1. *Principais dicas de segurança na internet para todos*

De crianças a avós e profissionais, as ameaças online podem afetar qualquer pessoa. Conhecer as regras da internet deve ser uma prioridade. Continue lendo para ver um resumo das ameaças cibernéticas atuais, juntamente com uma lista de dicas de segurança na internet que todos devem seguir. Antes de começar, instale um aplicativo de segurança para ajudar a proteger o seu dispositivo.

2. O que é segurança na internet?

A segurança na internet diz respeito a práticas e estratégias usadas para proteger as pessoas contra roubos online, fraudes e outras ameaças digitais. A segurança na internet envolve uma combinação de fatores, incluindo a instalação de um software de segurança, o conhecimento das regras e ameaças online, a adoção de práticas de navegação segura e a execução de uma boa higiene digital, como a criação de senhas fortes e exclusivas.

À medida em que a tecnologia ocupa uma parte cada vez maior de nossa vida cotidiana – desde a forma como nos comunicamos até como usamos equipamentos básicos (internet das coisas) – manter a segurança online é fundamental para garantir uma navegação segura. Embora as novas tecnologias da internet tragam grandes benefícios, elas também dão origem a novas ameaças cibernéticas. Isso significa que a conscientização sobre a segurança online é fundamental na a defesa contra ameaças como malwares e vírus.

Infelizmente, a maioria das pessoas não prioriza a proteção online. Os números e dados sobre a segurança na internet mostram um cenário preocupante:

- Em 2022, houve um aumento de 61% nos ataques de phishing.
- estima-se que 50% das pessoas usam a mesma senha em todas as suas contas.
- 81% das violações de dados em empresas são aparentemente causadas por senhas fracas.

3. Quais são os perigos da internet?

Os perigos da internet dizem respeito a qualquer coisa que possa prejudicar um usuário, seja de forma financeira, emocional ou física.

Veja a seguir exemplos de ameaças comuns à segurança digital:

- Roubo de identidade
- Phishing
- Golpes online
- Malwares, incluindo vírus, spywares, adwares, cavalos de Troia e ransomwares
- Bullying virtual

Reforce a sua segurança pessoal online usando um software de segurança em todos os seus dispositivos. E lembre-se de que Macs podem pegar vírus e celulares também podem ser infectados por malwares.

4. Dicas de segurança na internet para pais e filhos

A dica de segurança na internet mais importante para crianças é nunca compartilhar nenhuma informação pessoal, incluindo senhas, endereços residenciais ou escolares, aniversários e nem mesmo nomes de animais de estimação.
Aqui estão mais regras e diretrizes de segurança cibernética para interações online:

a. Não publique fotos pessoais

Fotos podem passar detalhes pessoais sobre as crianças, como o endereço de casa ou o nome da escola. Elas também podem revelar hobbies e outros interesses, que podem ser explorados por manipuladores.

b. Use nomes Falsos

Cibercriminosos podem obter muitas informações sobre uma pessoa a partir de seu nome. Certifique-se de que seus filhos sempre usem um nome de tela - pseudônimo (nunca o próprio) - e que ele não inclua nenhuma informação pessoal, como data de nascimento.

c. Tenha cuidado com os anúncios online

Ensine seus filhos a terem cautela antes de clicar em anúncios online para evitar a tentação. Ele bloqueia anúncios e ajuda a evitar o rastreamento na web.

d. Não responda mensagens de estranhos

Ensine as crianças a enviarem mensagens apenas às pessoas que elas conhecem. Estranhos podem mentir sobre a idade, gênero e outros detalhes importantes.

e. Denuncie o cyberbullying

O cyberbulling é um dos tópicos de segurança na internet mais assustadores para os pais. Incentive as crianças a se manifestarem caso sofram bullying virtual.
O cyberbullying pode ser particularmente perigoso para os jovens.

f. Configure controles parentais

Os telefones infantis mais seguros vêm com controles parentais para maior proteção. Descubra como configurar os controles parentais em dispositivos Android ou saiba mais sobre o controle parental do iPhone ou iPad. E converse com as crianças sobre como o controle parental pode ajudá-las a usar seus dispositivos de forma responsável.

