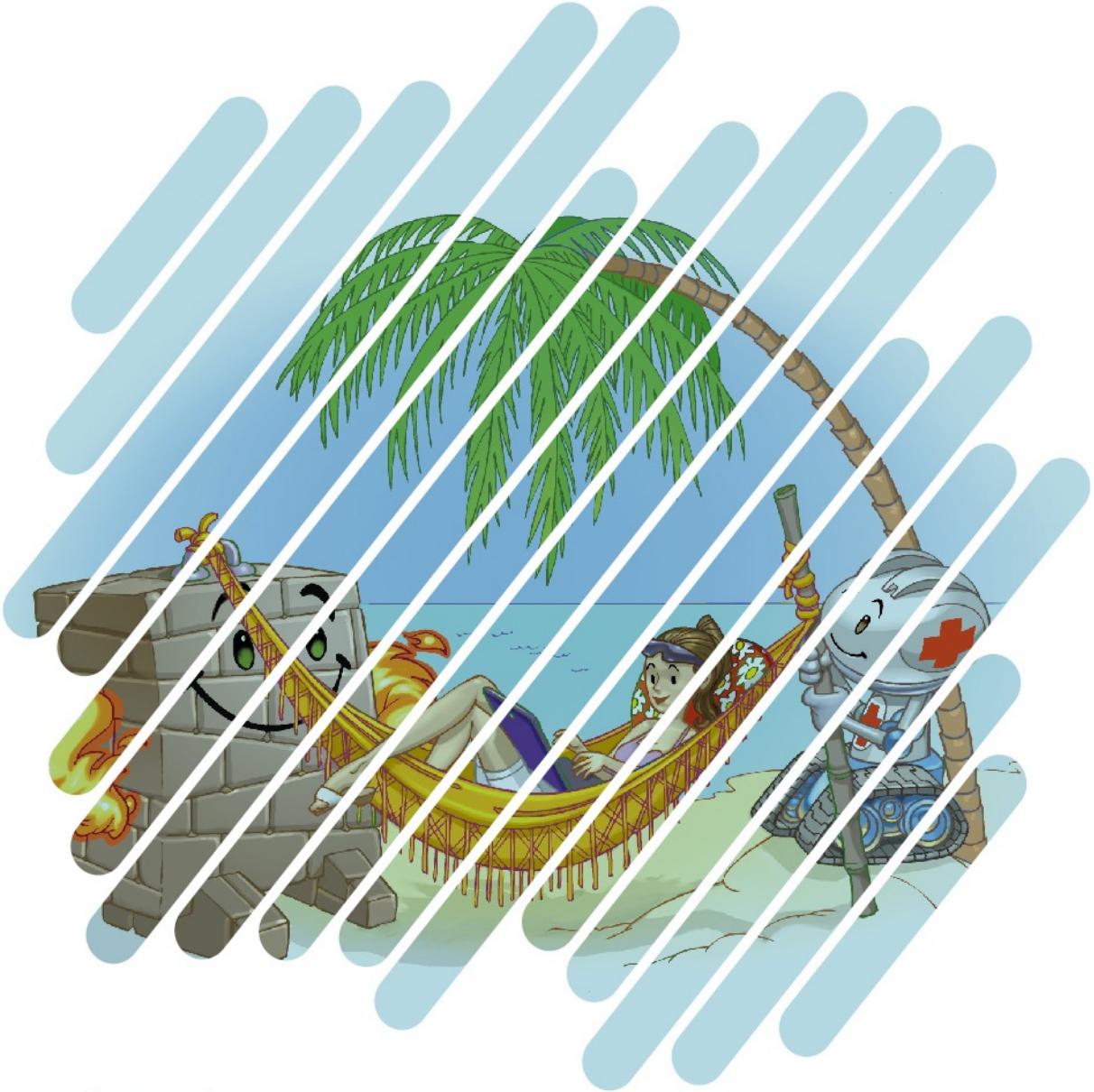


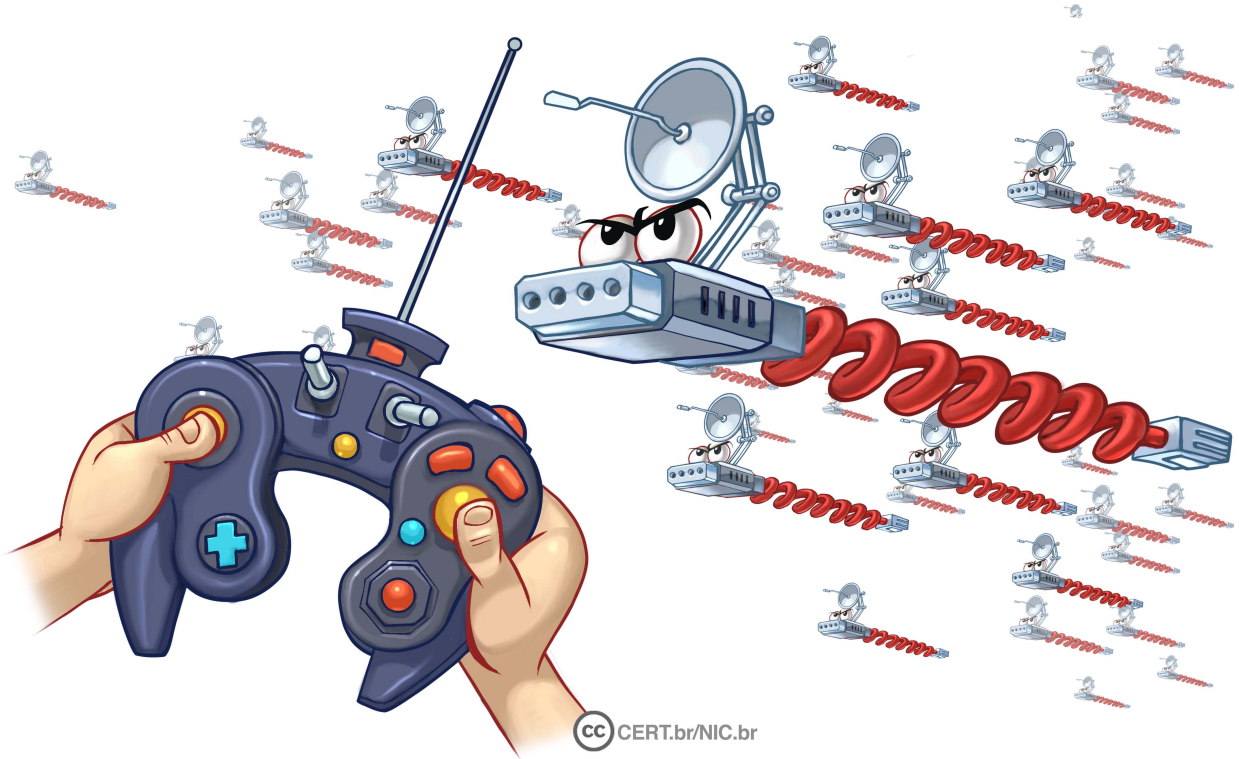
REDES

<Nome>
<Instituição>
<e-mail>

Agenda

- Riscos principais
- Cuidados gerais a serem tomados
- Configurando o acesso Internet da sua casa
- Configurando uma rede Wi-Fi doméstica
- Cuidados:
  - ao se conectar a redes Wi-Fi
  - ao usar redes móveis (3G/4G)
  - ao usar conexões *bluetooth*
- Saiba mais
- Créditos

Riscos principais



Riscos principais (1/3)

- **Independente do tipo de tecnologia usada, um equipamento conectado à rede, seja um computador, dispositivo móvel, *modem* ou roteador, pode ser invadido ou infectado por meio:**
  - **de falhas de configuração**
  - **da ação de códigos maliciosos**
  - **da exploração de vulnerabilidades**
  - **de ataques de força bruta, pelo uso de:**
    - senhas fracas
    - senhas padrão
    - senhas de conhecimento dos atacantes

Riscos principais (2/3)

