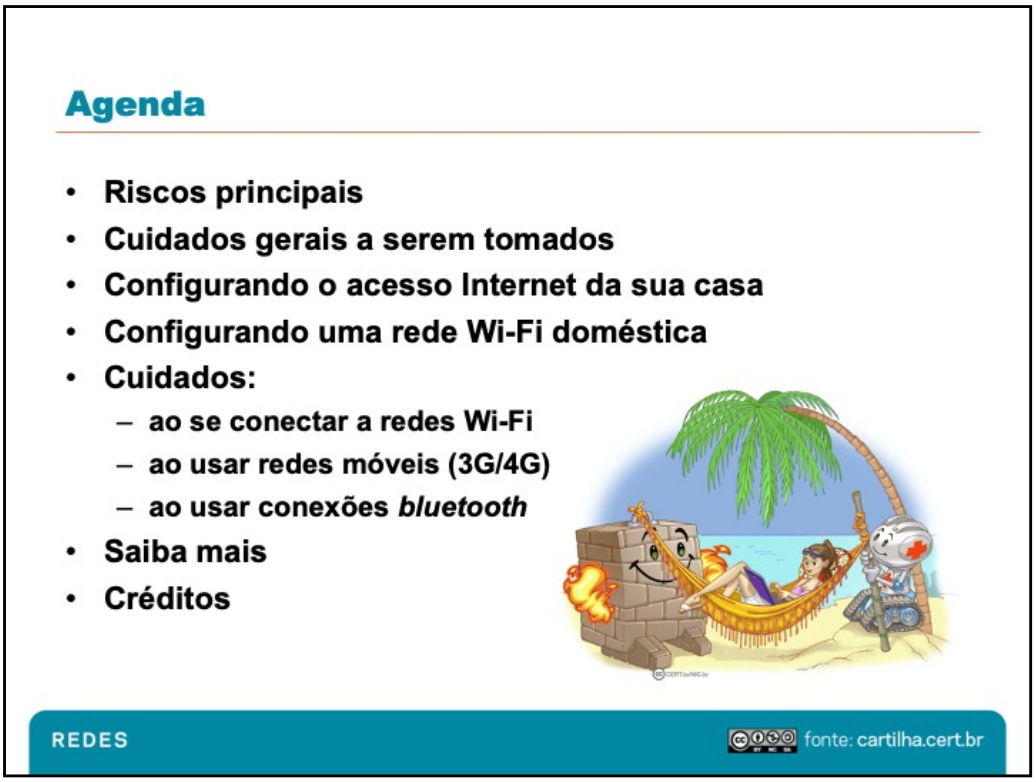
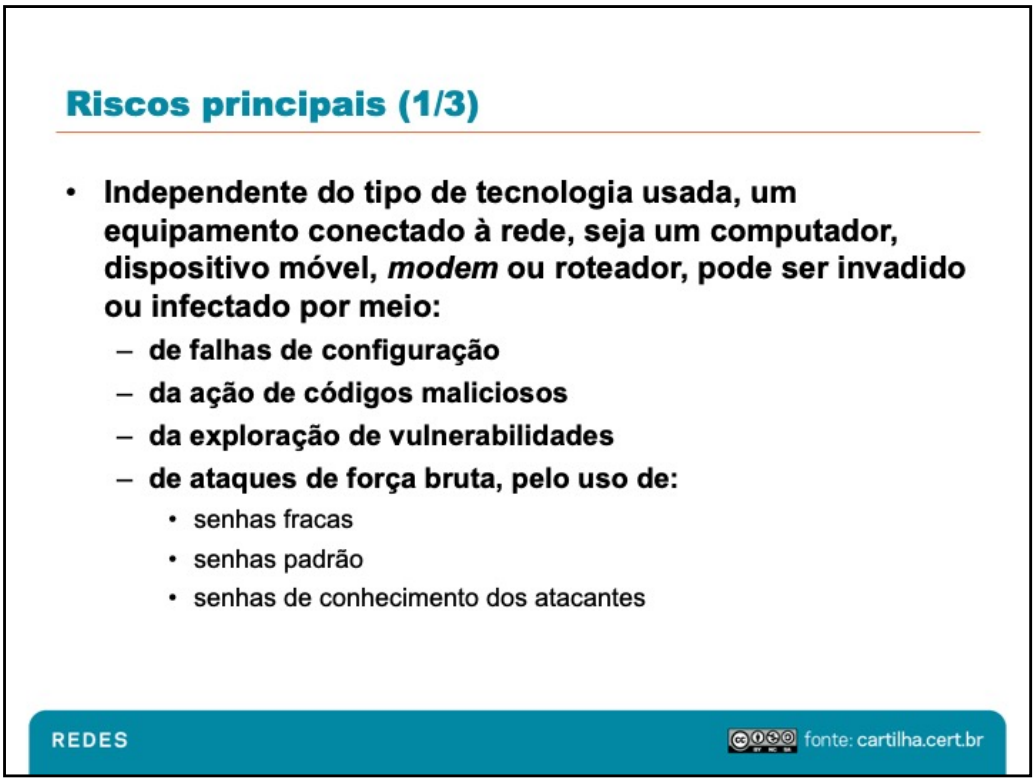


