

Guia de Segurança da Informação para

ESTUDANTES



Ilustração

Will Stopinski
Leandro Alves de Almeida
Debora Bacchi Camillo

Projeto Gráfico/Diagramação

Joise Nascimento
Silvio Turra

Conteúdo e Elaboração

GOVERNADOR DO ESTADO DO PARANÁ

Carlos Massa Ratinho Junior

Secretário de Estado da Educação

Professor Roni Miranda Vieira

Diretor-Geral

João Luis Giona Junior

Diretor de Educação

Anderfábio Oliveira dos Santos

Diretor de Tecnologia e Inovação

Claudio Aparecido de Oliveira

Bem-vindo ao guia essencial de segurança digital para estudantes! Este manual oferece estratégias práticas para proteger sua presença online e navegar com segurança no mundo digital.



Senhas Fortes

Aprenda a criar senhas seguras que protejam suas contas e informações pessoais contra invasores.



Proteção nas Redes Sociais

Descubra como configurar suas redes sociais para melhorar sua privacidade enquanto mantém conexões com colegas.



Backups Seguros

Conheça métodos práticos para garantir que seus trabalhos escolares e arquivos importantes estejam protegidos.



Segurança de Dispositivos

Estratégias simples para manter seus dispositivos protegidos contra ameaças digitais no ambiente escolar.



Sumário

Este guia está organizado nas seguintes seções para facilitar sua navegação:

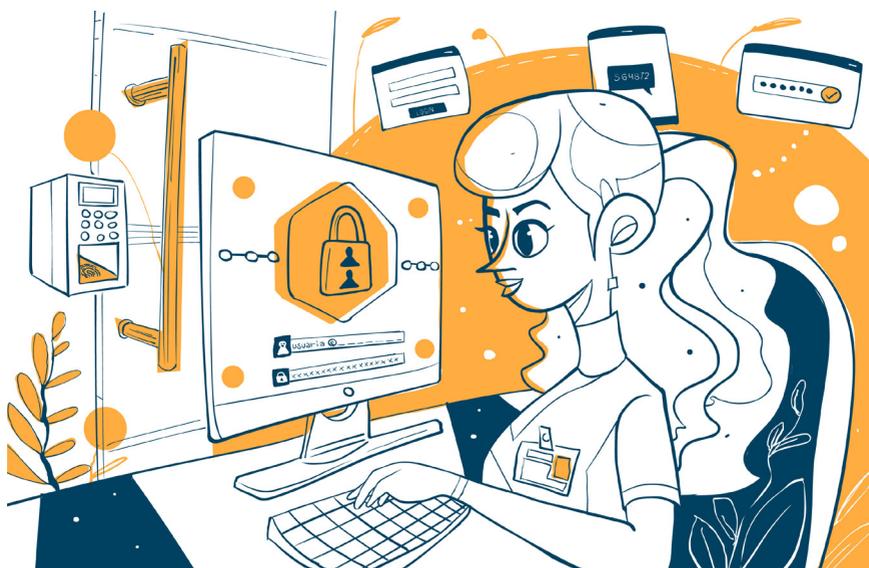
- 1. Introdução à Segurança da Informação**
- 2. Protegendo suas Redes Sociais**
- 3. Senhas e Autenticação**
- 4. Navegação Segura na Internet**
- 5. Cuidados com Dispositivos**
- 6. Backup de Dados**
- 7. Glossário de Termos**
- 8. Recursos Adicionais**

Cada seção contém informações e dicas que você pode aplicar imediatamente para aumentar sua segurança digital. Recomendamos que leia o guia completo, mas você também pode consultar seções específicas conforme sua necessidade.

Introdução à Segurança da Informação

A segurança da informação engloba práticas que protegem seus dados pessoais contra acessos não autorizados. No mundo digital, proteger informações é tão essencial quanto trancar sua casa.

Como estudante, você utiliza a internet para estudos, entretenimento e socialização, o que expõe suas tarefas escolares, conversas, fotos e dados pessoais a possíveis riscos.



