Segurança em Redes Sociais

Miriam von Zuben
miriam@cert.br

Uso de Redes Sociais no Brasil (1/2)

- **comScore (dezembro/2011):**
  - **Facebook: 36,1 milhões (assume liderança)**
  - **Orkut: 34,4 milhões**
  - **Twitter: 12,5 milhões**
  - **Google+: 4,3 milhões**
  - **Linkedin: 3,1 milhões**

- **Socialbakers (setembro/2012):**
  - **57 milhões de usuários – #2 no mundo**

Uso de Redes Sociais no Brasil (2/2)

- 66% acessam diariamente a Internet
- Atividades realizadas:
  - Comunicação (91%):
    - enviar e receber *e-mail*: 78%
    - enviar mensagens instantâneas: 72%
    - participar de *sites* de relacionamento: 69%
    - conversar por meio de programas, como o Skype: 23%
    - usar *microblogs*, como o Twitter: 22%
    - criar ou atualizar *blogs* e/ou páginas na Internet: 15%
  - Lazer (85%):
    - assistir filmes ou vídeos: 58%
    - jogar jogos *on-line*: 42%
    - divulgar filmes ou vídeos: 15%
    - fazer/atualizar *fotoblog*: 11%

Fonte: TIC DOMICÍLIOS e USUÁRIOS 2011 – CETIC.br

Riscos


LOTERIA DE
Kurkistão
Você ganhou
URGENTE
Você recebeu um telegrama on line!
CLIQUE
CRÉDITO
INSTALE O MÓDULO DE PROTEÇÃO
CRÉDITO FÁCIL
CC CERT.br/NIC.br

Riscos X Características

- Rápida velocidade de propagação de informações
- Facilidade de acesso
- Grande quantidade de:
  - usuários
  - informações pessoais
- Dificuldade de:
  - exclusão de informações
  - controle sobre as informações
- Alto grau de confiança depositada entre os usuários

Invasão de Privacidade

- Síndrome da celebridade: quantidade X qualidade
- Pequenos pedaços de informação podem ser agregados
- Privacidade deixou de ser uma questão individual
  - não adianta um usuário restringir se os amigos divulgam
- Mudanças em políticas de privacidade dos *sites*
  - sem aviso prévio
  - disponibilização de novos recursos
- Permissões concedidas a aplicações:
  - nem sempre são claras
  - podem se sobrepor a outras permissões

Furto de Identidade

- **Invasão de contas, por meio de:**
  - **senhas fracas**
  - **senhas reutilizadas**
  - **vazamento de senhas**
  - **engenharia social**
  - **perguntas de segurança**
  - **códigos maliciosos/*phishing***

- **Criação de perfis falsos, usados:**
  - **em golpes de engenharia social**
  - **para coletar informações da rede de contatos**
  - **para aproximar-se de outras pessoas**

"Facebook revela que 83 milhões de seus usuários são *fakes*"

TechTudo – 02/08/2012

Disponibilização Indevida de Informações

- Discussões em reuniões
- Batidas policiais
- Detalhes técnicos e lançamento de serviços e produtos
- Ataques
- Danos à imagem
  - usuários
  - empresas
- Dificuldade em diferenciar assuntos pessoais de profissionais
  - casos de demissão
  - perdas financeiras
- Disponibilização de informações para criminosos
  - tentativas de sequestro
  - para furto de bens

Danos à Imagem e à Reputação

- Por meio de calúnia e difamação
  - problemas psicológicos
  - dificuldade em arrumar emprego
- Frases fora de contexto: dúbias e/ou ofensivas
- Informações sendo usadas em:
  - processos seletivos
  - processos de seguros
  - investigações criminais
  - comprovação de união estável
  - divórcios (comprovação de traição e/ou renda)

Spam, *Phishing* e *Malware*

- **Atacantes procuram explorar:**
  - **rede de relacionamento**
  - **a "confiança" depositada por seguidores/amigos**
  - **necessidade de imediatismo**
  - **uso de *links* reduzidos**
  - **facilidade de instalação e disponibilização de aplicações**

