UDESC | FAED | PPGINFO

COMO PROTEGER SEUS DADOS NAS REDES SOCIAIS

OUTUBRO 2023

Quando o assunto é privacidade e segurança cibernética, as diretrizes se concentram em boas práticas que visam proteger os usuários online. Estas práticas podem ser aplicadas em diversas plataformas de redes sociais e aplicativos online.

É importante ressaltar que as políticas de privacidade podem mudar ao longo do tempo, portanto, é fundamental que os usuários estejam cientes dessas mudanças e façam ajustes em suas configurações de acordo com as diretrizes mais recentes fornecidas pelas redes sociais em questão.

Além disso, é recomendável buscar informações sobre privacidade online a partir de fontes confiáveis e atualizadas.

Este material foi elaborado como produto da dissertação de mestrado profissional:

Percepções sobre a privacidade nas redes sociais *online*
dos estudantes da Universidade do Estado de Santa Catarina

Do Programa de Pós-Graduação em em Gestão da Informação (PPGInfo) do
Centro de Ciências Humanas e da Educação (FAED) da
Universidade do Estado de Santa Catarina (UDESC)
Orientadora: Profª Drª Claudiane Weber

Juliana Sant'Anna

Mestre em Ciência da Informação pela UDESC
Bacharel em Ciência da Computação pela UFSC

Os dados da pesquisa

87%

dos estudantes que responderam a pesquisa passam mais de 2 horas por dia conectados nas redes sociais

100%

se preocupam com privacidade online, mas apena 51% já alterou suas configurações de privacidade

84%

não lêem os termos de uso e políticas de privacidade da redes sociais que utilizam

A seguir são apresentadas 10 dicas para proteger seus dados nas redes sociais.

Essas dicas podem ajudar a proteger sua privacidade online, mas lembre-se de que a segurança dos seus dados é uma responsabilidade contínua.

Ficar atento, ter um olhar crítico e tomar medidas proativas para proteger suas informações pessoais é essencial para manter sua segurança online.

01

Controle suas configurações de privacidade

Familiarize-se com as configurações de privacidade de cada rede social que você utiliza. Ajuste essas configurações para controlar quem pode ver suas postagens, suas informações pessoais e quem pode entrar em contato com você. Entre no seu perfil e procure por configurações (settings) e privacidade (privacy).

02 Utilize senhas fortes

Crie senhas longas e complexas, com pelo menos 8 caracteres e uma combinação de letras maiúsculas, minúsculas, números e caracteres especiais.

Esse tipo de senha não é descoberta facilmente por *crackers*, programas que utilizam poder computacional para quebrar senhas.

Além disso, tenha senhas diferentes para cada rede social para evitar o acesso não autorizado em massa, caso uma senha seja comprometida.

03 Ative a autenticação de dois fatores (2FA)

A autenticação de dois fatores, do inglês two-factor authentication (2FA) ou verificação em duas etapas é um método que quando habilitado, irá solicitar um código extra sempre que um dispositivo (celular ou computador) desconhecido for utilizado para fazer login no aplicativo. Dessa forma, se sua senha for descoberta, ainda assim será necessário saber o código extra para poder acessar a sua conta.

Portanto, sempre que possível, ative esta opção para adicionar uma camada extra de segurança aos acessos de seus aplicativos.

