www.virustotal.com/gui/**

- **Passo 2: Clique no botão "Escolher arquivo" e selecione o arquivo que você deseja verificar. Verifique se é um arquivo que você realmente precisa e confie na origem.**

- **Passo 3: Clique no botão "Enviar arquivo" para enviar o arquivo para o VirusTotal. Aguarde alguns instantes enquanto o arquivo é verificado por várias ferramentas antivírus.**

- **Passo 4: Quando a verificação estiver concluída, você verá os resultados na tela. Se houver algum problema de segurança detectado, o VirusTotal indicará qual é o problema. Se tudo estiver bem, você poderá baixar o arquivo com segurança.**

- **Passo 5: Evite clicar em links ou baixar anexos de fontes que você não confia. Se você receber um arquivo de alguém que não conhece, verifique-o primeiro usando o VirusTotal antes de baixá-lo.**

Lembre-se de que o VirusTotal não é uma ferramenta 100% eficaz, e é importante usar seu próprio julgamento e cautela ao lidar com arquivos suspeitos na internet. Nunca baixe ou execute um arquivo se você tiver dúvidas sobre sua origem ou segurança.

@kye3.sec

10 - Configure Alertas de Atividade de Conta

Configurar alertas de atividade de conta é uma ótima maneira de se manter informado sobre qualquer atividade suspeita em suas contas. Isso pode ajudá-lo a detectar rapidamente e resolver qualquer problema de segurança.

Passo a passo:

Vá para as configurações de segurança da sua conta e procure a opção de alertas de atividade. Ative os alertas para receber notificações por e-mail ou mensagem sempre que houver uma atividade suspeita.

@kye3.sec

11 - Use Uma Conexão Segura

Sempre use uma conexão segura ao acessar informações sensíveis ou confidenciais, como informações bancárias ou de login. Certifique-se de que o site comece com "https://" em vez de "http://".
Isso também vale para conexões abertas, como as de supermercados e bares.

Passo a passo: verifique se o site que você está visitando começa com "https://" e se há um ícone de cadeado ao lado do endereço. Se não houver, evite inserir informações confidenciais.

@kye3.sec

12 - Desative a Geolocalização

Desativar a geolocalização em suas contas de redes sociais e dispositivos pode ajudar a proteger sua privacidade. Os golpistas podem usar suas informações de localização para rastrear seus movimentos e realizar ataques.

Passo a passo:

Vá para as configurações de privacidade em suas contas de redes sociais e dispositivos e desative a geolocalização.

@kye3.sec

13 - Fique Atento às Notícias

Fique atento às notícias sobre golpes e vazamentos de dados para se manter informado sobre as ameaças atuais e como evitá-las.

Passo a passo:

Configure alertas de notícias sobre segurança cibernética e golpes em seus dispositivos e fique atento às informações divulgadas pelas empresas e órgãos de segurança.

Sites para se manter informado sobre as principais notícias sobre tecnologia:

- **Canaltech (https://canaltech.com.br/);**
- **TechCrunch (https://techcrunch.com/);**
- **Olhar Digital (https://olhardigital.com.br/);**
- **TechTudo (https://www.techtudo.com.br/).**

@kye3.sec

14 - Não Confie em E-mails de Phishing

Os golpistas usam e-mails de phishing para enganar as pessoas e roubar suas informações pessoais. Esses e-mails geralmente pedem que você clique em um link suspeito ou forneça informações pessoais.

Passo a passo:

Nunca clique em links suspeitos em e-mails de remetentes desconhecidos ou que pareçam suspeitos. Verifique sempre o endereço de e-mail do remetente e, se tiver dúvidas, exclua o e-mail.

Exemplo de E-mail Suspeito:

“*Assunto: URGENTE! Aviso de Segurança*

Prezado Cliente,

Sua conta bancária está em risco de fraude. Por favor, clique no link abaixo para verificar sua identidade e manter sua conta segura.

[Link suspeito]

Atenciosamente,

*Seu banco***”**

Análise: Este email é suspeito porque usa linguagem alarmista para tentar convencer o destinatário a clicar em um link suspeito. O link leva a um site desconhecido, o que pode levar à instalação de malware ou roubo de informações pessoais.

@kye3.sec

Exemplo de um E-mail Real:

“*Assunto: Convite para a festa de aniversário da Ana*

Olá João,

Como você está? Eu queria convidá-lo para a festa de aniversário da Ana, que será no próximo sábado às 19h no meu apartamento. Teremos muita comida, bebida e diversão. Por favor, deixe-me saber se você pode comparecer para que eu possa confirmar o número de convidados.

Abraços,

*Maria***”**

Análise: Este email é real porque é enviado de uma pessoa conhecida do destinatário e contém informações pessoais e relevantes. Não há links suspeitos ou linguagem alarmista, e a mensagem é direta e amigável.

@kye3.sec

15 - Use Uma Senha Forte Para o Wi-Fi

Usar uma senha forte para o Wi-Fi pode ajudar a proteger sua rede doméstica contra invasores. Certifique-se de que sua senha seja única e complexa.

Passo a passo:

Altere a senha do Wi-Fi nas configurações do roteador e certifique-se de que a senha seja forte e única (Primeiro tópico do E-Book).