- **Riscos principais:** são apresentados alguns dos riscos a que os usuários estão sujeitos ao usar redes, independente da tecnologia adotada.
- **Cuidados gerais a serem tomados:** são apresentados os principais cuidados que devem ser tomados para proteção de equipamentos de rede, computadores, dispositivos móveis e dados pessoais.
- **Configurando o acesso Internet da sua casa:** são apresentadas dicas de configuração segura de acesso residencial.
- **Configurando uma rede Wi-Fi doméstica**: são apresentadas dicas de configuração segura de equipamentos que oferecem conexões Wi-Fi.
- **Cuidados ao se conectar a redes Wi-Fi:** são apresentados os cuidados que se deve ter ao se conectar a redes Wi-Fi**.**
- **Cuidados ao usar redes móveis (3G/4G):** são apresentados os cuidados que se deve ter ao usar redes móveis.
- **Cuidados ao usar conexões *bluetooth:*** são apresentados os cuidados que se deve ter ao usar conexões *bluetooth*.
- **Saiba mais:** apresenta materiais de consulta onde você pode buscar mais informações e manter-se informado.
- **Créditos:** apresenta a lista de materiais usados como fonte das informações contidas nestes *slides*.

Inicialmente, grande parte dos acessos à Internet eram realizados por meio de conexão discada com velocidades que dificilmente ultrapassavam 56 Kbps. O usuário, de posse de um *modem* e de uma linha telefônica, se conectava ao provedor de acesso e mantinha esta conexão apenas pelo tempo necessário para realizar as ações que dependessem da rede.

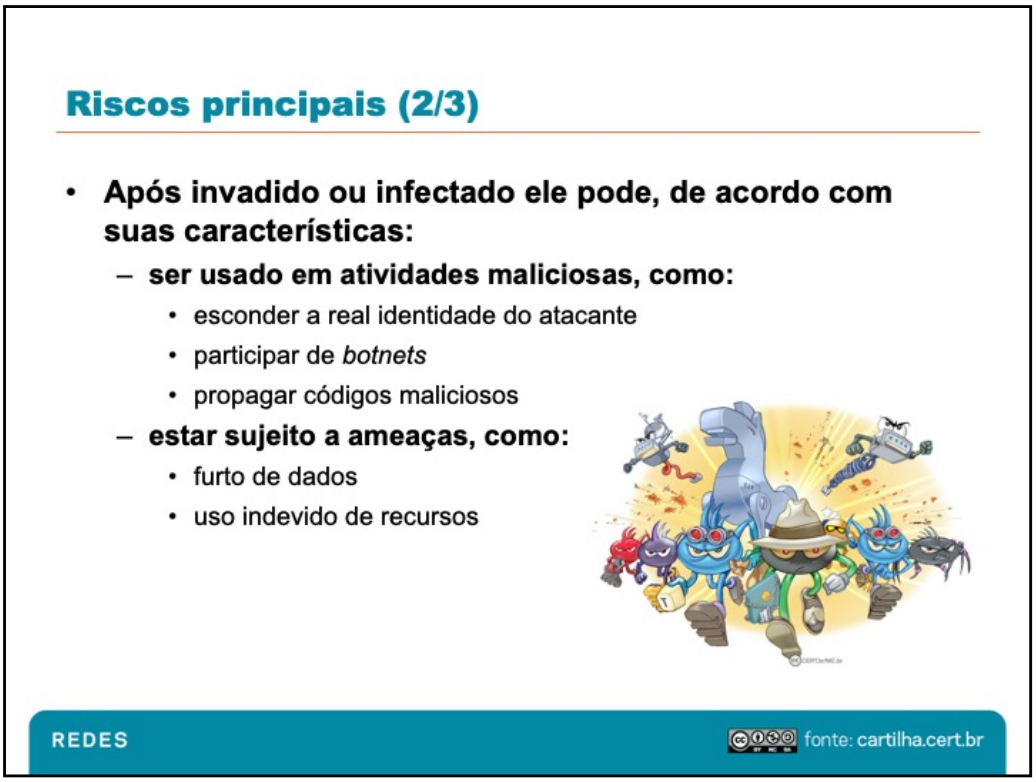
Desde então, grandes avanços ocorreram e novas alternativas surgiram, sendo que atualmente grande parte dos computadores pessoais ficam conectados à rede pelo tempo em que estiverem ligados e a velocidades que podem chegar a até 100 Mbps. Conexão à Internet também deixou de ser um recurso oferecido apenas a computadores, visto a grande quantidade de equipamentos com acesso à rede, como dispositivos móveis, TVs, eletrodomésticos e sistemas de áudio.

