SEGURANÇA NAS REDES SOCIAIS

DICAS GERAIS

SUPESP-CE
Superintendência de Pesquisa e Estratégia de Segurança Pública

CEARÁ
GOVERNO DO ESTADO
SECRETARIA DA SEGURANÇA PÚBLICA E DEFESA SOCIAL

EXPEDIENTE CARTILHA SEGURANÇA NAS REDES SOCIAIS

GOVERNADOR DO ESTADO DO CEARÁ

Camilo Sobreira de Santana

SECRETÁRIO DA SEGURANÇA PÚBLICA E DEFESA SOCIAL (SSPDS/CE)

Sandro Luciano Caron de Moraes

SUPERINTENDENTE DE PESQUISA E ESTRATÉGIA DE SEGURANÇA PÚBLICA (Supesp/CE)

José Helano Matos Nogueira

DIRETOR DE ESTRATÉGIA EM SEGURANÇA PÚBLICA (Diesp/Supesp)

Anderson Duarte Barboza

DIRETORA DE PESQUISA E AVALIAÇÃO DE POLÍTICAS DE SEGURANÇA PÚBLICA (Dipas/Supesp)

Manuela Chaves Loureiro Cândido

GERENTE DE ESTATÍSTICA E GEOPROCESSAMENTO (Geesp/Supesp)

Franklin de Sousa Torres

AUTOR

José Helano Matos Nogueira

DESIGNER

Juliana Mendes Teixeira de Lima

REVISÃO

Ascom/Supesp

SEGURANÇA NAS REDES SOCIAIS

O que são as redes sociais?

As redes sociais podem ser definidas como:

> ***Estruturas de relacionamento sociais compostas por pessoas ou organizações conectadas por um ou vários tipos de relações, que partilham valores e objetivos comuns.***

As redes sociais nos meios digitais podem operar em diferentes tipos de agrupamentos como, por exemplo, redes de relacionamentos (Facebook, Instagram, WhatsApp, Twitter, Google+, Youtube, MySpace), redes profissionais (LinkedIn, Yammer, Moodle), redes comunitárias (redes sociais em comunidades, bairros, cidades), redes políticas, redes religiosas, redes policiais etc.

RISCOS

- **Contato com pessoas mal-intencionadas.** Qualquer pessoa pode criar um perfil falso e você pode ter na sua lista de contatos pessoas com as quais jamais se relacionaria.
- **Furto de identidade.** Alguém tentar se passar por você criando um perfil falso, a partir de seus dados, com o objetivo de obter vantagens indevidas.
- **Invasão de perfil.** Seu perfil pode ser invadido por pessoas mal intencionadas e *hackers.*
- **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.
- **Engenharia Social.** Técnica por meio da qual uma pessoa procura persuadir outra a executar determinadas ações em proveito próprio ou alheio. É usada por indivíduos para tentar explorar a boa-fé ou abusar da ingenuidade e da confiança de outras pessoas, a fim de aplicar golpes, ludibriar ou obter informações sigilosas ou importantes.
- **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 conteúdo impróprio ou ofensivo.** Como não há um controle imediato sobre o que as pessoas postam, pode ocorrer de você se deparar com textos, imagens e vídeos que contenham crimes como venda de drogas, estelionato, racismo, pornografia infantil e etc.
- **Danos à imagem e à reputação.** Calúnia, injúria e difamação podem se propagar rapidamente e causarem grandes danos às pessoas envolvidas.
- ***Cyberbullying***. Há intimidação sistemática na rede mundial de computadores *(cyberbullying)*, quando se usarem os instrumentos que lhe são próprios para depreciar, incitar a violência, adulterar fotos e dados pessoais com o intuito de criar meios de constrangimento psicossocial.
- ***Sextortion* (Extorsão Sexual).** É a prática de extorquir dinheiro ou favores sexuais de alguém, ameaçando revelar textos, fotos ou vídeos comprometedores de cunho íntimo.

10 DICAS BÁSICAS DE SEGURANÇA

1. Uso de senha. As senhas precisam ser fortes. Uma senha forte é constituída de letras maiúsculas, minúsculas, números e caracteres especiais como "@" e "$" e com pelo menos oito caracteres. Troque sua senha com frequência, especialmente quando acessar as redes em locais públicos como Wi-Fi de aeroportos, bares, restaurantes, cybercafés ou no computador de outra pessoa.

2. Nunca clique em *links* suspeitos. Mesmo que pareçam ser de amigos ou empresas conhecidas.

3. Use a autenticação em duas etapas/dois fatores (2FA). Habilite a notificação de verificação em duas etapas, sempre que estes recursos estiverem disponíveis. A utilização de autenticação em dois fatores é um processo de segurança que exige que os usuários forneçam dois meios de identificação antes de acessarem suas contas e perfis.

4. Sempre encerre a sessão usando sair/desconectar/*logout*. Faça o encerramento da "sessão". Se você não fizer isto, a próxima pessoa que usar o computador pode ter acesso à sua conta.

5. Ajuste as configurações de segurança. Ajustes as configurações de suas redes sociais para que você tenha privacidade. Verifique se qualquer pessoa pode ter acesso a seus dados. Também é importante não expor dados como endereço, telefone, CPF. Só mostre as outras pessoas o que elas precisam realmente saber.

6. Seja cuidadoso ao fornecer a sua localização. Cuidado ao divulgar fotos e vídeos que permitam deduzir a sua localização. Não divulgue planos de viagens e nem por quanto tempo ficará fora da sua residência.

7. Proteja seus filhos. Informe sobre os riscos de uso das redes sociais. Oriente para não se relacionarem com estranhos, nunca fornecerem informações, imagens ou vídeos pessoais. Informe sobre os riscos de uso da *Webcam* e que ela não deve ser usada para se comunicar com estranhos. Não esquecer de conversar com seus filhos sobre o que eles fazem na Internet e nas redes sociais, bem como estabelecer limites de tempo e conteúdo.

8. Use opções como silenciar e bloquear, caso identifique abusos. Usar as opções como silenciar, bloquear e denunciar, sempre que achar necessário ou quando estiver incomodado com alguma atitude de outra pessoa.

9. Atualização dos *Softwares*. Atualizar os *softwares* básicos (Android, iOs, Windows) e aplicativos (Redes Sociais) toda vez que houver solicitação de atualização. Os sistemas operacionais e os aplicativos corrigem suas falhas e vulnerabilidades através das atualizações.

10. Use os canais de denúncia. Sempre que alguém passar dos limites éticos ou que você identifique como sendo uma prática de algum tipo de crime, faça a denúncia nos canais próprios nas redes sociais. No caso de crime, leve os vestígios materiais (*prints* de telas, textos, imagens, vídeos) para delegacia especializada em crimes cibernéticos ou digitais. Caso não haja essa delegacia especializada na sua cidade, então faça a notícia crime na delegacia mais próxima.

REALIZAÇÃO:

SUPESP-CE
Superintendência de Pesquisa e Estratégia de Segurança Pública

CEARÁ
GOVERNO DO ESTADO
SECRETARIA DA SEGURANÇA PÚBLICA E DEFESA SOCIAL