- **Após invadido ou infectado ele pode, de acordo com suas características:**
  - **ser usado em atividades maliciosas, como:**
    - esconder a real identidade do atacante
    - participar de *botnets*
    - propagar códigos maliciosos
  - **estar sujeito a ameaças, como:**
    - furto de dados
    - uso indevido de recursos

Riscos principais (3/3)

- **Um atacante pode, por exemplo:**
  - **disponibilizar uma rede insegura ou fingir ser uma rede conhecida, induzir os dispositivos a se conectarem a ela e, então, capturar dados (ataque de personificação)**
  - **invadir um equipamento de rede, alterar as configurações e direcionar as conexões para *sites* fraudulentos**
  - **interceptar o tráfego e coletar dados que estejam sendo transmitidos sem o uso de criptografia (*sniffing*)**
  - **fazer varreduras na rede (*scan*), a fim de descobrir outros computadores e, então, tentar executar ações maliciosas, como ganhar acesso e explorar vulnerabilidades**
  - **usar a rede para enviar grande volume de dados para um computador, até torná-lo inoperante ou incapaz de se comunicar (DoS)**

Cuidados gerais a serem tomados

Cuidados gerais (1/3)

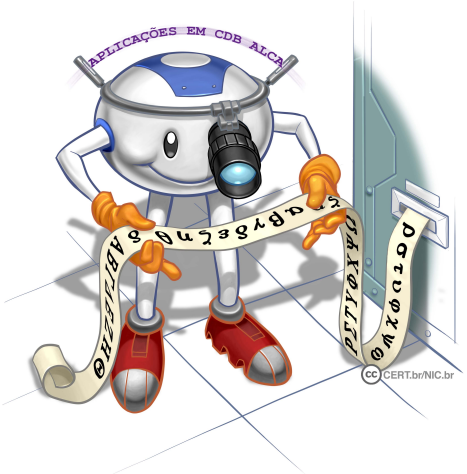
- **Proteja seus equipamentos de rede**
  - **atualize o *firmware***
    - seja cuidadoso ao fazer a atualização
    - verifique no *site* do fabricante os detalhes do procedimento
    - se necessário peça ajuda a alguém mais experiente
  - **altere a senha de administração**
    - use senhas bem elaboradas, com grande quantidade de caracteres e que não contenham dados pessoais, palavras conhecidas e sequências de teclado
    - lembre-se de guardar tanto a senha nova como a original
    - restaure a senha original somente quando necessário

Cuidados gerais (2/3)

- **Proteja seus computadores e dispositivos móveis**
  - **mantenha-os atualizados, com as versões mais recentes e com todas as atualizações aplicadas**
  - **utilize e mantenha atualizados mecanismos de segurança, como antivírus e *firewall* pessoal**
  - **desative a função de compartilhamento de recursos, somente a ative quando necessário e usando senhas bem elaboradas**
  - **ative as interfaces Wi-Fi e *bluetooth* somente quando for usá-las e desabilite-as após o uso**

Cuidados gerais (3/3)

- **Proteja seus dados**
  - **faça *backups* regularmente**
  - **use aplicações e protocolos que ofereçam criptografia, como:**
    - HTTPS para conexões *web*
    - PGP para o envio de *e-mails*
    - SSH para conexões remotas ou VPNs



