



Exército Brasileiro

CARTILHA DE SEGURANÇA

*REDES SOCIAIS E APLICATIVOS
DE TROCA DE MENSAGEM*



MENSAGEM INICIAL



As redes sociais e aplicativos de troca de mensagem estão presentes no cotidiano do homem contemporâneo. Essas redes já fazem parte da rotina das pessoas. Portanto, elas estão presentes no controle das finanças, na política e nos noticiários jornalísticos. No Exército Brasileiro não poderia ser diferente, a Instituição e seu público interno (militares e seus familiares), como parte significativa da sociedade moderna, já se encontram completamente “conectados”.

Devido à sua popularidade, e pela facilidade de serem conectadas por meio dos dispositivos móveis, as redes sociais também passaram a chamar a atenção de pessoas mal-intencionadas e de criminosos.

Dessa forma, a elaboração desta Cartilha é uma oportunidade para orientar a família militar quanto aos cuidados mínimos necessários para uma navegação segura pelo ambiente das redes sociais e aplicativos de troca de mensagem, diminuindo os riscos de tornar-se vítima de atores hostis.



ÍNDICE



Assunto	Pag
 Redes sociais e aplicativos de troca de mensagem	3
 Características	4
 Riscos	5
 Proteção pessoal e da família	6
 Práticas perigosas	11
 Segurança das mídias sociais institucionais	12
 Responsabilidade civil e criminal	13
 Referências	15

REDES SOCIAIS E APLICATIVOS DE TROCA DE MENSAGEM



A Internet trouxe muitas mudanças na maneira de as pessoas se relacionarem, sejam entre si ou com instituições, organizações, empresas ou qualquer pessoa conectada à rede mundial de computadores. A comunicação tornou-se mais fácil, rápida e participativa, sendo possível atingir grandes públicos, a longas distâncias, em poucos segundos. Essa facilidade foi impulsionada pela expansão das redes sociais e sua capacidade de interatividade.

Essas ferramentas do mundo moderno criaram nomenclaturas distintas para representar as ligações entre os usuários. Alguns exemplos são “conexões”, “contatos”, “amigos”, “seguidores e fãs”. Esses termos podem ser usados em diferentes momentos para caracterizar uma rede de integração, mas possuem o mesmo significado básico.

Para uma maior interação, as redes sociais criaram os perfis, a fim de permitir que os usuários publiquem seus dados pessoais, suas preferências, sua localização, pessoas que conhecem, pensamentos e sentimentos. Esses “perfis” podem ser considerados como um verdadeiro “diário eletrônico” público do usuário, que facilita a interação das pessoas por gostos, atividades, preferências musicais, afinidades e uma infinidade de possibilidades.

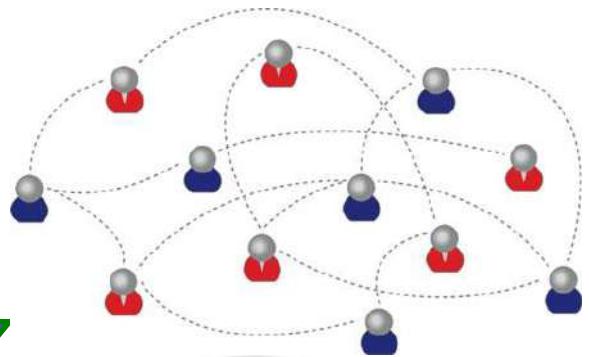
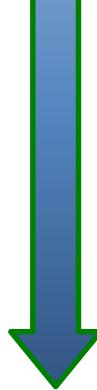
Um grande número de redes sociais e aplicativos de troca de mensagens está à disposição dos usuários na internet, tais como: Facebook, WhatsApp, Twitter, Instagram, Youtube, Snapchat, Telegram, Messenger, Linkedin e Viber, dentre outros.