@kye3.sec

16 - Use um Gerenciador de Senhas

Usar um gerenciador de senhas pode ajudá-lo a criar senhas fortes e únicas para cada uma de suas contas, sem ter que memorizá-las todas. Isso pode ajudar a proteger suas informações pessoais em caso de vazamentos de dados.

Passo a passo:

Baixe um gerenciador de senhas confiável e crie uma conta. Adicione suas informações de login para cada uma de suas contas e permita que o gerenciador crie senhas fortes e únicas para cada uma delas.

- **Passo 1: Escolha um gerenciador de senhas e baixe-o no seu dispositivo;**
- **Passo 2: Crie uma conta no gerenciador de senhas e escolha uma senha mestra segura;**
- **Passo 3: Adicione suas senhas no gerenciador, manualmente ou através da importação de outros gerenciadores ou navegadores;**
- **Passo 4: Quando precisar fazer login em um site ou aplicativo, abra o gerenciador de senhas e selecione a senha correspondente;**
- **Passo 5: Utilize o recurso de autocompletar do gerenciador para inserir automaticamente seu nome de usuário e senha nos campos de login;**
- **Passo 6: O gerenciador de senhas também pode gerar senhas fortes e exclusivas para você, o que ajuda a evitar o uso de senhas repetidas ou fáceis de adivinhar;**
- **Passo 7: Mantenha sua senha mestra segura e atualize-a regularmente.**

@kye3.sec

17 - Nunca Compartilhe Informações Pessoais Com Estranhos

Nossas informações pessoais são informações importantes e confidenciais que podem ser usadas para nos identificar, nos localizar ou nos prejudicar de várias maneiras. Compartilhá-las com estranhos pode colocar nossa privacidade em risco e expor-nos a riscos de fraude, roubo de identidade ou outros crimes.

Por exemplo, dados bancários podem ser usados por criminosos para roubar dinheiro de nossas contas bancárias, enquanto o CPF pode ser usado para abrir contas de crédito ou realizar compras em nosso nome. O endereço pode ser usado para nos localizar fisicamente ou para fins de assédio.

Portanto, é importante proteger nossas informações pessoais e compartilhá-las apenas com pessoas em quem confiamos e para fins legítimos. Sempre verifique a origem da solicitação de informações e evite compartilhá-las com estranhos ou em sites não confiáveis. É importante também verificar a política de privacidade e segurança de sites e aplicativos antes de fornecer informações pessoais.

@kye3.sec

18 - Não Compartilhe seu Código do PIX com Estranhos

O código do PIX é a chave para realizar transações financeiras através desse sistema de pagamento. Não compartilhe seu código do PIX com pessoas que você não conhece ou que não confia.

Passo a passo:

Nunca compartilhe seu código do PIX com estranhos, mesmo que pareçam confiáveis ou legítimos. Verifique se a solicitação é legítima antes de fornecer o código, como entrar em contato diretamente com a pessoa ou empresa solicitando o pagamento.

@kye3.sec

19 - Cuidado com a Clonagem de Cartões

A clonagem de cartões é um dos golpes mais comuns atualmente. Fique atento a movimentações estranhas na sua conta bancária e verifique sempre seus extratos com frequência.

Passo a passo:

Fique atento a movimentações estranhas na sua conta bancária, como saques ou compras que você não reconhece. Verifique seus extratos com frequência e entre em contato com seu banco imediatamente se notar algo suspeito.

@kye3.sec

20 - Cuidado ao Digitar Senhas em Caixas Eletrônicos ou Máquinas de Cartão

Ao digitar senhas em caixas eletrônicos ou máquinas de cartão, certifique-se de que ninguém esteja observando. Cuidado com dispositivos adicionais que possam ser instalados nas máquinas para capturar informações.

Passo a passo:

Verifique se há algum dispositivo suspeito na máquina antes de inserir seu cartão. Ao digitar a senha, certifique-se de que ninguém esteja observando e cubra o teclado com as mãos, se necessário.

@kye3.sec

Finalização

Espero que essas 20 dicas tenham sido úteis para ajudá-lo a se manter mais seguro na internet. Lembre-se sempre de ficar alerta e tomar precauções extras para garantir que suas informações pessoais e financeiras estejam protegidas.

Lembre-se de que a segurança na internet é um esforço contínuo, e que sempre há mais a aprender e a fazer para se manter protegido. Esteja sempre atento às ameaças em constante evolução e adapte-se às novas técnicas e ferramentas de segurança.

Se você precisar de ajuda ou quiser saber mais sobre como se manter seguro na internet, sinta-se à vontade para entrar em contato comigo ou com outros profissionais de cibersegurança confiáveis. Juntos, podemos trabalhar para tornar a internet um lugar mais seguro para todos.

Quem sou eu?

Meu nome é Guilherme Lasalvia, mas sou conhecido na comunidade de cibersegurança como "Kye3"(@kye3.sec). Há aproximadamente um ano tenho atuado na conscientização de pessoas e empresas sobre as formas de se manterem seguras na internet, e espero que essas dicas possam te ajudar a se sentir mais protegido(a) e seguro(a) online.