Configurando o acesso Internet da sua casa

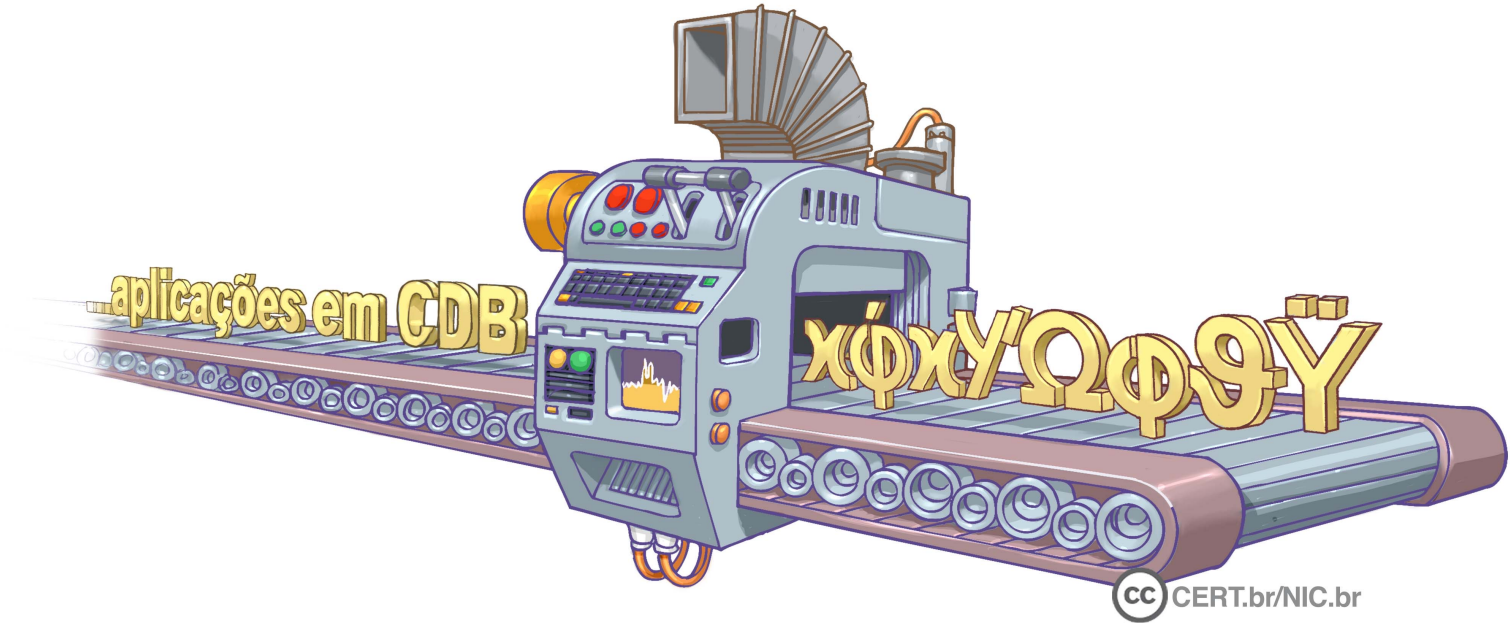
Acesso residencial

- Costuma ser realizado via roteadores ou *modems* de banda larga que podem prover também a funcionalidade de rede sem fio
- Acessíveis remotamente via senha de administração, que pode ser usada:
  - por você
  - pelo provedor de serviços Internet
  - por um atacante
- Infelizmente muitos destes equipamentos são instalados com senhas fracas, padrão ou de conhecimento dos atacantes e por isso precisam ser alteradas

Dicas de configuração

- **Siga os cuidados gerais para proteger seus equipamentos de rede, lembrando-se de:**
  - **atualizar o *firmware***
  - **alterar a senha de administração**
- **Desabilite:**
  - **o gerenciamento do equipamento de rede via Internet (WAN)**
    - funções de administração só estarão disponíveis via rede local
  - **a funcionalidade de rede sem fio caso não for usá-la**
    - caso deseje usá-la siga as dicas de como montar uma rede Wi-Fi doméstica
- **Desligue o equipamento de rede quando não estiver usando**

Configurando uma rede Wi-Fi doméstica



Rede Wi-Fi doméstica

- **Conexão Wi-Fi em uma residência ou escritório pode ser feita via:**
  - **equipamentos específicos, ou**
  - **como uma funcionalidade do roteador banda larga**

- **Em ambos os casos é necessário que alguns cuidados mínimos de segurança sejam tomados**

Dicas de configuração (1/2)

- Siga as recomendações gerais para proteger seus equipamentos de rede, lembrando-se de:
  - atualizar o *firmware*
  - alterar a senha de administração
- Altere a senha de autenticação de usuários
- Configure o modo WPA2 de criptografia
  - evite usar WPA e WEP
- Altere o nome da rede (SSID – *Server Set IDentifier*)
  - evite usar dados pessoais ou nomes associados ao fabricante/modelo, pois essas informações podem ser associadas a possíveis vulnerabilidades existentes