CARACTERÍSTICAS



Uma série de fatores tornou as redes sociais um ambiente participativo e livre, sem qualquer discriminação. Dentre esses fatores, destacam-se:



- facilidade de acesso;**
- rápida velocidade com que as informações se propagam;**
- grande quantidade de pessoas que elas conseguem atingir, de diferentes faixas etárias;**
- grande quantidade de informações pessoais que apresentam;**
- tempo significativo em que as informações ficam disponíveis;**
- alto grau de confiança que os usuários costumam depositar entre si; e**
- abertura de novas oportunidades de negócios.**

Algumas características importantes das redes sociais dizem respeito à dificuldade de exclusão e de manter-se sigilo. Aquilo que é publicado nelas nem sempre pode ser totalmente excluído ou ter o acesso controlado. Mesmo que se restrinja o acesso, não há como controlar a replicação das publicações.

Os sites costumam ter políticas próprias de privacidade e podem alterá-las sem aviso prévio, tornando público aquilo que antes era privado.

RISCOS



Nestes tempos de alta interação, tem crescido o uso da “engenharia social” por pessoas ou grupos mal-intencionados. Essa técnica visa obter informações ou acessos a informações pessoais que possam ser usadas na aplicação de golpes.



A falta de cuidados e a falta de preocupação com a segurança nas redes sociais podem trazer a seus usuários uma série de problemas graves, tais como: danos à pessoa, à família e até mesmo ao trabalho.

Estarmos atentos ao que postamos nas redes e às pessoas com quem nos relacionamos são procedimentos adequados para, entre outras, evitar ações de:

- invasão de privacidade;
- furto de identidade;
- invasão de perfil;
- instalação de programas maliciosos;
- acesso a conteúdos impróprios ou ofensivos;
- contato com pessoas mal-intencionadas;
- uso indevido de informações;
- danos à imagem e à reputação;
- vazamento de informações; e
- recebimento de mensagem contendo “códigos maliciosos” e phishing.



PROTEÇÃO PESSOAL E DA FAMÍLIA



Para nos protegermos dos riscos relacionados ao uso da Internet e, em especial, às redes sociais, é importante estarmos cientes de que ela não é “virtual”. Este é um termo que trata apenas da forma como ela se apresenta; não trata das responsabilidades e consequências inerentes ao seu uso, que é real.

Convém lembrar que as pessoas, empresas, organizações, entidades, enfim: todos os usuários que fazem uso das redes, e com os quais interagimos, são reais. Dessa forma, os riscos aos quais estamos expostos ao usá-las são os mesmos presentes em nosso dia a dia, e os golpes que são aplicados por meio delas, são similares àqueles que ocorrem na rua ou por telefone.

É preciso, portanto, que levemos para a Internet os mesmos cuidados e preocupações que temos fora dela, pois trata-se de um ambiente público, com baixo controle das informações divulgadas. Uma vez que as informações sejam postadas, qualquer pessoa da sua rede de contatos pode divulgá-las e, dificilmente, será possível apagá-las.

Para reduzir os riscos envolvendo o uso das redes sociais e proteger-se, é importante adotar uma postura preventiva e fazer com que a atenção à segurança seja um hábito incorporado à rotina, independentemente de questões como local, tecnologia ou meio utilizado. Essa postura preventiva deve ser mesclada com a aplicação de soluções técnicas que visam a proteger os usuários das ameaças conhecidas.

PROTEÇÃO PESSOAL E DA FAMÍLIA



ALGUNS PROCEDIMENTOS E RECOMENDAÇÕES SIMPLES, COMO AS RELACIONADAS ABAIXO, PODEM DEIXAR OS USUÁRIOS DE REDES SOCIAIS E INTERNET MENOS SUSCETÍVEIS A AÇÕES DE CRIMINOSOS E COLPISTAS.



Para proteger o seu perfil, elabore uma senha forte, que deve ser difícil de ser descoberta e fácil de ser lembrada.



A senha não deve ter qualquer tipo de dado pessoal (nomes, sobrenomes, contas de usuário, números de documentos, placas de carros, números de telefones e datas).



Não use senhas com as sequências de teclado (1qaz2wsx, qwerty, 123456789, asdfghjklç...). Além de uma péssima ideia, são as primeiras combinações a serem testadas pelos criminosos.



Não utilize nas senhas palavras que fazem parte de listas, tais como nomes de músicas, nomes de times de futebol, nomes de pessoas, etc.



Procure usar números aleatórios, não sequenciais, com um mínimo de 8 dígitos (quanto mais longa, melhor) em sistemas que utilizam exclusivamente caracteres numéricos.



