Privacidade

sti.seguranca@eesc.usp.br

Fonte - http://cartilha.cert.br/

Agenda

- **Privacidade**
- **Riscos principais**
- **Cuidados a serem tomados**
- **Créditos**

Fonte - http://cartilha.cert.br/

Privacidade (1/3)

- **Sua privacidade pode ser exposta na Internet:**
  - **independentemente da sua vontade**
  - **sem aviso ou consentimento prévio, quando:**
    - **alguém:**
      - **divulga informações sobre você**
      - **divulga imagens onde você está presente**
    - **um *site*:**
      - **altera as políticas de privacidade**
      - **coleta hábitos e preferências de navegação e repassa a terceiros**
    - **um impostor:**
      - **cria uma conta/perfil em seu nome e a usa para se passar por você**

Fonte - http://cartilha.cert.br/

Privacidade (2/3)

- Sua privacidade pode ser exposta na Internet:
  - independentemente da sua vontade
  - sem aviso ou consentimento prévio, quando:
    - **um atacante e/ou código malicioso:**
      - **acessa dados que você digita**
      - **acessa dados armazenados em seu computador**
      - **invade uma conta sua e acessa informações restritas**
      - **invade um computador no qual seus dados estão armazenados**
      - **coleta informações não criptografadas que trafegam na rede**

Fonte - http://cartilha.cert.br/

Privacidade (3/3)

- Sua privacidade pode ser exposta na Internet:
  - independentemente da sua vontade
  - sem aviso ou consentimento prévio, quando:
    - **um aplicativo instalado em seu computador/dispositivo móvel:**
      - **coleta dados pessoais e os envia ao desenvolvedor/fabricante**
    - **você:**
      - **compartilha recursos do seu computador**
        - » **sem configurar restrições de acesso adequadas**
      - **elabora senhas fracas**
        - » **facilitando a invasão de suas contas**
      - **acessa suas contas em computadores potencialmente infectados**
      - **não mantém a segurança do seu computador/dispositivo móvel**

Fonte - http://cartilha.cert.br/

Riscos principais

Fonte - http://cartilha.cert.br/

Riscos principais (1/2)

- **Divulgação e coleta indevida de informações pessoais pode:**
  - **comprometer a sua privacidade, de seus amigos e familiares**
    - **mesmo com restrições de acesso não há como controlar que uma informação não será repassada**
  - **facilitar o furto da sua identidade**
    - **quanto mais dados você divulga mais fácil é para um impostor criar uma identidade falsa sua e usá-la em ações maliciosas, como:**
      - **acessar *sites***
      - **efetuar transações financeiras**
      - **enviar mensagens eletrônicas**
      - **abrir empresas fantasmas**
      - **criar contas bancárias ilegítimas**

BY NC SA

Fonte - http://cartilha.cert.br/

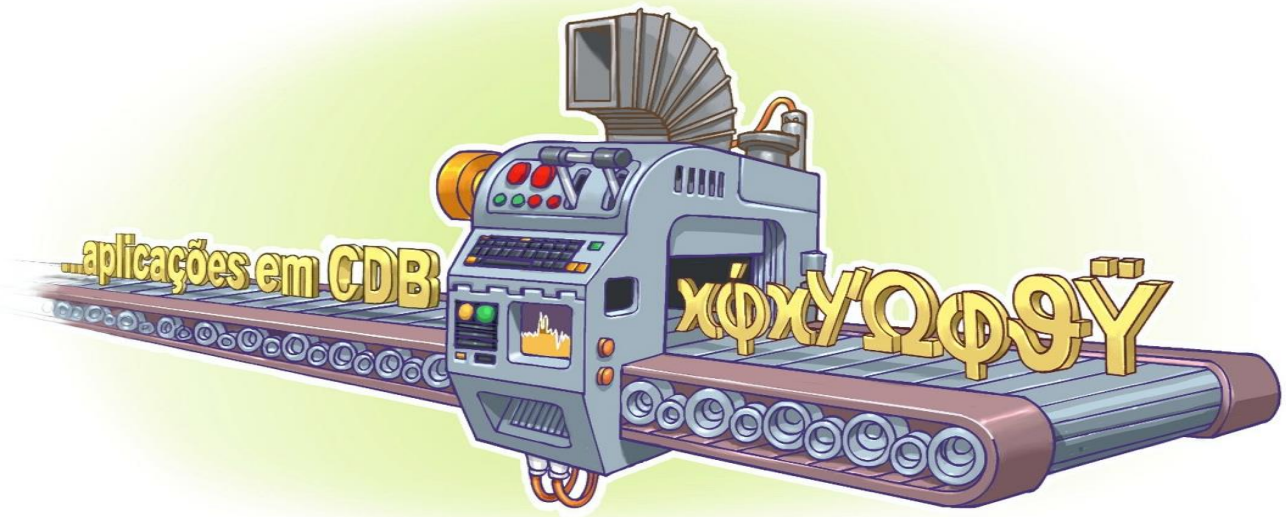
Riscos principais (2/2)