5. Dicas de segurança na internet para adultos

O número de possíveis ameaças à sua segurança pessoal online parece crescer a cada ano. Aqui estão as principais regras para ter segurança na internet:

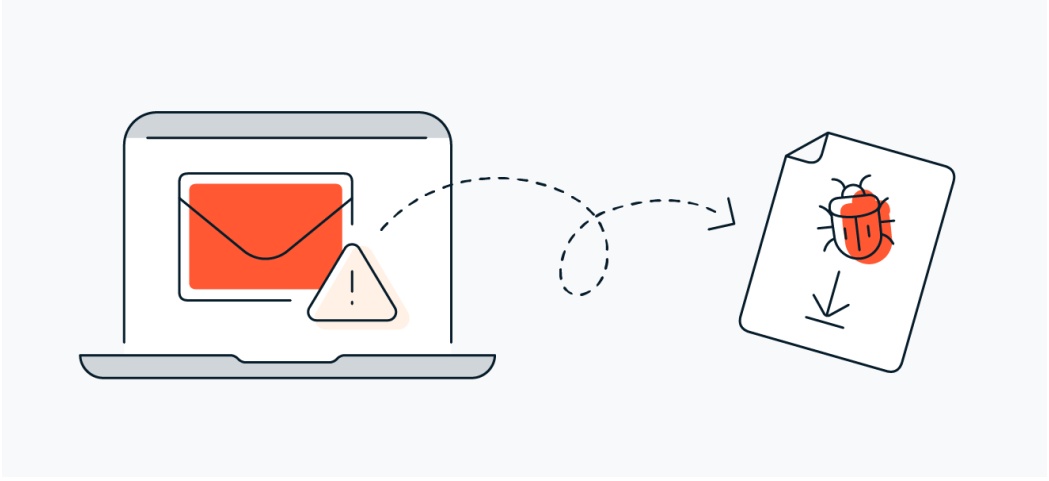
a. Não reutilize senhas

Para evitar o comprometimento de perfis e contas online, crie uma senha exclusiva para cada um deles. Saiba como criar senhas fortes e escolher o melhor gerenciador de senhas para manter o controle de todas elas.

b. Não abra anexos de fontes desconhecidas

Geralmente, anexos de e-mail são usados para entregar malwares que atacam seu dispositivo ou roubam seus dados. A menos que a origem seja de uma fonte confiável, não abra e nem faça download de nenhum anexo.

Verifique a fonte antes de fazer download ou abrir anexos.



c. Verifique a origem dos e-mails antes de clicar nos links

E-mails falsos podem levar a sites não seguros. Verifique se o e-mail é legítimo antes de clicar em um link. Os sinais de e-mails fraudulentos incluem erros de ortografia e saudações genéricas. Você deve sempre denunciar um golpe digital ao detectá-lo.

d. Revise as configurações de privacidade e políticas de dados

As informações pessoais podem ser valiosas para comerciantes e diferentes tipos de cibercriminosos. Mantenha a privacidade de seus dados revisando as configurações de privacidade e as políticas de dados dos aplicativos e serviços que você usa.

e. Dicas de segurança na internet ao viajar

Viajar para um novo destino é ótimo, mas usar uma rede Wi-Fi não confiável é arriscado.

6. Veja como navegar na internet com segurança durante uma viagem:

a. Use uma VPN

VPN é uma ferramenta que criptografa sua conexão com a internet, ajudando a manter os ciber criminosos afastados e impedir que corretores de dados acessem seus dados.
Instale um VPN e ative-o sempre que estiver viajando e usando uma rede Wi-Fi pública.

b. Tenha cuidado ao se conectar a redes Wi-Fi gratuitas

As conexões Wi-Fi gratuitas geralmente não são criptografadas, o que significa que cibercriminosos podem ver o que você está fazendo online. Use uma VPN para proteger sua conexão sempre que estiver usando um ponto de conexão Wi-Fi gratuito.

7. Dicas de segurança na internet para estudantes

A internet oferece ótimos recursos educacionais, bem como plataformas para socializar e aprender mais. Mas esses benefícios trazem armadilhas que podem afetar sua vida pessoal ou acadêmica.
Se você é estudante, proteja-se na internet com essas dicas de segurança:

a. Verifique as informações online

O fato de você ter lido uma informação online não significa que ela seja verdadeira. Sempre verifique os valores e dados fazendo referências cruzadas em outros sites ou com outras fontes. O fato de você ter lido algo online não significa que aquilo seja verdadeiro.

b. Tenha cuidado com quem você conhece

Perfis falsos em redes sociais podem ser difíceis de identificar, portanto, tome cuidado com estranhos que entram em contato com você. Nunca revele informações pessoais e tenha cuidado se alguém pedir informações confidenciais.

c. Evite o compartilhamento excessivo

Pense duas vezes sobre o que você está compartilhando ou publicando online sobre si mesmo. Quanto mais você se mantiver off-line ou em privacidade, maior será a probabilidade de evitar o roubo de identidade.

