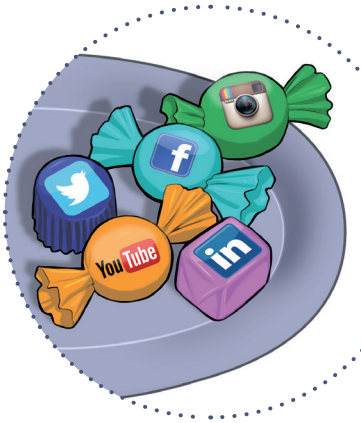
Publicação cert.br

Cartilha de Segurança para Internet

Fascículo Redes Sociais

https://cartilha.cert.br/

nic.br cgi.br



O acesso às redes sociais já está incorporado ao cotidiano de grande parte dos usuários da Internet e, muito provavelmente, do seu.

As redes sociais possuem características que as diferenciam dos outros meios de comunicação, como:

- ✓ a facilidade de acesso
- ✓ a rápida velocidade com que as informações se propagam
- ✓ a grande quantidade de pessoas que elas conseguem atingir, de diferentes faixas etárias
- ✓ a grande quantidade de informações pessoais que apresentam
- ✓ a dificuldade de exclusão e controle sobre as informações divulgadas
- ✓ o tempo em que as informações ficam disponíveis
- ✓ o alto grau de confiança que os usuários costumam depositar entre si
- ✓ as novas oportunidades de negócios que trazem

Além disso as redes sociais estão presentes nos mais diversos meios, como pessoal, profissional, econômico, político e jornalístico.

Todas essas características somadas a popularidade dos dispositivos móveis fizeram com que as redes sociais chamassem a atenção, também, de pessoas mal-intencionadas.

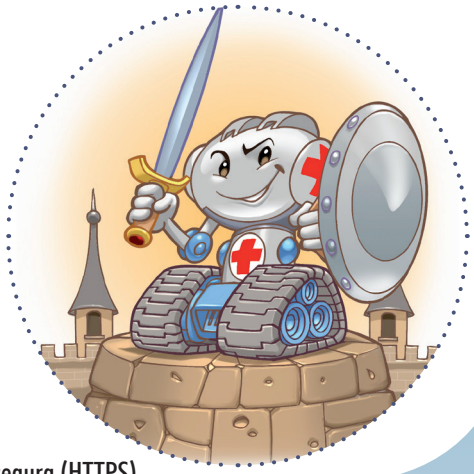
Por isso, para usar as redes sociais de forma segura, é muito importante que você esteja ciente dos riscos que elas podem representar e possa, assim, tomar medidas preventivas para evitá-los.

Redes Sociais:
Curta com moderação

Riscos *principais*

- ✓ **Contato com pessoas mal-intencionadas:** qualquer um pode criar um perfil falso e, sem que saiba, você pode ter na sua lista de contatos pessoas com as quais jamais se relacionaria no dia a dia
- ✓ **Furto de identidade:** assim como você pode ter um impostor na sua lista de contatos, também pode acontecer de alguém tentar se passar por você e criar um perfil falso
- ✓ **Invasão de perfil:** seu perfil pode ser invadido por meio de ataques de força bruta, do acesso a páginas falsas ou do uso de computadores infectados
- ✓ **Uso indevido de informações:** aquilo que você divulga pode vir a ser mal-interpretado e usado contra você
- ✓ **Invasão de privacidade:** quanto maior a sua rede de contatos, maior é o número de pessoas que possui acesso ao que você divulga, e menores são as garantias de que suas informações não serão repassadas
- ✓ **Recebimento de mensagens maliciosas:** alguém pode lhe enviar uma mensagem contendo boatos ou induzi-lo a clicar em um *link* que o fará instalar um código malicioso ou acessar uma página Web comprometida
- ✓ **Acesso a conteúdos impróprios ou ofensivos:** como não há um controle imediato sobre o que as pessoas divulgam, pode ocorrer de você se deparar com mensagens ou imagens que contenham pornografia, violência ou que incitem o ódio e o racismo
- ✓ **Danos à imagem e à reputação:** calúnia e difamação podem rapidamente se propagar, jamais serem excluídas e causarem grandes danos às pessoas envolvidas

