DICAS PARA

SEGURANÇA DIGITAL

Aline Oliveira Nyari
Advogada Especialista em Direito Digital & LGPD

INTRODUÇÃO

Oi! Se você chegou até aqui, é porque em algum momento já ficou na dúvida se estava realmente segura usando as redes sociais, né?

Seja no **Instagram, Facebook, TikTok** ou qualquer outra plataforma, a verdade é que estamos cada vez mais expostos.
E sim, os riscos são reais — desde o vazamento de dados até golpes financeiros e invasões de contas.

Mas calma, não tô aqui pra te assustar. Muito pelo contrário! Meu objetivo com esse e-book é descomplicar a segurança digital pra você. Nada de termos técnicos difíceis ou explicações que parecem manuais de TI.
Aqui, a ideia é te mostrar, de forma simples e direta, como proteger seus dados e usar as redes sociais com mais tranquilidade e consciência.
Você não precisa ser hacker ou especialista em tecnologia pra se proteger — só precisa de informação certa, prática e atualizada.
E é exatamente isso que eu vou te entregar por aqui.

Bora juntos transformar a forma como você usa a internet?

ESTRATÉGIA DE BLINDAGEM DIGITAL

Adote este método simples e eficaz:

REMOVER:
e-mails vazados, senhas fracas, telefones públicos no perfil.

PROTEGER:
ativar 2FA via app, atualizar dados, criar e-mails seguros.

GUARDAR E MONITORAR: códigos de backup, alertas de login e apps conectados.


CAPÍTULO I
SEGURANÇA NO INSTAGRAM

Como proteger sua conta

A primeira coisa que eu sempre falo é:
a sua senha é a sua primeira linha de defesa, então nada de usar “123456” ou o nome do seu pet, tá?
Cria uma senha forte, com letras maiúsculas, minúsculas, números e símbolos.
E o mais importante: **ativa a autenticação em dois fatores (2FA).**
É rapidinho e aumenta MUITO a segurança da sua conta.

Pra ativar, é só ir nas **configurações > Segurança > Autenticação de dois fatores e seguir o passo a passo.**

Isso faz com que, mesmo que alguém descubra sua senha, ainda precise de um código que vai pro seu celular. Um a zero pra você!

Ah! E **cuidado** com aplicativos de terceiros que pedem acesso à sua conta.
Muitos deles parecem inofensivos, mas podem estar coletando suas informações.

Identificando perfis falsos

Identificando perfis falsos
Eles estão por toda parte: perfis falsos que imitam pessoas conhecidas ou marcas famosas. E o objetivo quase sempre é o mesmo: enganar, aplicar golpes ou coletar dados. Fique de olho em sinais como:

- **Fotos de perfil genéricas ou sem rosto.**
- **Poucas postagens e seguidores.**
- **Mensagens suspeitas com links estranhos.**
- **Promessas de dinheiro fácil ou sorteios milagrosos.**

Recebeu algo estranho?
Não clique em links e não compartilhe informações.
Se for **golpe**, denuncie o perfil direto no app. É simples, rápido e ajuda a proteger outras pessoas também.

Gerenciando permissões de acesso

Sabe aqueles joguinhos, apps de edição de fotos ou extensões que você conectou no Instagram? Pois é... muitos deles continuam tendo acesso mesmo depois que você para de usar.
Entra lá em:
Configurações > Segurança > Aplicativos e sites e faz uma limpa.
Remove tudo o que você não usa mais.

Evitando golpes e ataques

Os golpistas estão cada vez mais criativos. Te mandam mensagens dizendo que você ganhou um prêmio, que sua conta será verificada, ou até fingem ser um amigo pedindo ajuda. Mas o objetivo sempre é o mesmo: te enganar pra conseguir dados, dinheiro ou acesso à sua conta.
Dicas práticas pra não cair nessa:
Nunca informe códigos por mensagem.
Desconfie de links encurtados ou mal escritos.
Cuidado com mensagens que apelam pro emocional ou urgência.
Se algo parecer estranho, confirme com a pessoa por outro canal.
E lembre-se: o Instagram nunca vai te pedir senha ou código por DM.

CAPÍTULO 2

SEGURANÇA NO FACEBOOK

Configurações de privacidade eficientes

O **Facebook** é uma verdadeira mina de ouro de dados — e se você não tiver cuidado, acaba mostrando mais do que gostaria. A boa notícia? Dá pra ajustar isso rapidinho.

Vai em:

Configurações e Privacidade > Verificação de Privacidade.

Ali, o próprio Facebook te guia passo a passo pra ajustar quem pode ver suas postagens, quem pode te adicionar como amigo e até como suas informações são usadas fora da plataforma.

E **revise se seu telefone, e-mail ou outras infos estão visíveis publicamente** — o ideal é ocultar ou deixar visível apenas pra você.

Dicas para evitar vazamento de informações

Parece bobo, mas tem gente que posta tudo:

localização, rotina, fotos dos filhos, CPF (sim, já vi isso!).
A gente esquece que qualquer informação pode ser usada por golpistas.