Tenha cuidado com o que você compartilha online, especialmente com estranhos.

8. Dicas de segurança na internet para todos

Priorizar a segurança da navegação na internet garante a proteção do seu dispositivo e dados. Embora os ciber criminosos geralmente visem grupos específicos para golpes, há algumas dicas universais sobre como se proteger.
Aqui está a nossa lista com as 10 principais regras e dicas de segurança na internet para todos:

- **Verifique se os sites são seguros**
  Verifique se os sites que você acessa têm um certificado SSL e usam o protocolo de segurança*"https"*, que é criptografado (o "http" não é). Essa é apenas uma etapa que pode ajudar a evitar golpes como o spoofing.
- **Instale as atualizações de software mais recentes**
  Cibercriminosos estão constantemente encontrando novos vetores de ataque. As atualizações de software mais recentes para seu dispositivo e aplicativos ajudam a corrigir riscos e vulnerabilidades de segurança.
- **Faça backup de seus dados**
  No caso de um ataque de malware ou falha do dispositivo, talvez seja necessário formatar o aparelho. O backup dos seus dados em um dispositivo de armazenamento externo e na nuvem pode ser um salva-vidas.
- **Cuidado com o que você publica**
  As informações que você compartilha online podem ser usadas contra você ou permitir que alguém roube sua identidade. Mantenha-se em segurança na internet ocultando detalhes importantes sobre você.
- **Atenção às notícias falsas**
  Sites de fake news podem roubar informações pessoais ou espalhar malwares. Preste atenção à ortografia das URLs. Esses sites geralmente usam "tiposquatting", em que um domínio tem praticamente a mesma aparência ao endereço de uma marca legítima, talvez com uma letra a mais.
- **Use um gerenciador de senhas**
  É difícil manter o controle de tantas senhas, mas não se comprometa tornando-as mais simples. Use um gerenciador de senhas para atualizar e armazenar as credenciais de acesso à conta.

- **Use a 2FA**
  Com a autenticação de dois fatores (2FA), você usa dois métodos para acessar uma conta. Se sua senha for roubada, sua conta protegida por 2FA permanecerá segura e privada.
- **Use uma VPN**
  Você ainda está se perguntando se realmente precisa de uma VPN? A resposta é sim. Uma VPN garante seu anonimato ao ocultar seu endereço IP e atividades online.
- **Use um antivírus confiável**
  O Windows Defender é suficiente para proteger seu dispositivo? Em alguns casos, talvez. Mas nada se compara aos antivírus modernos pagos, que são atualizados para proteger os usuários contra as ameaças mais recentes.
- **Evite anexos ou links suspeitos**
  Links e anexos não seguros podem levar ao roubo de dados ou infecções por malwares. E-mails falsos ou sites maliciosos podem parecer muito convincentes, portanto, pense duas vezes antes de clicar em qualquer coisa.

Seguir as práticas recomendadas de segurança na internet e adotar uma boa higiene digital ajuda a manter você protegido contra ameaças. Se você acha que seus dados pessoais ou credenciais de acesso já podem ter vazado na web, use uma ferramenta de verificação de invasões para descobrir e alterar suas senhas.

9. Ganhos rápidos

Práticas de segurança na internet não precisam tomar muito tempo. Embora a melhor abordagem seja adaptar uma estratégia de segurança baseada em suas atividades online, as regras básicas da internet se aplicam a todos. Tenha sempre em mãos essas dicas de segurança online:

- Crie senhas fortes e exclusivas para suas contas.
- Use uma 2FA.
- Não compartilhe muitas informações em redes sociais.
- Tenha cuidado ao se conectar a redes Wi-Fi públicas.
- Instale um antivírus confiável.
- Ative recursos de segurança em seus dispositivos e contas.
- Feche contas não utilizadas.
- Instale um firewall para proteger sua rede e seus dispositivos.
- Use nossa VPN grátis no seu PC e demais dispositivos

10. Proteja-se com uma segurança online rígida

A segurança adequada na internet requer uma abordagem multifacetada. O Antivírus Pago oferece proteção confiável para o complexo mundo digital da atualidade. Além de um mecanismo antimalware avançado, ele pode detectar vulnerabilidades da rede para ajudar a proteger sua Wi-Fi.

11. Restrições de Acesso

Garanta sempre que te ausentas, que o seu dispositivo, o computador, o telemóvel ou Tablet, estão com a tela bloqueada. Esta ação, evita que pessoas não autorizadas tenham acesso ao seu computador. Crie se possível, níveis de acesso diferenciado e com mais de um recurso de proteção.