- Divulgação e coleta indevida de informações pessoais pode:
  - **facilitar a invasão de suas contas de usuário**
    - **senhas e respostas a dicas/perguntas de segurança podem ser adivinhadas caso usem dados pessoais**
  - **fazer com que propagandas direcionadas sejam apresentadas**
  - **favorecer o recebimento de *spam***
  - **colocar em risco a sua segurança física**
  - **causar:**
    - **perdas financeiras**
    - **perda de reputação**
    - **falta de crédito**

CC BY NC SA

Fonte - http://cartilha.cert.br/

Cuidados a serem tomados



Fonte - http://cartilha.cert.br/

Ao acessar/armazenar *e-mails* (1/2)

- **Configure seu programa leitor *de e-mails* para não abrir imagens que não estejam na própria mensagem**
  - **o acesso a imagem pode confirmar que o *e-mail* foi lido**
- **Use programas leitores de *e-mails* que permitam que as mensagens sejam criptografadas**
  - **mensagens criptografadas somente poderão ser lidas por quem conseguir decodificá-las**
- **Use conexão segura ao acessar *e-mails* via navegadores**
  - **isto pode evitar que eles sejam interceptados**

Fonte - http://cartilha.cert.br/

Ao acessar/armazenar *e-mails* (2/2)

- Armazene *e-mails* confidenciais em formato criptografado
  - isso dificulta que sejam lidos por atacantes e códigos maliciosos
  - você pode decodificá-los sempre que desejar lê-los
- Use criptografia para conexão entre seu leitor de *e-mails* e os servidores de *e-mail* do seu provedor
- Seja cuidadoso ao acessar seu *Webmail*
  - digite a URL diretamente no navegador
  - tenha cuidado ao clicar em *links* recebidos por meio de mensagens eletrônicas

Fonte - http://cartilha.cert.br/

Ao navegar na *Web* (1/2)

- **Seja cuidadoso ao usar *cookies:***
  - **Use uma ou mais das seguintes opções:**
    - **defina um nível de permissão superior ou igual a "médio"**
    - **configure para que:**
      - **os *cookies* sejam apagados quando o navegador for fechado**
      - ***cookies* de terceiros não sejam aceitos**
    - **você pode também configurar para que, por padrão:**
      - **os *sites* não possam definir *cookies:***
        - » **e criar listas de exceções, liberando os *sites* considerados confiáveis e onde o uso é realmente necessário**
      - **os *sites* possam definir *cookies:***
        - » **e criar listas de exceções, bloqueando os *sites* indesejados**

Fonte - http://cartilha.cert.br/

Ao navegar na *Web* (2/2)

- **Quando disponível procure utilizar:**
  - **navegação anônima**
    - **principalmente ao usar computadores de terceiros**
    - **informações sobre navegação não serão armazenadas**
  - **opções que indiquem que você não quer ser rastreado**
    - **"*Do Not Track*"**
    - **listas de proteção contra rastreamento**

Fonte - http://cartilha.cert.br/

Ao divulgar informações na *Web* (1/4)

- **Avalie com cuidado as informações divulgadas:**
  - **em sua página *Web*, rede social ou *blog***
  - **elas podem ser usadas para:**
    - **aplicar golpes de engenharia social**
    - **obter informações sobre você**
    - **atentar contra a segurança do seu computador**
    - **atentar contra a sua segurança física**
- **Considere que você está em um local público**
- **Pense bem antes de divulgar algo**
  - **não é possível voltar atrás**