Por isso:

- Evite postar em tempo real que está viajando.
- Não compartilhe fotos de documentos ou boletos.
- Cuidado com comentários em promoções e sorteios.
- Reveja o que seus amigos podem marcar você — dá pra ativar a aprovação manual de marcações!

Menos é mais quando o assunto é segurança.

CAPÍTULO 3

SEGURANÇA NO TIKTOK

Fazendo um uso seguro do aplicativo

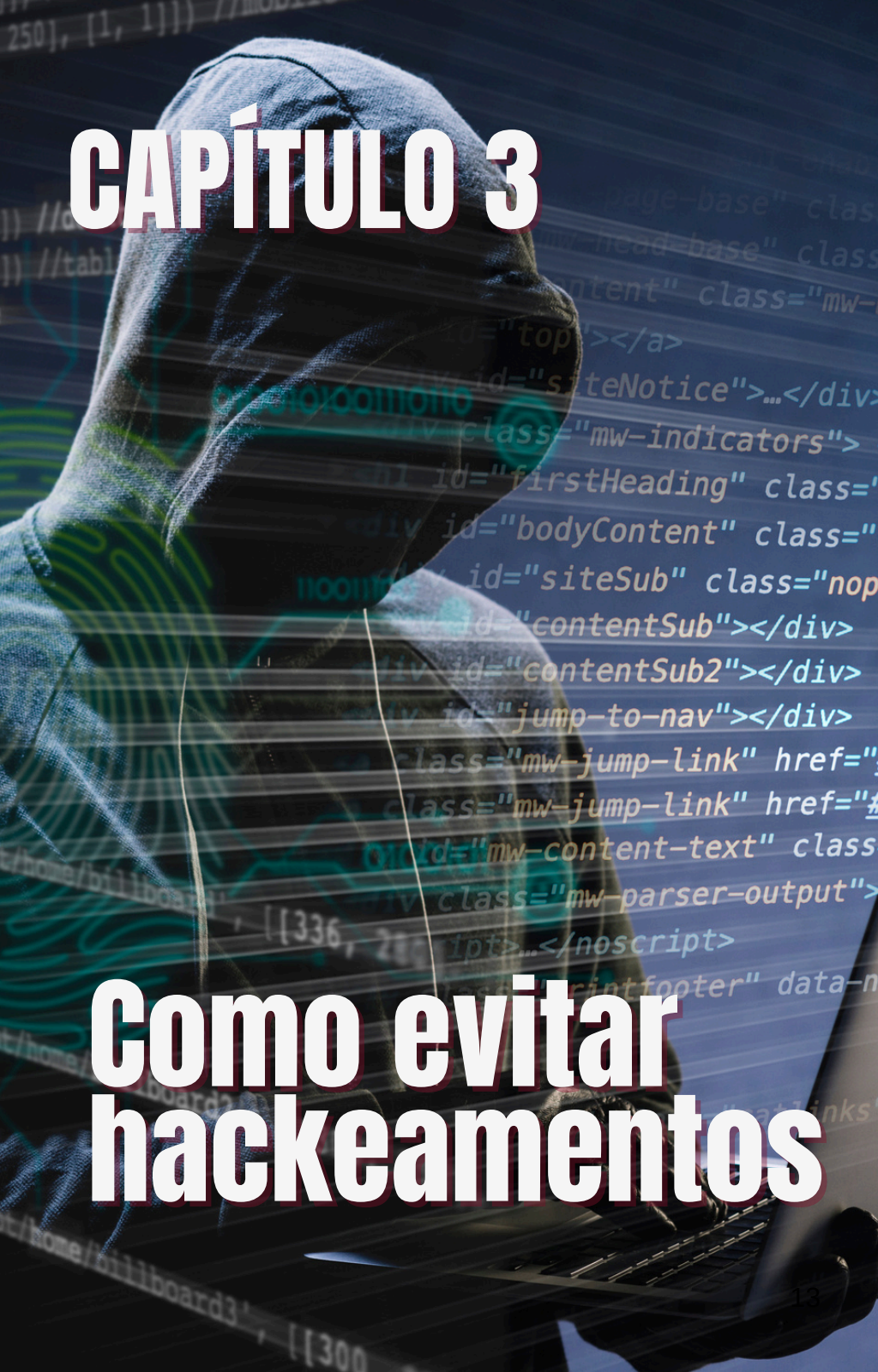
O TikTok é divertido, viciante e... um pouquinho perigoso se você não souber usar com atenção. O primeiro passo é garantir que sua conta esteja protegida com senha forte e autenticação em dois fatores.

Depois, é importante ficar de olho nos desafios virais perigosos, links enviados por DM e mensagens de contas suspeitas. Use a plataforma com consciência — **se algo parece estranho, provavelmente é.**

Configurando a privacidade do seu perfil

Você pode deixar seu perfil privado se quiser um uso mais restrito. Vai em Configurações > Privacidade e ativa a opção.
Outras dicas que eu sigo:

- **Bloqueio de mensagens diretas de desconhecidos.**
- **Aprovação de seguidores.**
- **Controle de quem pode comentar, ver seus vídeos ou usar seus sons.**



CAPÍTULO 3

Como evitar hackeamentos

Esse é o pesadelo de muita gente:

ter a conta invadida e perder tudo. Mas sabe o que é pior?

