TEMA DA AULA DE HOJE

- **Dispositivos móveis**
- **Riscos principais**
- **Cuidados a serem tomados**

Dispositivos móveis (1/2)

- ***Tablets*, *smartphones*, celulares etc.**
- **Cada vez mais populares**
- **Executam ações realizadas em computadores pessoais**
  - **Navegação web**
  - ***Internet Banking***
  - **Acesso a *e-mails***
  - **Acesso a redes sociais**

Dispositivos móveis (2/2)

- **Principais características:**
  - **Auxílio em tarefas cotidianas**
    - Grande quantidade de informações pessoais e profissionais
    - Agenda, contatos, chamadas realizadas, mensagens recebidas
  - **Conectividade**
    - Wi-Fi, 3G
  - **Peso e portabilidade**
    - Leves e de tamanho reduzido
    - Fáceis de serem carregados em bolsas/bolsos
  - **Diversas funcionalidades integradas**
    - GPS, câmera

PRINCIPAIS RISCOS

DISPOSITIVOS MÓVEIS

Segurança da Informação, 2º DS – Prof. Everson Sousa

Riscos principais (1/6)

- **Dispositivos móveis X computadores pessoais**
  - **Funcionalidades similares**
  - **Riscos similares:**
    - Códigos maliciosos
    - *Phishing*
    - Acesso a conteúdo impróprios ou ofensivos
    - Contato com pessoas mal-intencionadas
    - Perda de dados
    - Dificuldade de manter sigilo
- **Possuem características que os tornam ainda mais atraentes para atacantes e pessoas mal-intencionadas**

Riscos principais (2/6)

- **Vazamento de informações**
  - **Grande quantidade de informações pessoais armazenadas**
  - **Rápida substituição de modelos**
    - Sem a devida exclusão das informações gravadas
  - **Informações podem ser indevidamente coletadas**
    - Mensagens SMS
    - Lista de contatos
    - Calendários
    - Históricos de chamadas
    - Fotos e vídeos
    - Senhas e números de cartão de crédito

Riscos principais (3/6)

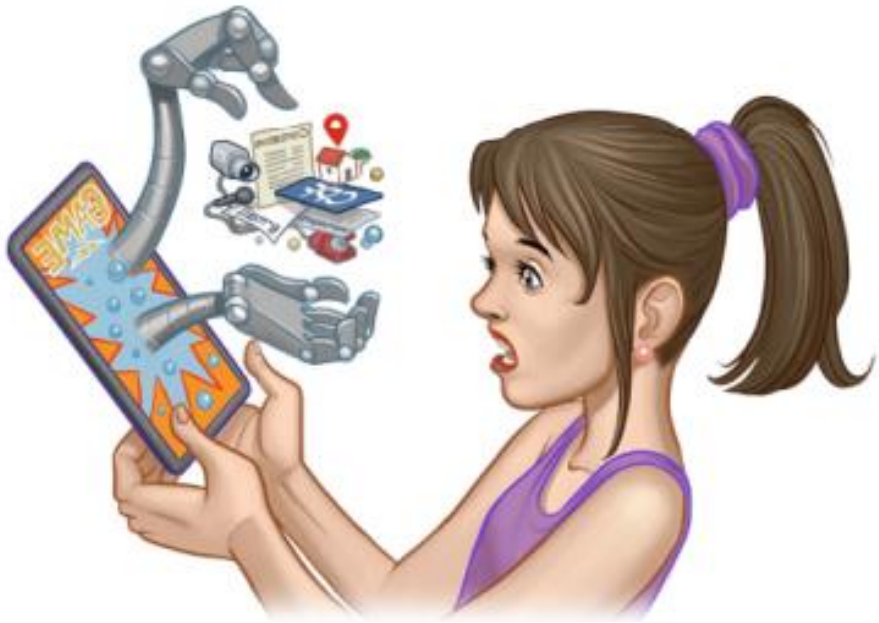
- **Maior possibilidade de perda e furto**
  - **Tamanho reduzido**
  - **Alto valor financeiro**
  - **Representam status**
  - **Atraem atenção de assaltantes**
  - **Constantemente em uso**
  - **Usados em locais públicos**
  - **Facilmente esquecidos e perdidos**

