

Segurança nas redes sociais



Mensagem Inicial

O Exército Brasileiro está atento às oportunidades, ameaças e riscos presentes nos novos ambientes de convívio que são as redes sociais.

Dessa forma, elaborou a presente Cartilha com a certeza de que as ideias e as mensagens nela contidas serão de grande valia para a segurança e o bem-estar da família militar.

Índice



- 1 - Redes sociais
- 2 - Atrativos e possibilidades
- 3 - Riscos principais
- 4 - Cuidados a serem tomados
- 5 - Você sabia?
- 6 - Regras para páginas institucionais
- 7 - Condutas e possíveis enquadramentos
- 8 - Referências bibliográficas



1 - Redes Sociais

Vamos entender o que é rede social

A internet provocou mudanças nos relacionamentos entre pessoas e, consequentemente, entre públicos e instituições. Vivemos conectados em rede e é neste cenário que se articula a comunicação humana. As recentes formas de interatividade, participação e sociabilidade ganharam expressão com o surgimento de novas ferramentas tecnológicas. Expandiu-se a capacidade do cidadão de expressar suas ideias, de fazê-las circular diante de um público maior.



Dessa forma, a web e as mídias sociais são meios de comunicação que podem potencializar os relacionamentos entre indivíduos. Vêm-se destacando como importantes ferramentas na sociedade atual, em função de democratizar a informação e promover uma comunicação bi-direcional entre os atores envolvidos. Neste contexto, surgiram as redes sociais. O que seriam então redes sociais?

Redes de relacionamento que permitem aos usuários:

- fornecer informações sobre si;
- acessar informações sobre outros usuários;
- utilizar mecanismos de comunicação;
- agrupar-se, de acordo com afinidades, características, interesses e objetivos em comum; e
- criar, gerenciar e compartilhar um tipo de diário público com informações do tipo:

- quem você é?
- onde você está?
- o que você curte?
- quem você conhece?
- o que está acontecendo?
- no que você está pensando?
- o que seus amigos dizem sobre você?
- onde você tem estado?

2 - Atrativos e Possibilidades



- Rápida velocidade de propagação de informações
- Grande quantidade de usuários
- Facilidade de acesso
- Grande quantidade de informações pessoais
- Tempo que as informações ficam disponíveis

3 - Riscos Principais

Atenção! As redes sociais trazem riscos

- Invasão de privacidade
- Furto de identidade
- Invasão de perfil
- Instalação de programas maliciosos
- Acesso a conteúdos impróprios ou ofensivos
- Contato com pessoas mal intencionadas
- Disponibilização de informações para criminosos, que podem ser usadas:
 - em tentativas de sequestro
 - para furto de bens
- Uso indevido de informações
- Danos à imagem e à reputação
- Vazamento de informações
- Recebimento de mensagens contendo:
 - códigos maliciosos
 - *phishing*



4 - Cuidados a serem tomados

Lembrar das sete fraquezas mortais nas redes sociais, segundo a empresa americana CISCO SYSTEMS INC.



1. *Sex appeal* (apelo sexual)
2. Ganância
3. Vaidade
4. Confiança
5. Preguiça
6. Compaixão
7. Urgência

a) PRESERVE A SUA PRIVACIDADE

- Considere que você está em um local público
- Pense bem antes de divulgar (não há como voltar atrás)
- Use as opções de privacidade oferecidas pelos sites
 - procure ser o mais restritivo possível
- Mantenha seu perfil e seus dados privados
- Restrinja o acesso ao seu endereço de e-mail
- Seja seletivo ao aceitar seus contatos
- Não acredite em tudo o que você lê
- Seja cuidadoso ao se associar a grupos e comunidades
- Seja cuidadoso ao divulgar fotos e vídeos
 - Ao observar onde foram gerados, pode ser possível deduzir sua localização
- Não divulgue:
 - planos de viagens
 - por quanto tempo ficará ausente de sua residência
- Ao usar redes sociais baseadas em geolocalização:
 - faça *check-in* apenas em locais movimentados
 - faça *check-in* ao sair do local, ao invés de quando chegar



b) RESPEITE A PRIVACIDADE ALHEIA

- Evite falar sobre ações, hábitos e rotina de outras pessoas
- Não divulgue, sem autorização:
 - imagens em que outras pessoas apareçam
 - mensagens ou imagens copiadas do perfil de usuários que restrinjam o acesso
- Tente imaginar como a outra pessoa se sentiria ao saber que aquilo está se tornando público



c) PROTEJA SEU COMPUTADOR

- Mantenha seu computador seguro com:
 - todos os programas instalados nas versões mais recentes
 - todas as atualizações aplicadas
- Utilize e mantenha atualizados mecanismos de segurança
 - antispam
 - antimalware
 - firewall pessoal
- Desconfie de mensagens recebidas
 - Mesmo que tenham sido enviadas por conhecidos
 - Podem ter sido enviadas de contas falsas ou invadidas
- Seja cuidadoso ao acessar links reduzidos
 - Use complementos que permitam que você expanda o link, antes de clicar sobre ele