Em sistemas de senhas alfanuméricas, mescle números, letras (maiúsculas e minúsculas) e caracteres especiais da maneira mais “bagunçada” possível.



Crie uma senha para cada sistema, “não” utilize a mesma senha para uma rede social e um sistema bancário ou sites de compra. O ideal é uma senha para cada site.



A senha deve ser trocada periodicamente.



Para proteger a sua privacidade e a de sua família, ou mesmo informações de sua organização, não seja vítima de uma das sete fraquezas mortais das redes sociais (CISCO SYSTEMS INC.)

- Sex appeal (apelo sexual)**
- Ganância**
- Vaidade**
- Confiança**
- Preguiça**
- Compaixão**
- Urgência**



PROTEÇÃO PESSOAL E DA FAMÍLIA



ALGUNS PROCEDIMENTOS E RECOMENDAÇÕES SIMPLES, COMO AS RELACIONADAS ABAIXO, PODEM DEIXAR OS USUÁRIOS DE REDES SOCIAIS E INTERNET MENOS SUSCETÍVEIS A AÇÕES DE CRIMINOSOS E COLPISTAS.



Ao utilizar as redes sociais, lembre-se:

Pense bem antes de divulgar (não há como voltar atrás).



Mantenha seu perfil e dados pessoais o mais restrito possível, utilizando as configurações disponibilizadas pelos aplicativos.



Não acredite em tudo que você lê.



Seja seletivo ao aceitar convites de amizade.



Restrinja o acesso ao seu endereço de e-mail e ao número de seu telefone.



Tome cuidado ao associar-se a grupos e comunidades.



Não divulgue planos de viagem, passeios, participação em eventos e outras atividades. Ao fazê-lo, você pode estar transmitindo informações a criminosos, facilitando ações contra seu patrimônio.



Ao divulgar fotos e vídeos, tenha cuidado com o conteúdo exibido e fique atento com a divulgação de sua localização.



A função *check-in* é muito utilizada por usuários de redes sociais, mas tome cuidado. Apenas a utilize quando estiver em locais movimentados e ao sair do local, e não quando chegar.



Não divulgue, nas redes sociais, horários de escolas, atividades desportivas, rotinas em geral de seus filhos. Estas informações podem ser usadas por criminosos.



Preocupe-se com a sua privacidade e a de seus amigos. Não divulgue imagens, vídeos ou mensagens alheias de maneira pública, caso o seu amigo não o tenha feito.



Algumas redes sociais oferecem a opção de confirmação de login, via SMS, quando o acesso ocorre em máquina/dispositivo diferente do usual. Este procedimento dificulta que sua identidade seja furtada.

PROTEÇÃO PESSOAL E DA FAMÍLIA



ALGUNS PROCEDIMENTOS E RECOMENDAÇÕES SIMPLES, COMO AS RELACIONADAS ABAIXO, PODEM DEIXAR OS USUÁRIOS DE REDES SOCIAIS E INTERNET MENOS SUSCETÍVEIS A AÇÕES DE CRIMINOSOS E COLPISTAS.



Para complementar a sua segurança e a de sua família, são necessários, ainda, cuidados com os dispositivos utilizados para acesso às redes e à Internet de modo geral. Veja algumas dicas:



Mantenha os programas e aplicativos (App) atualizados.



Utilize antivírus de boa qualidade.



Utilize firewall (mesmo que seja o disponível no Sistema Operacional).



Não abra links enviados via e-mail. Na sua maioria, são mecanismos de “phishing” ou vírus.



Nunca informe senhas via e-mail ou telefone (principalmente se você receber a ligação).



Compartilhe com seus dependentes estas informações e adote uma política de segurança. Por exemplo:



Oriente seus dependentes sobre os riscos do uso das redes sociais.



Deixe o computador ao acesso de todos na casa e mantenha controle sobre dispositivos móveis.



Alerte-os sobre o perigo de marcar encontros e de se relacionarem com estranhos.



Alerte-os sobre o perigo no uso de câmeras (webcam).



Oriente-os para que não divulguem dados pessoais, hábitos e rotinas da família e localização geográfica (principalmente futuras).



Alerte-os sobre a necessidade da manutenção do respeito em comentários, principalmente quando tratar de temas polêmicos, evitando comentários discriminatórios sobre etnia, religião e nacionalidade, entre outros.