Dicas de configuração (2/2)

- **Desabilite:**
  - **difusão (*broadcast*) do SSID**
    - evitando que o nome da rede seja anunciado para outros dispositivos, dificultando o acesso por quem não sabe a identificação
  - **WPS (*Wi-Fi Protected Setup*)**
    - para evitar acessos indevidos
  - **gerenciamento remoto (via rede sem fio)**
    - funções de administração só estarão disponíveis por quem tiver acesso físico ao equipamento

Cuidados ao se conectar a redes Wi-Fi

Wi-Fi – Cuidados ao conectar (1/4)

- **Não permita que seus dispositivos conectem-se automaticamente:**
  - **a redes públicas**
  - **a redes que você já tenha visitado**
    - um atacante pode configurar uma rede com o mesmo nome de uma rede já utilizada por você
    - sem saber você estará acessando essa rede falsa

- **Lembre-se de apagar as redes que você visitou**
  - **isso ajuda a preservar a sua privacidade**

Wi-Fi – Cuidados ao conectar (2/4)

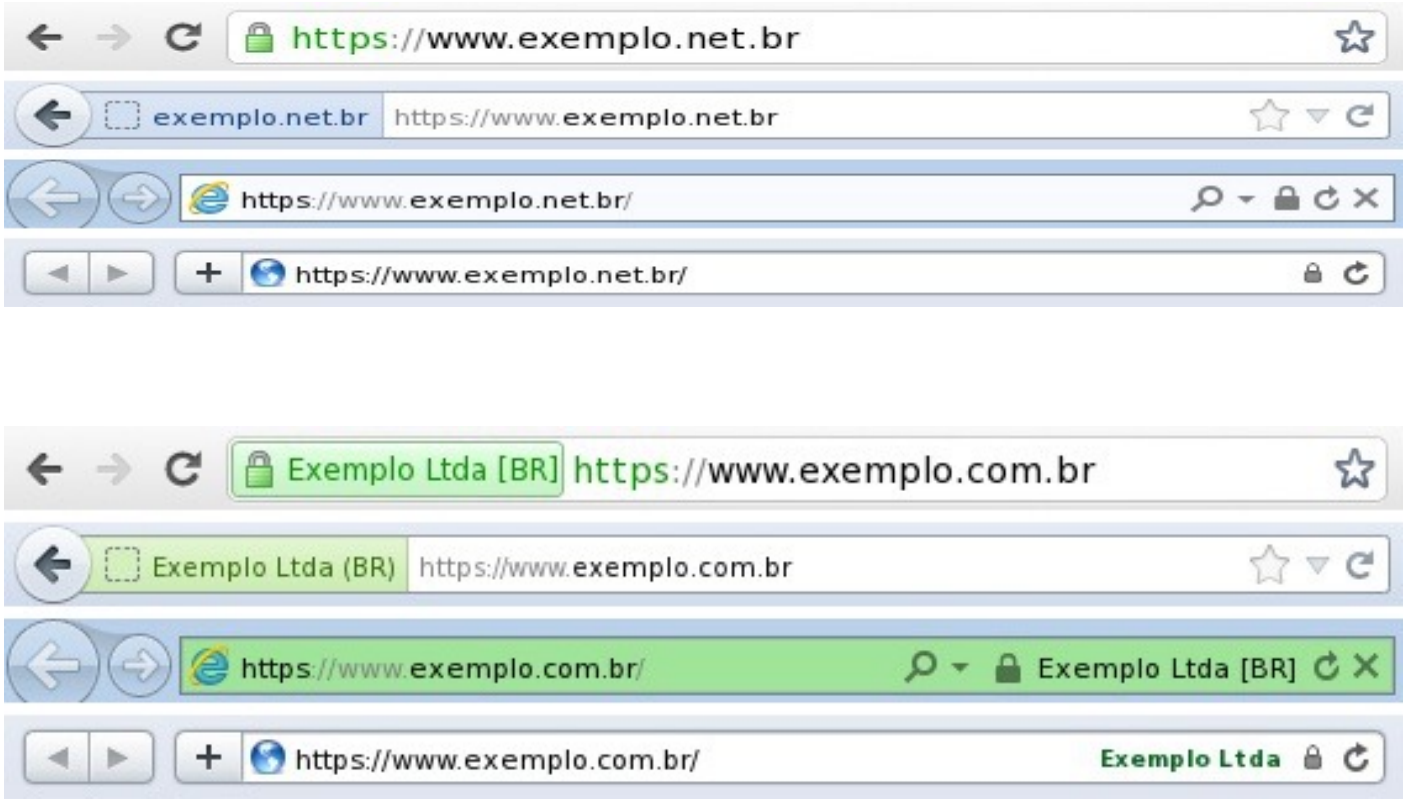
- **Algumas redes públicas, como as encontradas em aeroportos, hotéis e conferências, redirecionam a navegação no primeiro acesso para um *site* de autenticação**
  - **essa autenticação serve apenas para restringir os usuários e não garante que as informações trafegadas serão criptografadas**