Riscos principais (4/6)

- **Invasão de privacidade**
  - **Intencional:**
    - Dispositivos sempre à mão
    - Uso generalizado
    - Alguém pode tirar uma foto sua e publicar sem seu conhecimento ou permissão
  - **Localização fornecida por aplicativos de geolocalização (GPS)**
  - **Dados pessoais coletados por códigos maliciosos/atacantes**
  - **Excesso de informações pessoais sendo fornecidas**
    - Locais que frequenta
    - Horários, rotina, hábitos e bens pessoais

Riscos principais (5/6)

- **Instalação de aplicativos maliciosos**
  - **Grande quantidade de aplicativos sendo desenvolvidos**
    - Diferentes autores
    - Diferentes funcionalidades
    - Dificuldade de manter controle
  - **Podem existir aplicativos:**
    - Não confiáveis
    - Com erros de implementação
    - Especificamente desenvolvidos para:
      - Executar atividades maliciosas
      - Coletar dados dos aparelhos



Riscos principais (6/6)

- **Propagação de códigos maliciosos**
  - **Códigos maliciosos recebidos por meio de:**
    - Mensagens SMS
    - E-mails
    - Redes sociais etc.
  - **Dispositivo infectado pode:**
    - Ter os dados coletados
    - Ter os dados apagados
    - Participar de ataques na Internet
    - Fazer parte de *botnets*

CUIDADOS A SEREM TOMADOS

DISPOSITIVOS MÓVEIS

Segurança da Informação, 2º DS – Prof. Everson Sousa

Antes de adquirir um dispositivo

- **Observe os mecanismos de segurança disponibilizados**
  - **Diferentes modelos e fabricantes**
  - **Escolha o que considerar mais seguro**
- **Caso opte por um modelo já usado**
  - **Restaure as configurações de fábrica/originais antes de usá-lo**
- **Não adquira um dispositivo:**
  - **Ilegalmente desbloqueado (jailbreak)**
  - **Com permissões de acesso alteradas**
    - Ação ilegal
    - Violação dos termos de garantia
    - Comprometimento da segurança e do funcionamento

Ao usar seu dispositivo (1/4)

- **Mantenha seu dispositivo seguro:**
  - **Com a versão mais recente dos programas instalados**
  - **Com todas as atualizações aplicadas**
- **Não siga links recebidos via mensagens eletrônicas**
  - **SMS, e-mails, redes sociais etc.**
- **Instale e mantenha atualizados**
- **Mecanismos de segurança**
  - **Antivírus**
  - **Antispam**
  - **Antimalware**
  - **Firewall pessoal**

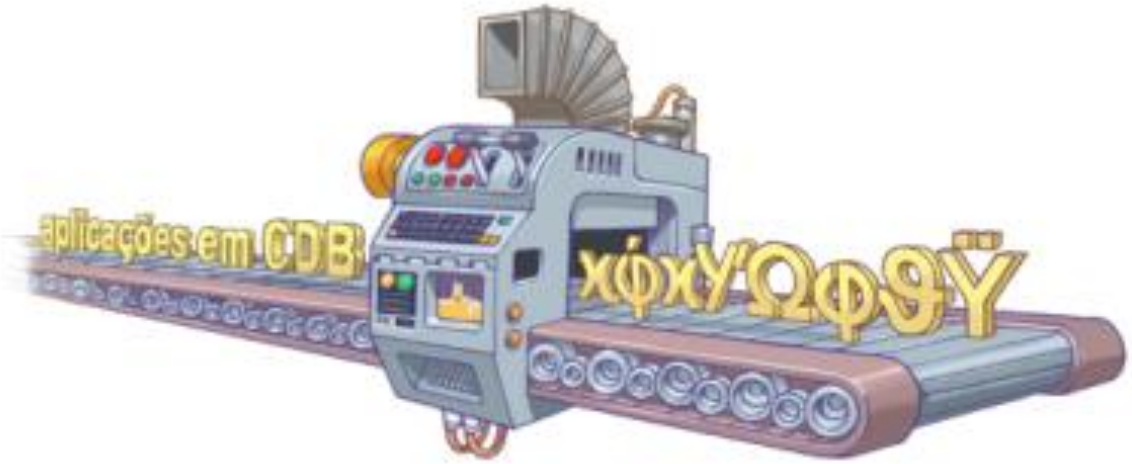
Ao usar seu dispositivo (2/4)