A maioria dos casos acontece por falhas simples que poderiam ser evitadas.

Aqui vão 20 regras de ouro pra você se proteger:

DICA 1: Senha forte e única

Nunca use a mesma senha em mais de uma rede social. Use gerenciadores de senha se for difícil lembrar, tipo o LastPass, Bitwarden ou 1Password.

DICA 2: Ative a autenticação de dois fatores (2FA):

- Ative o 2FA em todas as contas importantes (e-mail, redes sociais, bancos).
- Prefira apps autenticadores como Google Authenticator ou Authy.
- Evite usar SMS, pois é vulnerável a clonagem de chip.

DICA 3: Proteja seu e-mail principal como se fosse sua chave-mestra:

- Ative 2FA.
- Revise acessos de apps conectados.
- Crie uma conta só para cadastros secundários.
- No Gmail: Configurações > Segurança > Verificação em duas etapas.

DICA 4: Nunca reutilize senhas em serviços diferentes:

- Utilize um gerenciador de senhas para armazenar e gerar credenciais exclusivas.
- Crie senhas aleatórias para cada serviço.

DICA 5: Cuidado com phishing (e-mails ou mensagens falsas):

- Verifique o remetente.
- Não clique em links suspeitos.
- Passe o mouse sobre o link antes de clicar para ver o destino.
- Denuncie no Outlook ou Gmail como "Phishing".

DICA 6: Mantenha seu sistema operacional e aplicativos atualizados:

- Ative atualizações automáticas no Windows/macOS/iOS/Android.
- Atualize apps frequentemente pela loja oficial (Google Play ou App Store).

DICA 7: Não compartilhe dados sensíveis por e-mail ou mensageiros:

- Use criptografia (ex: ProtonMail para e-mails sensíveis).
- Evite compartilhar senhas, documentos pessoais e informações bancárias.

DICA 8: Tenha um antivírus confiável instalado (inclusive no celular):

- Recomendado: Kaspersky, BitDefender, Norton.

Mantenha o antivírus atualizado

DICA 9: Use VPN em redes Wi-Fi públicas:

- Utilize VPNs confiáveis como NordVPN ou ProtonVPN.
- Nunca acesse apps bancários em Wi-Fi público sem VPN.

DICA 10: Cuidado com QR Codes e links encurtados:

- Use apps como Kaspersky QR Scanner para escanear com segurança.
- Prefira digitar URLs manualmente.

DICA 11: Revise acessos autorizados em suas contas Google e Outlook:

- Google: myaccount.google.com > Segurança > Dispositivos e apps com acesso.
- Outlook: account.live.com > Privacidade > Apps e serviços conectados.

DICA 12: Ative alertas de login suspeito:

- No Google, ative notificações de atividade de login.
- No Outlook, configure alertas de acesso incomum.

DICA 13: Verifique a privacidade das suas redes sociais (Instagram/TikTok):

- Instagram: Configurações > Privacidade > Conta privada / Restringir mensagens.
- TikTok: Configurações > Privacidade > Controle quem pode ver, comentar ou interagir com você.

DICA 14: Não salve senhas no navegador:

- Utilize gerenciadores de senhas seguros.
- Navegadores como Chrome são alvos frequentes de roubo de credenciais

DICA 15: Limpe cookies e cache regularmente:

- No navegador: Configurações > Privacidade > Limpar dados de navegação.

DICA 16: Atente-se a apps suspeitos com permissões excessivas:

- Revise permissões no Android: Configurações > Apps > Permissões.
- No iOS: Ajustes > Privacidade.

DICA 17: Tenha um plano de resposta a incidentes:

- Tenha backup de arquivos importantes.
- Salve contatos de suporte de bancos, operadoras e serviços digitais.

DICA 18: Proteja câmeras e microfones:

- Tampe a câmera do notebook.
- Desabilite microfone quando não estiver em uso nas configurações do sistema.

DICA 19: Use navegadores seguros e extensões de proteção:

- Use Brave ou Firefox.
- Extensões recomendadas: HTTPS Everywhere, uBlock Origin, Privacy Badger.
-

DICA 20: Eduque-se continuamente sobre segurança digital:

- Acompanhe portais como Tecmundo, CISO Advisor, The Hacker News.
- Participe de cursos gratuitos e certificações (Google, NIC.br, Udemy).

CONCLUSÃO

A segurança digital é uma jornada.

Pequenas mudanças em seus hábitos podem evitar **grandes prejuízos.**

Adote essas medidas como rotina e **ajude** outras pessoas a se protegerem também.

Salve e compartilhe este e-book e consulte sempre que quiser revisar sua **segurança online!**

Até o próximo conteúdo!

Aline Oliveira
Advogada | Especialista em Direito Digital e LGPD

@alineoliveyra.adv