Este guia apresentará métodos para identificar ameaças e adotar práticas seguras no ambiente digital.



Por que a Segurança Digital é Importante para Estudantes?



Proteção da Privacidade

Suas informações pessoais podem ser mal utilizadas se expostas inadequadamente.



Prevenção contra Cyberbullying

Contas invadidas podem ser usadas para enviar mensagens ofensivas, prejudicando sua reputação.



Proteção de Trabalhos Escolares

Falhas de segurança podem resultar na perda de trabalhos e afetar seu desempenho acadêmico.



Desenvolvimento de Hábitos Saudáveis

Práticas de segurança aprendidas cedo formam hábitos úteis para toda a vida.

Protegendo suas Redes Sociais: Visão Geral

As redes sociais são essenciais para sua vida social, mas podem expor informações privadas. Gerenciar adequadamente suas contas é fundamental para sua segurança digital.



Com uso consciente, você aproveita os benefícios da conexão online enquanto protege sua privacidade. Nas próximas seções, apresentaremos medidas para proteger suas contas nas diversas plataformas.



Configure sua Conta como Privada

Contas públicas permitem que qualquer pessoa veja suas publicações e informações pessoais. Proteja sua privacidade configurando suas redes sociais corretamente.



Por que configurar como privado?

Contas públicas permitem que qualquer pessoa, mesmo desconhecidos, veja suas publicações, fotos e informações pessoais. Isso aumenta significativamente os riscos à sua privacidade e segurança.

Como fazer

- Acesse as configurações de privacidade da rede social
- Procure por opções como “Conta Privada” ou “Quem pode ver meu conteúdo”
- Selecione a opção mais restritiva disponível
- Revise regularmente essas configurações, pois elas podem mudar após atualizações

Lembre-se: cada rede social tem suas próprias configurações de privacidade. Dedique um tempo para explorar e configurar adequadamente cada plataforma que você utiliza.

Seja Seletivo com seus Seguidores



Analise antes de aceitar

Aceitar seguidores ou amigos desconhecidos em suas redes sociais pode parecer inofensivo, mas representa um risco real à sua privacidade e segurança.

Perfis falsos são frequentemente utilizados para coletar informações pessoais ou para fins maliciosos.



Em caso de dúvida, recuse

Adote a prática de aceitar apenas pessoas que você conhece pessoalmente ou com quem tem conexões verificáveis. Antes de aceitar um pedido de amizade ou seguidor, pergunte a si mesmo: **“Eu realmente conheço essa pessoa? Por que ela quer me seguir?”**



Verifique as conexões

Se tiver dúvidas sobre quem está tentando conectar-se a você, **o mais seguro é recusar ou adiar a decisão até obter mais informações.** Sua segurança digital depende das conexões que você aceita.



Limite Informações Pessoais nas Redes Sociais

Localização

Evite compartilhar sua localização ou fazer check-in em lugares que você frequenta regularmente, como sua escola.



Rotina

Não publique detalhes sobre sua rotina diária, como horários de aulas ou atividades extracurriculares.

Endereço

Nunca compartilhe seu endereço residencial ou informações que possam revelar onde você mora.



Contatos

Mantenha seu número de telefone e e-mail privados, compartilhando apenas com pessoas de confiança.

Cuidados ao Compartilhar Fotos



Informações Reveladas

Fotos podem revelar muito mais informações do que imaginamos. Ao compartilhar imagens nas redes sociais, fique atento a detalhes que podem comprometer sua privacidade ou a de seus colegas.

O Que Evitar

Evite publicar fotos que mostrem o uniforme da sua escola, a fachada da sua casa ou placas com nomes de ruas.



Respeito à Privacidade

Sempre peça permissão antes de postar fotos que incluam outras pessoas. Respeitar a privacidade dos outros é fundamental para uma convivência saudável no ambiente digital. Lembre-se que, uma vez na internet, é difícil ter controle sobre quem vê ou compartilha suas imagens.



