# Segurança em Foco

**CPSI -** Comissão Permanente de Segurança da Informação
**SSI -** Seção de Suporte e Segurança da Informação
**ASCOM -** Assessoria de Comunicação Social e Cerimonial

# Segurança nas REDES SOCIAIS

Edição nº08
Fevereiro/2021

**As redes sociais estão cada vez mais presentes no nosso dia a dia. Facebook, Twitter, Instagram e Whatsapp são alguns exemplos. Através delas, nos comunicamos com amigos, familiares e colegas. Nos relacionamos com pessoas que têm as mesmas afinidades que nós. Crescentemente, também temos usado as redes sociais para nos informar sobre acontecimentos e notícias, divulgar nossa opinião sobre determinado assunto e, até mesmo, dialogar com e cobrar governos e empresas sobre determinado serviço ou produto. Quanto maior a popularidade da rede social, maior o perigo de cair em golpes online praticados por cibercriminosos. Por isso, aprender a navegar com segurança é primordial.**

## Seguem **alguns riscos**:

**Invasão de privacidade:** a medida em que você divulga informações pessoais sua e de pessoas próximas, você pode comprometer a privacidade sua e de seus amigos e familiares. Essas informações podem vir ser usadas contra vocês em algum momento podendo prejudicá-los;

**Perda de controle sobre o conteúdo:** mesmo que você restrinja o acesso às suas contas e use os filtros de privacidade, não há como controlar que suas informações não serão repassadas por aqueles que têm ou tiveram acesso a elas;

**Divulgação de boatos:** hoje em dia as informações circulam numa velocidade espantosa e podem se propagar rapidamente pela rede num pequeno espaço de tempo. Se isso pode ser positivo em alguns casos, também pode ser prejudicial com a divulgação de informações falsas que podem gerar pânico, prejudicar pessoas, empresas e até processos eleitorais;

**Dificuldade em excluir conteúdo:** os conteúdos que são postados na internet e nas mídias sociais nem sempre podem ser excluídos ou ter o acesso controlado. Com isso, uma opinião pessoal ou uma foto que você postar numa rede social pode ali permanecer por um longo período, podendo vir a um dia ser usada contra você;

**Perseguição:** quando temos informações, fotos ou vídeo visíveis para todos nas redes sociais, podemos ser vítimas de um perseguidor. Se não configuramos as privacidades nas redes sociais, qualquer um pode acessar tudo o que é publicado, o que pode se tornar um problema e um risco para nossa integridade.

## Diante destes riscos, podemos tomar os seguintes cuidados:

**1. Seja prudente na divulgação de informações pessoais:** seja cauteloso quando for divulgar informações pessoais nas mídias sociais. Evite fotos que apresentam sua casa com detalhes, compras caras ou aquisições importantes. Criminosos estão online em busca desses perfis. Quanto mais informação você postar, mais fácil será para uma pessoa mal-intencionada ou um criminoso cibernético usar essa informação para roubar sua identidade, acessar seus dados, ou cometer outros crimes como perseguir você e membros de sua família;

**2. Configure e atualize os filtros de privacidade e segurança:** os filtros de privacidade e segurança das mídias sociais são recursos que têm avançado muito nos últimos anos. Procure conhecê-los e usá-los, pois são eles que permitem ajudá-lo a controlar quem pode ver e compartilhar suas informações e o que você posta. Procure sempre revisar periodicamente seus filtros de segurança e ver se estão atualizados;

**3. Proteja sua reputação:** pense antes de postar. Uma vez postado, um conteúdo pode ser reproduzido em larga escala. Isso pode ocorrer mesmo que você não tenha permitido;

**4. Não adicione pessoas que você não conhece:** verifique se a pessoa que lhe adicionou realmente é um conhecido seu. Se você não o conhece, tenha cautela em aceitar o convite de amizade. Alguns perfis falsos são criados, com o objetivo de acessar dados que só seus amigos podem ver;

**5. Não clique em tudo:** compartilhar coisas ou acessar links, vídeos ou coisas do tipo pode ser tentador, mas é preciso cuidado. Esses links podem ter vírus que irão prejudicar sua máquina ou expor suas informações. Ao compartilhar links maliciosos para seus amigos você pode estar contribuindo com a propagação de algum vírus;

**6. Saiba o que você publicou a seu próprio respeito:** uma das formas mais comuns usadas pelos hackers para invadir contas financeiras ou outras é clicando no link "Esqueceu sua senha?" na página de login da conta. Para entrar na sua conta, eles buscam as respostas para suas perguntas de segurança, como seu aniversário, cidade de origem, turma do colégio ou o nome do meio de sua mãe. Se o site permitir, faça as suas próprias perguntas de senha e não as extraia de nenhum material que possa ser encontrado com uma busca rápida;

**7. Cuidado ao fazer login em sites que se autenticam com sua conta do Facebook ou Google:** apesar de facilitar a vida o usuário por não ter que criar mais um usuário e senha, você tem que saber que estes sites obterão acesso ao seu perfil público do Facebook, seu endereço de e-mail, sua localização e outras informações públicas do seu perfil;

**8. Escolha sua rede social com cuidado:** avalie o site que você pretende usar e entenda claramente a política de privacidade. Descubra se o site monitora o conteúdo postado pelos usuários. Você fornecerá informações pessoais para esse site, por isso use os mesmos critérios que usaria para selecionar um site onde você inseriria o seu cartão de crédito.

**Lembre-se de que: ainda que os cibercriminosos sejam muito cuidadosos, está em nossas mãos cuidar da segurança que aplicamos às nossas informações.**

**Fique ligado: no próximo mês, falaremos sobre Clonagem de Whatsapp!**

Tribunal Regional Eleitoral - RN