Cuidados
a serem tomados



Proteja o seu perfil:

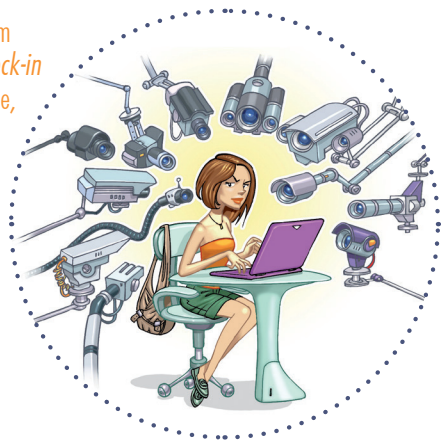
- ✓ Acesse o *site* da rede social sempre usando conexão segura (HTTPS)
- ✓ Seja cuidadoso ao usar e ao elaborar as suas senhas
  - use senhas longas, compostas de diferentes tipos de caracteres
  - não use dados pessoais, como nome, sobrenome e datas
  - evite usar a mesma senha para acessar diferentes *sites*
- ✓ Habilite a notificação de *login* e a verificação em duas etapas, sempre que estes recursos estiverem disponíveis
- ✓ Evite cadastrar perguntas de segurança que possam ser facilmente descobertas
- ✓ Procure cadastrar um *e-mail* de recuperação que você acesse regularmente
- ✓ Solicite o arquivo com suas informações ou verifique o registro de atividades, caso desconfie que seu perfil tenha sido indevidamente usado
- ✓ Use opções como silenciar, bloquear e denunciar, caso identifique abusos

Mantenha seu computador e dispositivos móveis seguros:

- ✓ Mantenha todos os programas instalados com as versões mais recentes
- ✓ Aplique todas as atualizações disponíveis
- ✓ Utilize e mantenha atualizados mecanismos de segurança, como *antispam*, antivírus e *firewall* pessoal
- ✓ Desconfie de mensagens recebidas, mesmo que tenham sido enviadas por conhecidos
- ✓ Seja cuidadoso ao acessar *links* reduzidos
  - use complementos que permitam que você expanda o *link* antes de clicar sobre ele

Proteja a sua privacidade:

- ✓ Considere que você está em um local público, que tudo que você divulga pode ser lido ou acessado por qualquer pessoa
- ✓ Pense bem antes de divulgar algo, pois não é possível voltar atrás
- ✓ Use as configurações de privacidade oferecidas pelos *sites* e seja o mais restritivo possível
- ✓ Mantenha seu perfil e seus dados privados
- ✓ Restrinja o acesso ao seu endereço de *e-mail*
- ✓ Seja cuidadoso ao aceitar seus contatos e ao se associar a grupos
- ✓ Não confie na promessa de anonimato oferecida por algumas redes sociais e aplicativos
  - de acordo com as informações divulgadas é possível inferir a sua identidade e de outras pessoas
- ✓ Seja cuidadoso ao fornecer a sua localização
  - cuidado ao divulgar fotos e vídeos, pois ao observar onde eles foram gerados pode ser possível deduzir a sua localização
  - não divulgue planos de viagens e nem por quanto tempo ficará ausente da sua residência
  - ao usar redes sociais baseadas em geolocalização, procure fazer *check-in* apenas em locais movimentados e, de preferência, ao sair do local
  - cuidado ao confirmar sua presença em eventos públicos organizados via redes sociais



Respeite a privacidade alheia:

- ✓ evite falar sobre as ações, hábitos e rotina de outras pessoas
- ✓ não divulgue, sem autorização, imagens em que outras pessoas apareçam
- ✓ não divulgue mensagens ou imagens copiadas do perfil de pessoas que restrinjam o acesso
- ✓ tente imaginar como a outra pessoa se sentiria ao saber que aquilo está se tornando público

Proteja seus filhos:

- ✓ Informe seus filhos sobre os riscos de uso das redes sociais
- ✓ Respeite os limites de idade estipulados pelos *sites*
- ✓ Não exponha excessivamente seus filhos
  - muitos pais criam perfis em nome dos filhos e postam sobre eles ou como se fossem eles. Isso pode desagradar e confundir as crianças
  - evite constranger seus filhos, divulgando fotos ou comentários que possam embaraçá-los
  - seja cuidadoso ao divulgar imagens de seus filhos. O que para você pode ser algo inocente, para outras pessoas pode ter uma conotação diferente
- ✓ Oriente-os:
  - para não se relacionarem com estranhos e nunca fornecerem informações pessoais
  - para não divulgarem informações sobre hábitos familiares e nem de localização (atual ou futura)
  - para não marcarem encontros com estranhos
  - sobre os riscos de uso da *webcam* e que ela não deve ser usada para se comunicar com estranhos
  - para usar opções como silenciar, bloquear e denunciar, caso alguém os esteja incomodando

Proteja a sua vida profissional:

- ✓ Cuide da sua imagem profissional
- ✓ Ao usar redes sociais profissionais procure ser formal e evite tratar de assuntos pessoais
- ✓ Antes de postar algo avalie se, de alguma forma, aquilo pode atrapalhar a sua carreira
- ✓ Cuidado ao permitir que seus filhos usem o mesmo computador ou dispositivo móvel que você usa para tratar de assuntos profissionais
  - alguns aplicativos, como jogos, divulgam automaticamente nas redes sociais, dependendo das configurações
- ✓ Verifique se sua empresa possui um código de conduta e evite divulgar detalhes sobre o seu trabalho
- ✓ Oriente seus familiares para não divulgarem informações sobre a sua empresa e vida profissional

Proteja a sua empresa:

- ✓ Crie um código de conduta
- ✓ Invista em treinamento e em campanhas de conscientização
- ✓ Informe aos funcionários sobre as regras de acesso durante o expediente e sobre o comportamento esperado, referente à divulgação de informações profissionais e à emissão de opiniões que possam comprometer a empresa
- ✓ Cuide da imagem. Observe a opinião de clientes e consumidores ou qualquer ação que envolva o nome da empresa, para que seja capaz de tomar atitudes em tempo de evitar algum dano

Consulte a **Cartilha de Segurança** para a Internet para mais detalhes sobre os riscos de uso das redes sociais e os cuidados a serem tomados:

https://cartilha.cert.br/privacidade/#11.1

INTERNET SEGURA.BR

Precisa conversar sobre o uso seguro da Internet com **crianças e adolescentes**? O **Portal Internet Segura** apresenta uma série de iniciativas e de recomendações sobre esse assunto, confira!

http://internetsegura.br/

cert.br

Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

O CERT.br é o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Desde 1997, o grupo é responsável por tratar incidentes de segurança envolvendo redes conectadas à Internet no Brasil. O Centro também desenvolve atividades de análise de tendências, treinamento e conscientização, com o objetivo de aumentar os níveis de segurança e de capacidade de tratamento de incidentes no Brasil. Mais informações em https://www.cert.br/.

nic.br

Núcleo de Informação e Coordenação do Ponto BR

O Núcleo de Informação e Coordenação do Ponto BR - NIC.br (http://www.nic.br/) é uma entidade civil, sem fins lucrativos, que implementa as decisões e projetos do Comitê Gestor da Internet no Brasil. São atividades permanentes do NIC.br coordenar o registro de nomes de domínio - Registro.br (http://www.registro.br/), estudar e tratar incidentes de segurança no Brasil - CERT.br (https://www.cert.br/), estudar e pesquisar tecnologias de redes e operações - CEPTRO.br (http://www.ceptro.br/), produzir indicadores sobre as tecnologias da informação e da comunicação - CETIC.br (http://www.cetic.br/) e abrigar o escritório do W3C no Brasil (http://www.w3c.br/).

cgi.br

Comitê Gestor da Internet no Brasil

O Comitê Gestor da Internet no Brasil coordena e integra todas as iniciativas de serviços Internet no país, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados. Com base nos princípios de multilateralidade, transparência e democracia, o CGI.br representa um modelo de governança multissetorial da Internet com efetiva participação de todos os setores da sociedade nas suas decisões. Uma de suas formulações são os 10 Princípios para a Governança e Uso da Internet (http://www.cgi.br/principios). Mais informações em http://www.cgi.br/.

março / 2017