Fonte - http://cartilha.cert.br/

Ao divulgar informações na *Web* (2/4)

- **Divulgue a menor quantidade possível de informações, tanto sobre você como sobre seus amigos e familiares**
  - **oriente-os a fazer o mesmo**
- **Sempre que alguém solicitar dados sobre você ou ao preencher algum cadastro:**
  - **reflita se é realmente necessário que aquela empresa ou pessoa tenha acesso àquelas informações**
- **Ao receber ofertas de emprego pela Internet:**
  - **limite as informações disponibilizadas no currículo**
  - **só forneça mais dados quando estiver seguro de que a empresa e a oferta são legítimas**

BY NC SA

Fonte - http://cartilha.cert.br/

Ao divulgar informações na *Web* (3/4)

- **Fique atento a mensagens eletrônicas pelas quais alguém solicita informações pessoais, inclusive senhas**
- **Seja cuidadoso ao divulgar a sua localização geográfica**
  - **com base nela, é possível descobrir a sua rotina, deduzir informações e tentar prever os seus próximos passos**
- **Verifique a política de privacidade dos *sites* que você usa**
  - **fique atento às mudanças, principalmente aquelas relacionadas ao tratamento de dados pessoais**

CC BY NC SA

Ao divulgar informações na *Web* (4/4)

- **Use as opções de privacidade oferecidas pelos *sites***
  - **procure ser *o* mais restritivo possível**
- **Mantenha seu perfil e seus dados privados**
- **Seja seletivo ao aceitar seus contatos**
- **Seja cuidadoso ao se associar a grupos e comunidades**

Fonte - http://cartilha.cert.br/

Ao manipular dados e recursos

- **Armazene dados sensíveis em formato criptografado**
- **Mantenha *backups* em locais seguros e com acesso restrito**
- **Cifre o disco do seu computador e dispositivos removíveis**
- **Ao usar serviços de *backup online:***
  - **considere a política de privacidade e de segurança do *site***
- **Ao compartilhar recursos do seu computador:**
  - **estabeleça senhas para os compartilhamentos**
  - **compartilhe pelo tempo mínimo necessário**

Fonte - http://cartilha.cert.br/

Contas e senhas

- **Seja cuidadoso ao elaborar as suas senhas**
  - **use senhas longas, com diferentes tipos de caracteres**
  - **não utilize dados pessoais**
    - **nome, sobrenome e datas**
    - **dados que possam ser facilmente obtidos**
- **Evite reutilizar suas senhas**
- **Não forneça suas senhas para outra pessoa**
- **Ao usar perguntas de segurança:**
  - **evite escolher questões cujas respostas sejam facilmente adivinhadas**

Fonte - http://cartilha.cert.br/

Computador e dispositivos móveis

- **Mantenha o seu computador/dispositivo móvel seguro:**
  - **com a versão mais recente de todos os programas instalados**
  - **com todas as atualizações aplicadas**
- **Utilize e mantenha atualizados mecanismos de segurança:**
  - ***antispam, antimalware e firewall* pessoal**
- **Ao instalar aplicativos desenvolvidos por terceiros:**
  - **seja cuidadoso ao permitir o acesso aos seus dados pessoais**
  - **verifique se as permissões necessárias são coerentes**
  - **seja seletivo ao selecionar os aplicativos**
    - **escolha aqueles bem avaliados e com grande número de usuários**

BY NC SA

Fonte - http://cartilha.cert.br/

Mantenha-se informado (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

CC BY NC SA

Fonte - http://cartilha.cert.br/

Mantenha-se informado (2/2)

Portal Internet Segura

http://www.internetsegura.br/

Campanha Antispam.br

http://www.antispam.br/

Fonte - http://cartilha.cert.br/

Créditos

- **Fascículo Privacidade**

  http://cartilha.cert.br/fasciculos/

- **Cartilha de Segurança para Internet**

  http://cartilha.cert.br/

cert.br
Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

nic.br
Núcleo de Informação e Coordenação do Ponto BR

cgi.br
Comitê Gestor da Internet no Brasil

CC BY NC SA