- **Mantenha controle físico**
  - **Principalmente em locais de risco**
  - **Procure não o deixar sobre a mesa**
  - **Cuidado com bolsos/bolsas em ambientes públicos**

- **Proteja sua privacidade**
  - **Seja cuidadoso ao:**
    - Publicar sua geolocalização
    - Permitir que aplicativos acessem seus dados pessoais

Ao usar seu dispositivo (3/4)

- **Proteja suas senhas**
  - **Cadastre senhas de acesso bem elaboradas**
  - **Se possível, configure-o para aceitar senhas complexas (alfanuméricas)**
  - **Use senhas longas, com diferentes tipos de caracteres**
  - **Não utilize:**
    - Sequência de teclado
    - Dados pessoais, como nome, sobrenome e datas
    - Dados que possam ser facilmente obtidos sobre você



Ao usar seu dispositivo (4/4)

- **Proteja seus dados**
  - **Configure:**
    - Senha de bloqueio na tela inicial
    - Código PIN
  - **Faça backups periódicos**
  - **Mantenha informações sensíveis em formato criptografado**
  - **Use conexão segura quando a comunicação envolver dados confidenciais**
    - Senhas
    - Número de cartão de crédito

Ao instalar aplicativos

- **Procure obter aplicativos de fontes confiáveis**
  - **Lojas confiáveis**
  - **Site do fabricante**
- **Escolha aplicativos:**
  - **Bem avaliados**
  - **Com grande quantidade de usuários**
- **Verifique com seu antivírus antes de instalar o aplicativo**
- **Observe as permissões para execução**
  - **Elas devem ser coerentes com a finalidade do aplicativo**
    - Um aplicativo de jogos, por exemplo, não necessariamente precisa ter acesso a sua lista de chamadas

Ao acessar redes

- **Seja cuidadoso ao usar redes Wi-Fi públicas**
  - **Desabilite a opção de conexão automática**
- **Mantenha interfaces de comunicação desativadas**
  - **Bluetooth, infravermelho e Wi-Fi**
  - **Somente as habilite quando necessário**
- **Configure o bluetooth para que o dispositivo não seja identificado (ou "descoberto) por outros**

Ao se desfazer do seu dispositivo

- **Apague todas as informações nele contidas**
- **Restaure as configurações de fábrica**

Em caso de perda ou furto (1/2)

- **Configure-o previamente, se possível, para que:**
  - **Seja localizado/rastreado e bloqueado remotamente, por meio de serviços de geolocalização**
  - **Uma mensagem seja mostrada na tela**
    - **Para aumentar as chances de ele ser devolvido**
  - **O volume seja aumentado ou que saia do modo silencioso**
    - **Para facilitar a localização**
  - **Os dados sejam apagados após um determinado número de tentativas de desbloqueio sem sucesso**

CUIDADO! Principalmente se você deixar crianças pequenas "brincarem" com seu dispositivo!

Em caso de perda ou furto (2/2)

- **Informe:**
  - **A sua operadora**
    - Solicite o bloqueio do seu número (chip)
  - **A empresa onde você trabalha**
    - Caso haja dados e senhas profissionais nele armazenadas
  - **Altere as senhas que possam estar nele armazenadas**
  - **Bloqueie cartões de crédito cujo número esteja nele armazenadas**
  - **Ative a localização remota, caso a tenha configurado**
    - **Se necessário, apague remotamente os dados gravados**