PROTEÇÃO PESSOAL E DA FAMÍLIA



ALGUNS PROCEDIMENTOS E RECOMENDAÇÕES SIMPLES, COMO AS RELACIONADAS ABAIXO, PODEM DEIXAR OS USUÁRIOS DE REDES SOCIAIS E INTERNET MENOS SUSCETÍVEIS A AÇÕES DE CRIMINOSOS E COLPISTAS.



Além de todos os problemas de privacidade familiar e de segurança, temos que nos preocupar com a nossa atividade profissional e a imagem da Instituição. Por isso:

- ⚠ Antes divulgar informações, avalie se elas podem afetar negativamente as suas atividades, se podem comprometer o sigilo de informações ou a privacidade de pessoas, e se a divulgação delas não fere regulamentos, normas, leis ou preceitos institucionais.
- ⚠ Cuidado ao emitir opiniões que possam comprometer a Instituição.
- ⚠ Informações profissionais, postadas em redes sociais, são de responsabilidade de quem as postou, podendo essa pessoa responder civil ou criminalmente pelos danos causados, salvo quando a postagem for autorizada formalmente pela instituição.



PRÁTICAS PERIGOSAS



Algumas práticas no uso das redes sociais são bastante perigosas, dentre elas ressaltam-se:

- ❖ Aceitar convites para grupos e comunidades de pessoas desconhecidas.
- ❖ Aceitar a “amizade” de pessoas estranhas, sem qualquer verificação.
- ❖ Informar dados pessoais, endereço, contas bancárias e senhas, via redes sociais.
- ❖ Misturar assuntos pessoais com assuntos profissionais.



SEGURANÇA DAS MÍDIAS SOCIAIS INSTITUCIONAIS



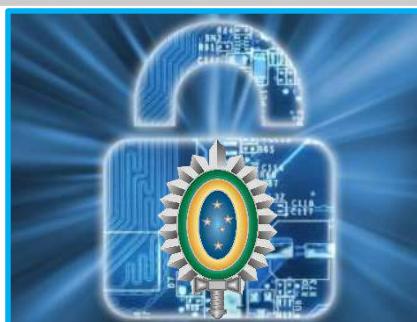
Algumas práticas no uso das redes sociais são bastante perigosas, dentre elas ressaltam-se:

As redes sociais são grandes veículos de comunicação em massa, e o Exército Brasileiro, buscando uma maneira de prover informações de maneira rápida ao público externo, faz uso de algumas destas ferramentas: Facebook, Youtube, Instagram, Twitter, Blogger e Flickr.

O Centro de Comunicação Social do Exército (CComSEEx) é o órgão oficial do Exército, responsável pelo gerenciamento e uso dessas mídias. Trata-se do meio preferencial de contato com o público externo (Palavra Oficial do Exército).

É importante lembrar que informações de caráter pessoal, informações sensíveis ou classificadas não deverão constar de páginas de Organização Militar, mídias ou redes sociais, conforme previsto na Portaria nº 1.067, de 8 de setembro de 2014, que aprova as Instruções Gerais para a Salvaguarda de Assuntos Sigilosos (EB10-IG-01.011), 1ª Edição - 2014.

Uma das principais preocupações, atualmente, é: como manter informações estratégicas, assegurar o sigilo, preservar a segurança de dados em um mundo que conjuga a todo instante o verbo compartilhar? Há, também, a questão relativa ao monitoramento das redes e às ações reativas quando da divulgação de dados e informações que possam representar danos à imagem da Instituição.