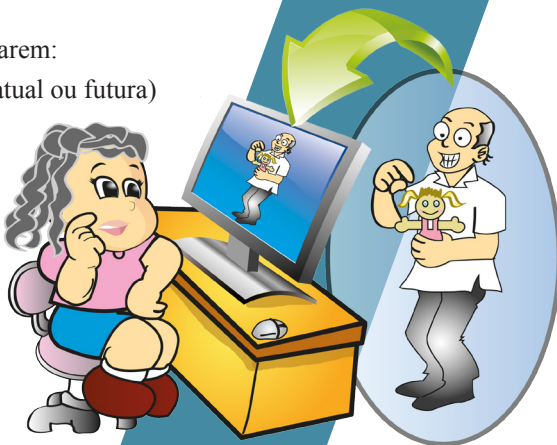


d) PROTEJA SEU PERFIL

- Seja cuidadoso ao elaborar as suas senhas:
 - use senhas longas, compostas de diferentes tipos de caracteres
 - não utilize dados pessoais, como nome, sobrenome e datas
- Seja cuidadoso ao usar as suas senhas:
 - evite usar a mesma senha para acessar diferentes sites
 - evite, se possível, usar sua senha em computadores de terceiros
- Habilite as notificações de login
- Lembre-se sempre de fechar a sua sessão (logout)
- Denuncie aos responsáveis pela rede social caso identifique abusos, tais como:
 - imagens indevidas
 - perfis falsos
 - spam

e) PROTEJA SEUS FILHOS

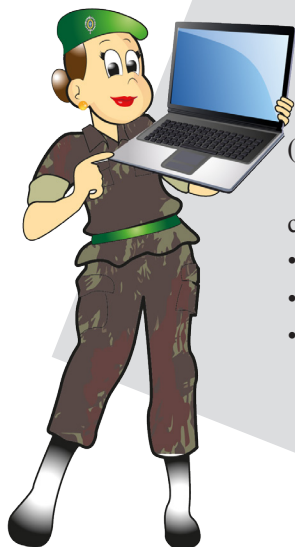
- Oriente-os sobre os riscos de uso das redes sociais
- Respeite os limites de idade estipulados pelos sites
- Deixe o computador em um local público da casa
- Oriente-os para não se relacionarem com estranhos:
 - não marcarem encontros
 - não usem a webcam
- Oriente-os para não divulgarem:
 - localização geográfica (atual ou futura)
 - dados pessoais
 - hábitos familiares



18+

f) PROTEJA SUA VIDA PROFISSIONAL

- Cuide da sua imagem profissional
- Antes de divulgar uma informação:
 - avalie se ela pode atrapalhar o seu emprego atual
 - avalie se ela pode atrapalhar um processo seletivo futuro
 - lembre-se que ela poderá ser acessada por seus chefes e colegas de trabalho
 - observe se ela não fere os preceitos previstos no regulamento de sua instituição



g) PROTEJA SUA INSTITUIÇÃO

- Crie um código de conduta
- Informe os servidores sobre:
 - os riscos de uso das redes sociais
 - as regras de acesso durante o expediente
 - o comportamento esperado, referente a:
 - 1) Divulgação de informações profissionais (sigilosas ou não)
 - 2) Emissão de opiniões que possam comprometer a sua organização militar (OM)
- Invista em treinamento
- Cuide da imagem
- Observe ações que envolvam o nome da OM

5 - Você sabia?

Existem muitas contas e perfis falsos nas redes sociais

As redes sociais geram uma atmosfera propícia ao desenvolvimento de relacionamentos de toda ordem: afetivos, profissionais, comerciais etc. Nesse ambiente, parece que as pessoas esqueceram do velho brocardo familiar de segurança: “não fale com estranhos”.