04

Esteja ciente do que você curte ou comenta

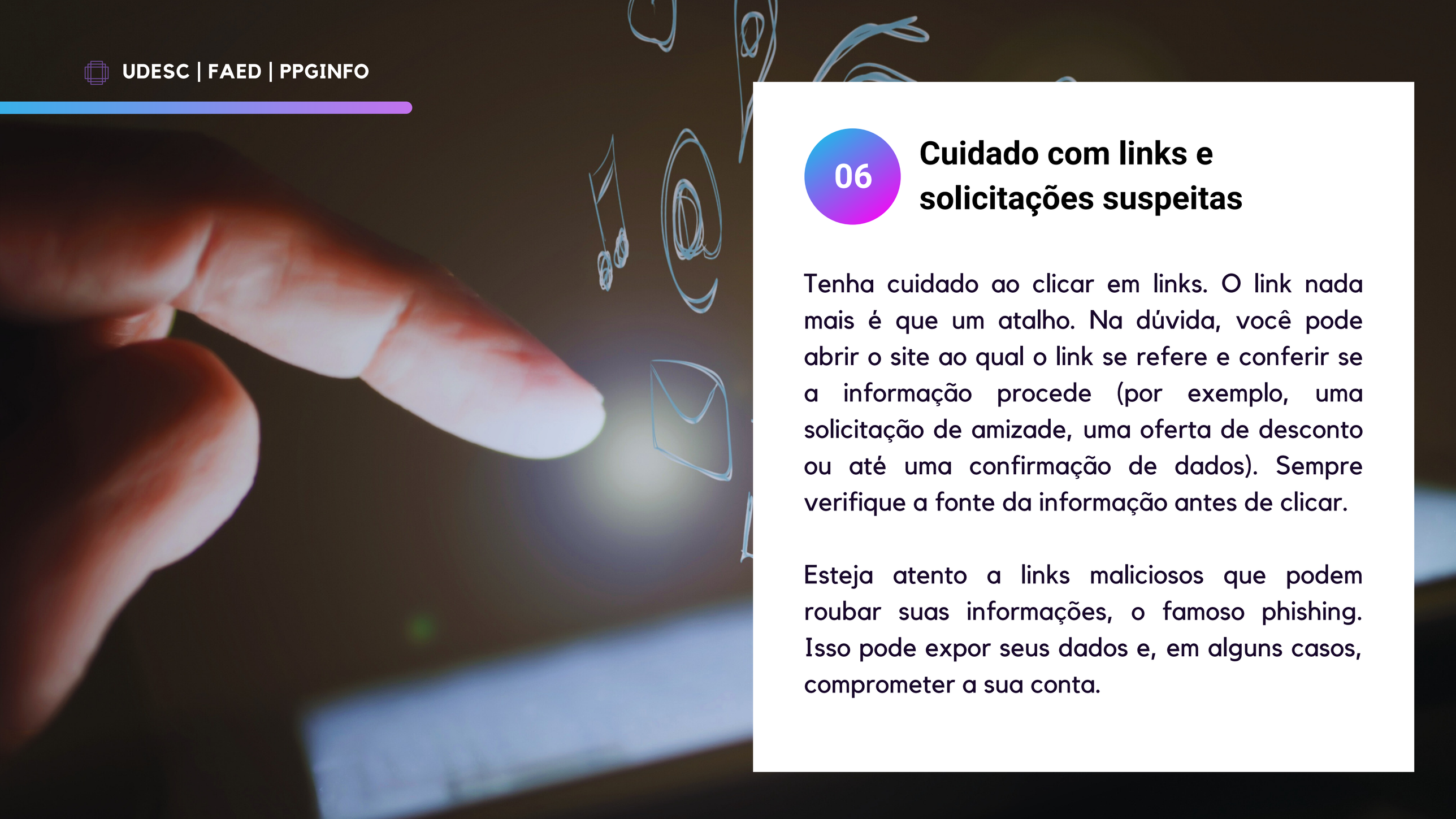
Suas interações podem revelar informações sobre seus interesses e crenças.
Pense duas vezes antes de curtir ou comentar em postagens controversas.
Lembre-se que a cada interação você fornece dados para que o algoritmo possa utilizar para filtrar dados e direcionar suas próximas informações.

05

Evite a geolocalização em tempo real

Verifique se a opção de localização está ativa. Desabilite a geolocalização em tempo real, especialmente em fotos e postagens. Isso pode revelar sua localização atual, permitindo que as pessoas saibam onde você está a todo momento.

Além disso, informações como seu endereço e onde você trabalha podem ser deduzidas a partir da frequência de acessos a mesma localização.



06

Cuidado com links e solicitações suspeitas

Tenha cuidado ao clicar em links. O link nada mais é que um atalho. Na dúvida, você pode abrir o site ao qual o link se refere e conferir se a informação procede (por exemplo, uma solicitação de amizade, uma oferta de desconto ou até uma confirmação de dados). Sempre verifique a fonte da informação antes de clicar.

Esteja atento a links maliciosos que podem roubar suas informações, o famoso phishing. Isso pode expor seus dados e, em alguns casos, comprometer a sua conta.