RESPONSABILIDADE CRIMINAL



CONDUTA	INFRAÇÃO	LEGISLAÇÃO	PENA
Falar em rede social que alguém deve se matar ou sugerir como fazê-lo.	Induzimento, instigação ou auxílio ao suicídio.	Art. 207, CPM Art. 122, CP	Reclusão de 2 a 6 anos, se o suicídio se consumar.
Falar em uma comunidade que alguém cometeu algum crime (ex.: ele é um ladrão, porque furtou o dinheiro de fulano...).	Calúnia.	Art. 214, CPM	Detenção, de 6 meses a 2 anos.
		Art. 138, CP	Detenção, de 6 meses a 2 anos, e multa.
Postar conteúdo sobre pessoa, imputando-lhe fato ofensivo à sua reputação.	Difamação.	Art. 215, CPM	Detenção, de 3 meses a 1 ano.
		Art. 139, CP	Detenção, de 3 meses a 1 ano, e multa.
Enviar e-mail mencionando características negativas de uma pessoa (ex.: gorda, feia, ignorante, etc.).	Injúria.	Art. 216, CPM	Detenção, até 6 meses.
		Art. 140, CP	Detenção, de 1 a 6 meses, ou multa.
Propalar fatos nas redes sociais, que sabe inverídicos, capazes de ofender a dignidade ou abalar a credibilidade das Forças Armadas ou a confiança que estas merecem do público.	Ofensa às Forças Armadas.	Art. 219, CPM	Detenção, de seis meses a um ano.



RESPONSABILIDADE CRIMINAL



CONDUTA	INFRAÇÃO	LEGISLAÇÃO	PENA
Enviar e-mail, dizendo que vai causar-lhe mal injusto e grave. (Enviar e-mail, dizendo que vai "pegar a pessoa" depois da aula).	Ameaça.	Art. 223, CPM	Detenção, até 6 meses, se o fato não constitui crime mais grave. Parágrafo único. Se a ameaça é motivada por fato referente a serviço de natureza militar, a pena é aumentada de um terço.
			Detenção, de 1 a 6 meses, ou multa.
Enviar vírus, comando, instrução ou programa de computador que destrua equipamento ou dados eletrônicos.	Dano simples.	Art. 259, CPM	Detenção, até seis meses.
	Dano.	Art. 163, CP	Detenção, de 1 a 6 meses, ou multa.
Copiar conteúdo de terceiros sem autorização ou sem mencionar a fonte, baixar MP3 ilegalmente, usar software ou jogo sem licença.	Violação de Direito Autoral.	Art. 184, CP	Detenção, de 3 meses a 1 ano, ou multa.
Revelação de segredos de terceiros na internet.	Divulgação, sem justa causa, de informações sigilosas ou reservadas.	Art. 153, CP	Detenção, de 1 a 6 meses, ou multa. se o fato não constitui crime mais grave. Detenção, de 1 (um) a 4 (quatro) anos, e multa (§ acrescido pela Lei nº 9.983, de 14 JUL 2000)
Invasão de redes de computadores	Invasão de dispositivo informático alheio	Art. 154-A CP	3 meses a 1 ano. Obs: § 1º / 5º, Inc IV.

REFERÊNCIAS



BRASIL. Código Penal. Decreto-Lei nº 2.848, de 7 DEZ 1940.



BRASIL. Código Penal Militar. Decreto-Lei nº 1.001, de 21 OUT 1969.



CERT.BR. Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Cartilha de segurança para Internet. Fascículo redes sociais, AGO 2012. Disponível em <<http://cartilha.cert.br/>>.



EXÉRCITO BRASILEIRO. Instruções Gerais para Salvaguarda e Assuntos Sigilosos (EB10-IG-01.011), aprovadas pela Portaria nº 1.067, de 8 SET 2014.



MINISTÉRIO DO TRABALHO E EMPREGO. Segurança da informação e comunicações: responsabilidade de todos - Brasília: MTE, SPOA, CGPGE, 2011. 20 p. II.



PRESIDÊNCIA DA REPÚBLICA. Gabinete de Segurança Institucional. Departamento de Segurança da Informação e Comunicações. Diretrizes para o uso seguro das redes sociais na administração pública federal, NC 15/IN01/DSIC/GSIPR, de 11 JUN 2012.



SECRETARIA DE COMUNICAÇÃO SOCIAL DA PRESIDÊNCIA DA REPÚBLICA. Manual de orientação para atuação em redes sociais, OUT 2012.



NOVAMÉRICA. Manual de mídias sociais, JUL 2014.



FEDERAÇÃO BRASILEIRA DE BANCOS (FEBRABAN). Cartilha de redes sociais, MAIO 2013.



OS NOSSOS RECURSOS HUMANOS SOB A PROTEÇÃO VIGILANTE DA **CONTRAINTELIGÊNCIA**