- ***Spear phishing***

- **Dados CERT.br:**
  - **desde 2009: 453 URLs de *phishing* de redes sociais**

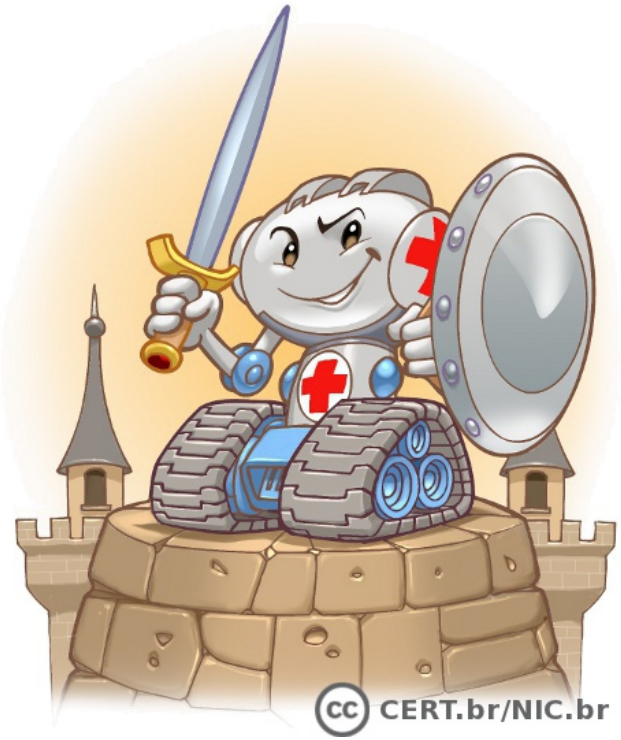
Outros Riscos

- **Perda de dados**
  - **não há garantia de continuidade**
- **Uso excessivo**
- **Sentimento de exclusão social**
- **Para crianças (principalmente):**
  - **acesso a conteúdos impróprios ou ofensivos**
  - ***cyberbulling***
  - **contato com pessoas mal-intencionadas**

TIC CRIANÇAS 2010 – CETIC.br (5 a 9 anos)

- **29% usam redes sociais**
- **39% usam sem acompanhamento**
- **21% acessam do próprio quarto**
- **21% dos pais não controlam ou restringem o uso da Internet**

Cuidados a serem tomados



Preservar a Privacidade

- Considerar que está em um local público
- Usar as opções de privacidade oferecidas pelos *sites*
  - ser o mais restritivo possível
- Manter perfil e dados privados
- Restringir o acesso ao endereço de *e-mail*
- Ser cauteloso ao:
  - divulgar informações (na há como voltar atrás)
  - aceitar contatos
  - dar acesso à aplicativos
  - se associar a grupos e comunidades
- Não acreditar em tudo que lê

Cuidados ao Fornecer a Localização

- **Ser cuidadoso ao divulgar fotos e vídeos**
  - **ao observar onde foram gerados pode ser possível deduzir a localização**
- **Não divulgar:**
  - **planos de viagens**
  - **por quanto tempo ficará ausente da residência**
- **Ao usar redes sociais baseadas em geolocalização:**
  - **fazer *check-in* apenas em locais movimentados**
  - **fazer *check-in* ao sair do local, ao invés de quando chegar**

Respeitar a Privacidade Alheia

- Não falar sobre as ações, hábitos e rotina de outras pessoas

- Não divulgar, sem autorização:
  - imagens em que outras pessoas apareçam
  - mensagens ou imagens copiadas do perfil de usuários que restrinjam o acesso

- Imaginar como a outra pessoa se sentiria ao saber que aquilo está se tornando público

Proteger o Perfil (1/3)

- **Ser cuidadoso ao elaborar as senhas**
  - **fácil de lembrar X difícil de ser deduzida**
  - **usar senhas longas, compostas de diferentes tipos de caracteres**
  - **não utilizar sequências de teclado, contas de usuário, palavras de dicionários, dados pessoais (disponíveis na redes sociais)**
  - **elaborar senhas distintas para acessar diferentes serviços**
    - **avaliar o risco envolvido**
    - **não misturar pessoal X profissional**
  - **criar padrão próprio de formação**

Proteger o Perfil (2/3)

- Ser cuidadoso ao usar senhas
  - não expor nem compartilhar
  - não armazenar no navegador sem usar criptografia
  - evitar utilizar em computadores de terceiros
  - adotar um mecanismo de gerenciamento de senhas
    - papel guardado em local seguro
    - programa específico
    - arquivo criptografado (não esquecer a chave mestra)
  - trocar senhas regularmente
    - trocar imediatamente caso suspeite que tenha sido comprometida

Proteger o Perfil (3/3)

- Utilizar sempre conexões seguras (https)
- Habilitar notificações de *login*
- Ser cauteloso ao instalar e dar acesso a aplicativos
- Lembrar-se sempre de fechar a sessão (*logout*)
- Denunciar aos responsáveis pela rede social caso identifique abusos, tais como:
  - imagens indevidas
  - perfis falsos
  - *spam*

Proteger o Computador (1/2)

- **Manter seu computador seguro com:**
  - **todos os programas instalados nas versões mais recentes**
  - **todas as atualizações aplicadas**
- **Utilizar e manter atualizados mecanismos de segurança**
  - ***antispam***
  - ***antimalware***
  - ***firewall* pessoal**

Proteger o Computador (2/2)

- **Desconfiar de mensagens recebidas**
  - **mesmo que enviadas por conhecidos**
  - **podem ter sido enviadas de contas falsas ou invadidas**
- **Ser cuidadoso ao acessar *links* reduzidos**
  - **usar complementos que permitam expandir o *link*, antes de clicar sobre ele**

Mais Informações (1/2)

Cartilha de Segurança para Internet

http://cartilha.cert.br/

RSS

http://cartilha.cert.br/rss/cartilha-rss.xml

Twitter

http://twitter.com/certbr

Mais Informações (2/2)

Portal Internet Segura

http://www.internetsegura.br/

INTERNET SEGURA.BR

Campanha Antispam.br

http://www.antispam.br/

Perguntas?

Miriam von Zuben

miriam@cert.br

- **CGI.br - Comitê Gestor da Internet no Brasil**

  http://www.cgi.br/
- **NIC.br - Núcleo de Informação e Coordenação do .br**

  http://www.nic.br/
- **CERT.br - Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil**

  http://www.cert.br/