- **Procure usar redes que ofereçam criptografia WPA2**
  - **evite usar WEP e WPA**

Wi-Fi – Cuidados ao conectar (3/4)

- **Certifique-se de usar conexão segura**
  - **alguns indícios apresentados pelo navegador *web* são:**
    - o endereço começa com https://
    - o desenho de um “cadeado fechado” é mostrado na barra de endereço
      - ao clicar sobre ele são exibidos detalhes sobre a conexão e certificado digital em uso
    - um recorte colorido (branco ou azul) com o nome do domínio do *site* é mostrado ao lado da barra de endereço (à esquerda ou à direita)
      - ao passar o *mouse* ou clicar sobre o recorte são exibidos detalhes sobre a conexão e certificado digital em uso
    - a barra de endereço e/ou recorte são apresentados em verde e no recorte é colocado o nome da instituição dona do *site*

Wi-Fi – Cuidados ao conectar (4/4)



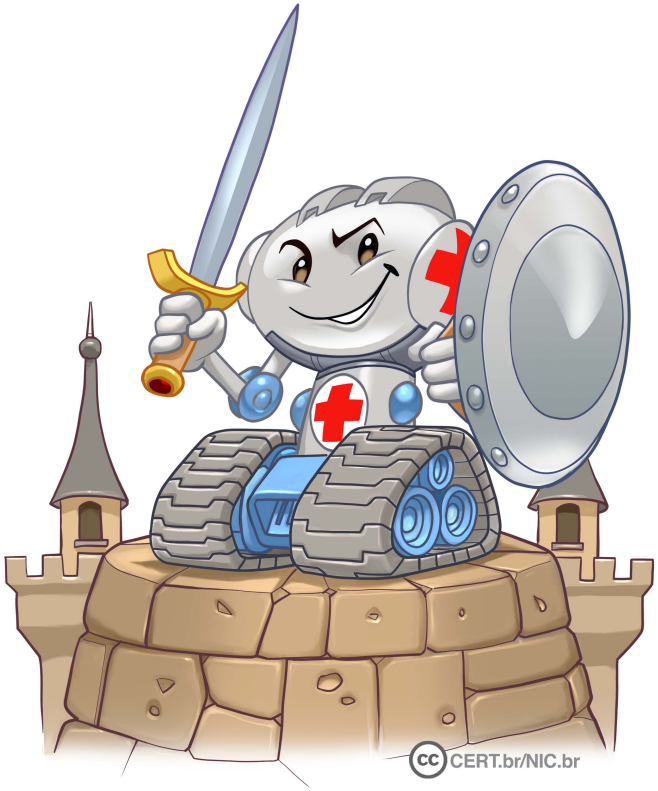
Cuidados ao usar redes móveis (3G/4G)

Redes móveis – Cuidados

- **Mantenha seus equipamentos seguros**
  - **um dispositivo infectado conectado via rede móvel pode ser usado para:**
    - desferir ataques
    - enviar as informações coletadas
    - se propagar para outros dispositivos