Nas redes sociais, existem muitos perfis e contas falsos. Ora são empregados como preparatórios de uma ação criminosa, ora servem para levantamento de dados. De maneira geral, todos agem de forma a conquistar a confiança da vítima.

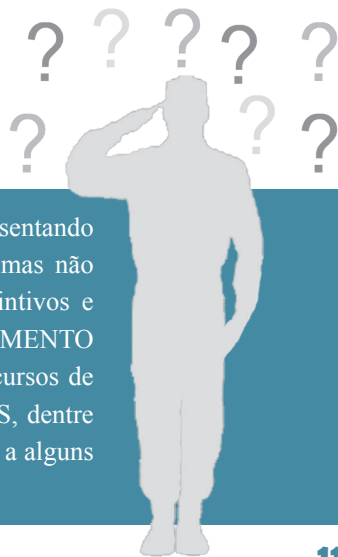
Forças oponentes em conflito no Oriente Médio estariam usando perfis falsos de mulher, na rede social, para extrair informações dos soldados inimigos. Com isso, esses soldados estariam postando dados e fotos, facilitando sua identificação pessoal, a da unidade e a do local onde estão baseados.

Já aconteceu na Força

Em setembro de 2012, foi identificada uma conta falsa em nome de um Comandante de OM no site FACEBOOK. Diversos militares dessa Unidade receberam um “convite” para acessarem a conta criada em nome do Comandante. Um dia depois, a página não se encontrava mais disponível para visualização.

Existem falsos militares nas redes

Nas redes sociais, também existem pessoas se apresentando como militares, ostentando inclusive uniformes, mas não o são. Esses falsos militares usam variados distintivos e brevês de forma irregular, contrariando o REGULAMENTO DE UNIFORMES DO EXÉRCITO (RUE). São cursos de AÇÕES DE COMANDOS, FORÇAS ESPECIAIS, dentre outros de elite. Esses criminosos têm comparecido a alguns lugares fardados com o uniforme 4º A1.



A engenharia social é largamente empregada nas redes sociais

A Engenharia Social é a “garimpagem” de informações vitais sobre uma pessoa, produto ou organização como preparação de um ataque. Pode ser considerada sinônimo de espionagem. Tais informações são provenientes quase sempre de pessoas próximas, cônjuges, pais, filhos e amigos.

As redes sociais virtuais facilitaram as ações dos engenheiros sociais, pois reúnem grande quantidade de dados pessoais ou de organizações, já relacionados, em um mesmo ambiente (textos, áudios, fotos, vídeos, planilhas etc). Essas redes são responsáveis por mais de 60% do tráfego da Rede Mundial.

Mesmo o ambiente privado dessas redes sociais não garante confidencialidade. Também não há garantia de que os dados sejam apagados quando o usuário assim o desejar. Além disso, alguns criminosos têm escolhido suas vítimas pelas imagens, de carros e casas, e rotinas divulgadas nas redes sociais.



Previna-se de prejuízos, seguindo regras simples no espaço cibernético:

- evite postar suas fotos ou vídeos nas redes sociais, inclusive de sua família, de seus bens (casa, carro etc) e o local de sua residência. Essas informações são monitoradas e podem facilitar ações ilícitas, colocando em risco sua própria integridade física ou a de seus familiares;
- mesmo o ambiente privado dessas redes não garante confidencialidade, podendo inclusive comprometer atividades profissionais;
- evite o cadastro de seus dados pessoais em fontes desconhecidas ou inidôneas. Tais dados podem ser usados por funcionários inescrupulosos ou estelionatários para a prática de crimes no sistema financeiro (abertura de contas bancárias, aquisição de cartões etc);
- tenha cuidado com o conteúdo publicado nas redes sociais, evitando opiniões ofensivas a pessoas, empresas ou instituições, pois tais opiniões podem ser enquadradas como criminosas.

Fique atento!

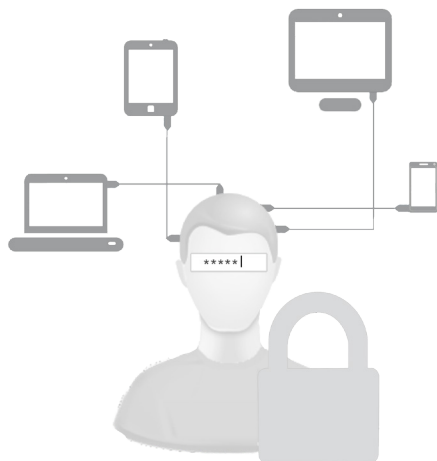
Não se exponha. Você não sabe quem está do outro lado.
Oriente seus familiares quanto aos riscos no mundo virtual.