Oriente seus Amigos sobre Privacidade



Conversas em Grupo

Discuta privacidade online com seus amigos e desenvolvam estratégias para proteção mútua.

Combinados de Turma

Estabeleça acordos com seus colegas sobre o compartilhamento responsável de conteúdo nas redes sociais.



Alerta de Riscos

Avise discretamente amigos que estejam compartilhando informações sensíveis sobre os possíveis perigos.

Compartilhe este Guia

Divulgue estas orientações para promover a segurança digital entre seu círculo social.



Utilizando Listas de Contatos nas Redes Sociais

A maioria das redes sociais permite criar grupos ou listas de contatos para gerenciar quem pode ver seu conteúdo. Você pode **criar listas separadas para familiares, amigos próximos e colegas de escola**.

Ao publicar, selecione qual lista terá acesso à informação. Isso permite **compartilhar momentos pessoais apenas com pessoas próximas**, mantendo um perfil mais genérico para outros contatos. O uso eficiente dessas listas é essencial para uma presença digital segura.

Benefícios das listas de contatos

- Personalização do conteúdo para diferentes públicos
- Maior controle sobre sua privacidade online
- Redução de riscos de exposição indesejada
- Organização mais eficiente da sua rede de contatos

Como criar e gerenciar listas nas principais redes sociais

Cada plataforma tem seu próprio sistema. O **Instagram** oferece "Melhores Amigos" para stories exclusivos. No **Facebook**, crie listas como "Família" ou "Escola". No **Twitter (nome atual "X")**, as listas organizam quem você segue, enquanto no **TikTok**, controle quem vê seus vídeos.

Revise suas listas periodicamente e remova contatos quando necessário. Pessoas com quem você não interage ou não conhece bem não precisam acessar informações privadas.



Configurando publicações para listas específicas

Antes de publicar, pergunte-se: "Quem deveria ver isso?". Use as opções de visibilidade como "Público", "Amigos" ou listas personalizadas para cada publicação.

Limite informações sensíveis e fotos pessoais a listas restritas. Para conteúdos gerais, opte por audiências mais amplas. Essa abordagem seletiva reduz significativamente os riscos de exposição indevida.

Crie diferentes níveis de compartilhamento entre seus contatos. Com o tempo, esse hábito se torna natural e fortalece sua segurança digital.

Senhas e Autenticação: Visão Geral

Suas senhas são as chaves do seu mundo digital. A gestão adequada delas e a utilização de métodos de autenticação mais avançados são fundamentais para proteger suas informações pessoais.

- **Senhas Únicas: Não use a mesma senha para todas as suas contas online.** Assim como não se deve utilizar a mesma chave para sua casa, armário escolar e o diário.
- **Autenticação em Dois Fatores: Adicione uma camada extra de segurança às suas contas** utilizando não apenas senhas, mas também códigos enviados ao seu celular ou e-mail.
- **Gerenciadores de Senhas: Utilize ferramentas que armazenem suas senhas com segurança,** permitindo que você use senhas mais complexas sem precisar memorizá-las.
- **Autenticação Biométrica: Use sistemas modernos que utilizam características únicas do seu corpo,** como impressão digital ou reconhecimento facial, para verificar sua identidade.





Criando Senhas Fortes



O que torna uma senha forte?

- Mínimo de 12 caracteres;
- Letras maiúsculas e minúsculas;
- Números e símbolos especiais;
- Sem palavras comuns ou dados pessoais;
- Única para cada serviço.

Método eficaz

Transforme uma frase memorável em senha:

Frase: “Eu amo estudar ciências na escola!”

Senha: “Eu4m0E\$tC13nc1a\$nE\$c0!4!”

Crie senhas complexas que você consegue lembrar facilmente.

Guia de Segurança da Informação para ESTUDANTES



**SEGURANÇA
DIGITAL**
EDUCAÇÃO DO PARANÁ



PARANÁ
GOVERNO DO ESTADO
SECRETARIA DA EDUCAÇÃO