- **Caso use um *modem* 3G/4G:**
  - **siga as recomendações de como configurar a Internet em sua casa**

Cuidados ao usar conexões *bluetooth*



Bluetooth – Cuidados (1/2)

- Mantenha as interfaces inativas e somente as habilite quando for usar
- Configure as interfaces para que a visibilidade seja “Oculto” ou “Invisível”
- Altere o nome padrão do dispositivo
  - evite usar na composição do novo nome dados que identifiquem o proprietário ou características técnicas do dispositivo
- Altere a senha (PIN) padrão do dispositivo
  - seja cuidadoso ao elaborar a nova

Bluetooth – Cuidados (2/2)

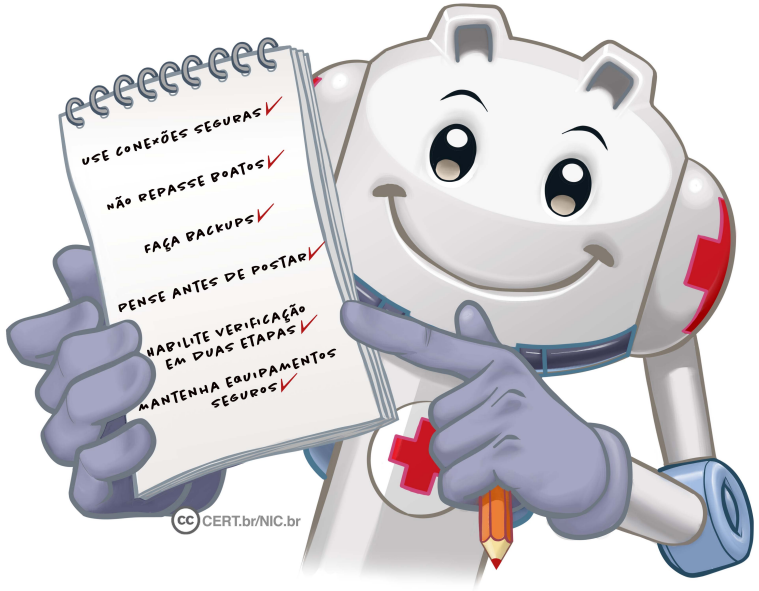
- Evite realizar o pareamento em locais públicos, reduzindo as chances de ser rastreado ou interceptado por um atacante
- Fique atento ao receber mensagens em seu dispositivo solicitando autorização ou PIN
  - não responda à solicitação se não tiver certeza que está se comunicando com o dispositivo correto
- No caso de perda ou furto de um dispositivo *bluetooth*, remova de seus outros equipamentos todas as relações de confiança já estabelecidas com este dispositivo

Saiba mais

- **Consulte os demais Fascículos da Cartilha de Segurança e o Livro Segurança na Internet: cartilha.cert.br**

- **Confira os demais materiais sobre segurança para os diferentes públicos: internetsegura.br**

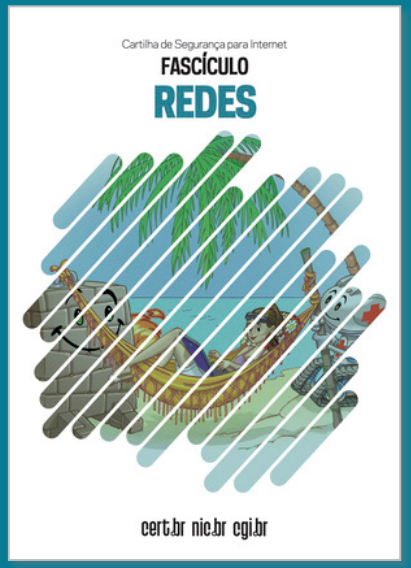
- **Acompanhe novidades e a dica do dia no Twitter do CERT.br twitter.com/certbr**



Créditos

- **Cartilha de Segurança para Internet**
  Fascículo Redes
  cartilha.cert.br/fasciculos

- **Livro Segurança na Internet**
  cartilha.cert.br/livro



cert.br nic.br cgi.br