07 Mantenha-se informado sobre quais dados são coletados

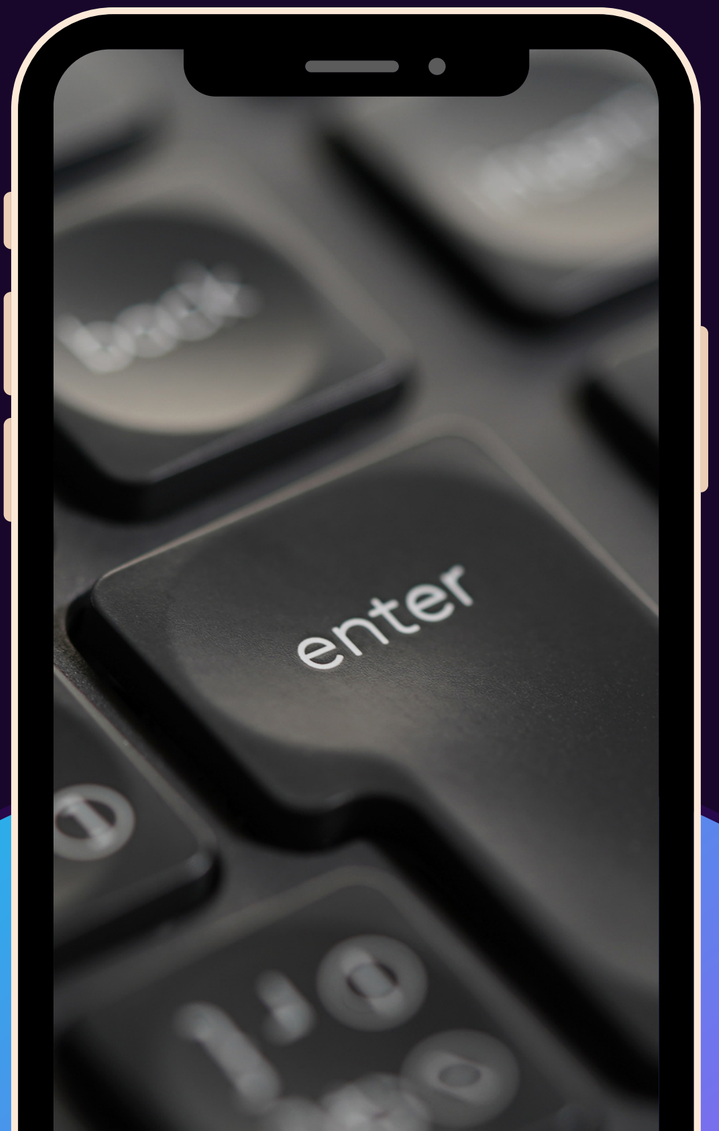
Procure identificar, nos termos de uso ou políticas de privacidade das redes sociais que você utiliza, quais dados são coletados, como são utilizados e com quem são compartilhados. A Lei Geral de Proteção de Dados (LGPD) garante que as empresas disponibilizem essas informações.

Revise regularmente suas configurações de privacidade, ou pelo menos quando receber aviso de que as políticas de privacidade ou termos de uso foram alterados.

08

Evite navegar na internet com seu e-mail aberto

Quando voce navega na internet no mesmo navegador em que seu e-mail está aberto (por exemplo o gmail), sua navegação pode estar sendo relacionada a sua conta de e-mail. Opte sempre por utilizador o navegador em modo anônimo ou modo privado.



09 Entenda como funcionam tecnologias como *cookies* e *web beacons*

Você não precisa dominar a inteligência artificial ou saber construir um aplicativo. Mas é importante conhecer o funcionamento e principalmente as consequências das principais tecnologias utilizadas atualmente.

Os *cookies* são arquivos utilizados para salvar sua identidade, seus acessos e suas preferências. Portanto, se você não deseja ser lembrado em um site, não aceite os *cookies* do mesmo.

Os *web beacons* (ou *web bugs*) são imagens invisíveis utilizadas em *sites* e *e-mails* para contabilizar os acessos a esses recursos.

10 Esteja no controle

Por fim, esteja sempre no controle dos seus dados, afinal é a sua identidade digital que está em risco. Seus acessos, buscas e interações formam seu perfil online, deixando um rastro digital que não é facilmente apagado.

As informações, mesmo depois de retiradas das redes sociais, permanecem nos servidores de forma oculta e ainda podem ser acessadas e utilizadas para inferências por algoritmos de Inteligência Artificial (IA).

Ao se sentir lesado, informe-se sobre como a Lei Geral de Proteção de Dados (LGPD) pode proteger seus direitos.

CONTATO

https://www.udesc.br/faed/ppginfo

juliana.santanna@udesc.br

+55 48 3664-8500

Av. Madre Benvenuta, 2007
Florianópolis, SC, Brasil