Usar senhas relacionadas ao conteúdo publicado nas redes sociais é um perigo

A senha é a chave de acesso a muitos recursos no espaço cibernético (e-mails; contas; mídias sociais; sistemas, especialmente os bancários). Na ausência de outros dispositivos, esse mecanismo de segurança constitui a base da proteção pessoal e também da organização.

As pessoas têm dificuldades em estabelecer senhas seguras, diferentes e nas quantidades necessárias ao seu dia a dia. Assim, as senhas de acesso a sistemas sensíveis são, não raro, encontradas no conteúdo pessoal publicado nas redes sociais. Normalmente, são senhas fracas como: nomes de guerra; Jesus; sampaio; flamengo; datas de nascimento; e 123456.



Atenção

Não use senhas relacionadas ao conteúdo publicado nessas redes (preferências esportivas, religiosas, hobbies etc.) nem à sua vida privada (nome ou sobrenome de familiares ou de animais domésticos, placa do automóvel, data de nascimento, cidade onde reside, etc.). A partir dessas informações, os criminosos cibernéticos direcionam suas ferramentas e obtêm acesso a sistemas, contas de e-mail e outros.

Não use palavras comuns de dicionários.

Proteja-se. Construa e use senhas seguras.

Utilize senhas diferentes, pelo menos as senhas de banco e de sistemas críticos.

Utilize senhas fortes e simples, com no mínimo 8 (oito) caracteres alfanuméricos e especiais.

Seguem alguns exemplos de construção de senhas fortes:

- N@+taS& (**N**ão **a**guento **m**ais **t**anta **s**enha);
- &P@csnhA (**É** **p**reciso **a**mar **c**omo **s**e **n**ão **h**ouvesse **a**manhã);
- M&l@nCia (**m**elancia).

6 - Regras para páginas

As mídias sociais estão sendo apropriadas por pessoas, empresas e instituições como grandes veículos de comunicação ou de mobilização, especialmente porque as redes sociais proporcionam informações rápidas e abrangem grande número de interessados.

O Exército também aproveita esse novo meio de relacionamento, a fim de prover informações rápidas ao seu público externo, preferencialmente pelo Centro de Comunicação Social do Exército (CCOMSEx), ao qual compete emitir parecer acerca da criação eventual de mídias sociais para uso específico e temporário.



institucionais em redes sociais



Entretanto, as informações sensíveis ou classificadas não deverão constar de páginas de OM em mídias sociais, conforme as Instruções Gerais para Salvaguarda de Assuntos Sigilosos (IG 10-51):

Art. 121. Nenhuma informação sensível ou classificada com grau de sigilo deverá constar das “Home Pages” das organizações militares, dos militares da ativa, da reserva ou dos servidores civis.

Parágrafo único. Para fins deste artigo, serão considerados como informações sensíveis: vista aérea da OM, fotografias internas de pontos importantes da OM (paióis, reserva de armamento, etc.), cadeia de comando, peculiaridades do emprego, características técnicas do material de emprego militar, informações pessoais dos integrantes da OM, informações contidas nos Quadros de Organização / Lotação ou de Material, dentre outras.

7 - Condutas e possíveis enquadramentos, segundo os códigos penais

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	Reclusão de 2 a 6 anos, se o suicídio se consumir
		Art. 122, CP	
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 a 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 o crédito 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.
Enviar e-mail a outro militar, 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.
		Art. 147, CP	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.

8 - Referências bibliográficas

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 de Assuntos Sigilosos (IG 10-51), aprovadas pela Portaria nº 011, de 10 JAN 2001.

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

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.

Anotações

Mídias Sociais



Em novembro de 2010, o Exército Brasileiro iniciou suas atividades nas mídias sociais.



COMPARTILHE

ASSISTA

SIGA

COMENTE

CURTA

The collage includes screenshots of the Exército Brasileiro YouTube channel, Twitter profile, Facebook page, and the EBlog website. It also features a photo of a soldier in a combat helmet with the slogan 'Braço Forte - Mão Amiga'.

Com a sua participação, atingimos mais de 427 mil fãs no Facebook, superamos 24 mil seguidores no Twitter, ultrapassamos 3 milhões de visualizações no Youtube e tivemos mais de 28 mil visitas no EBlog. Obrigado!





EXÉRCITO BRASILEIRO

Braço Forte - Mão Amiga