Nos próximos *slides* são apresentados alguns dos principais riscos associados ao uso de redes.



Por meio da exploração de vulnerabilidades, um equipamento pode ser infectado ou invadido e, sem que o dono saiba, participar de ataques, ter dados indevidamente coletados, ser usado para a propagação de códigos maliciosos, ter as configurações alteradas e fazer com que as conexões dos usuários sejam redirecionadas para *sites* fraudulentos.

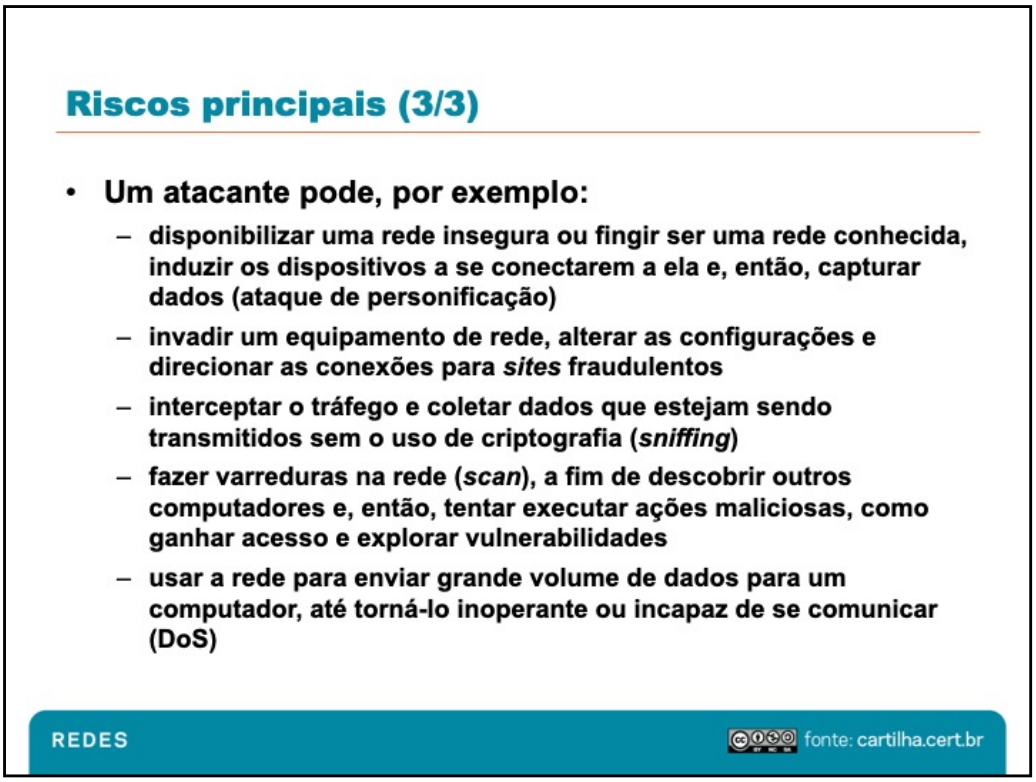
Equipamentos conectados à rede e que usem senhas como método de autenticação, estão expostos a ataques de força bruta. Muitos equipamentos, infelizmente, utilizam, por padrão, senhas de tamanho reduzido e/ou de conhecimento geral dos atacantes.



Botnet é uma rede formada por centenas ou milhares de equipamentos zumbis e que permite potencializar as ações danosas executadas pelos *bots*.

Quanto mais zumbis participarem da *botnet* mais potente ela será. O atacante que a controlar, além de usá-la para seus próprios ataques, também pode alugá-la para outras pessoas ou grupos que desejem que uma ação maliciosa específica seja executada.

Algumas das ações maliciosas que costumam ser executadas por intermédio de *botnets* são: ataques de negação de serviço, propagação de códigos maliciosos (inclusive do próprio *bot*), coleta de informações de um grande número de computadores, envio de *spam* e camuflagem da identidade do atacante (com o uso de *proxies* instalados nos zumbis).

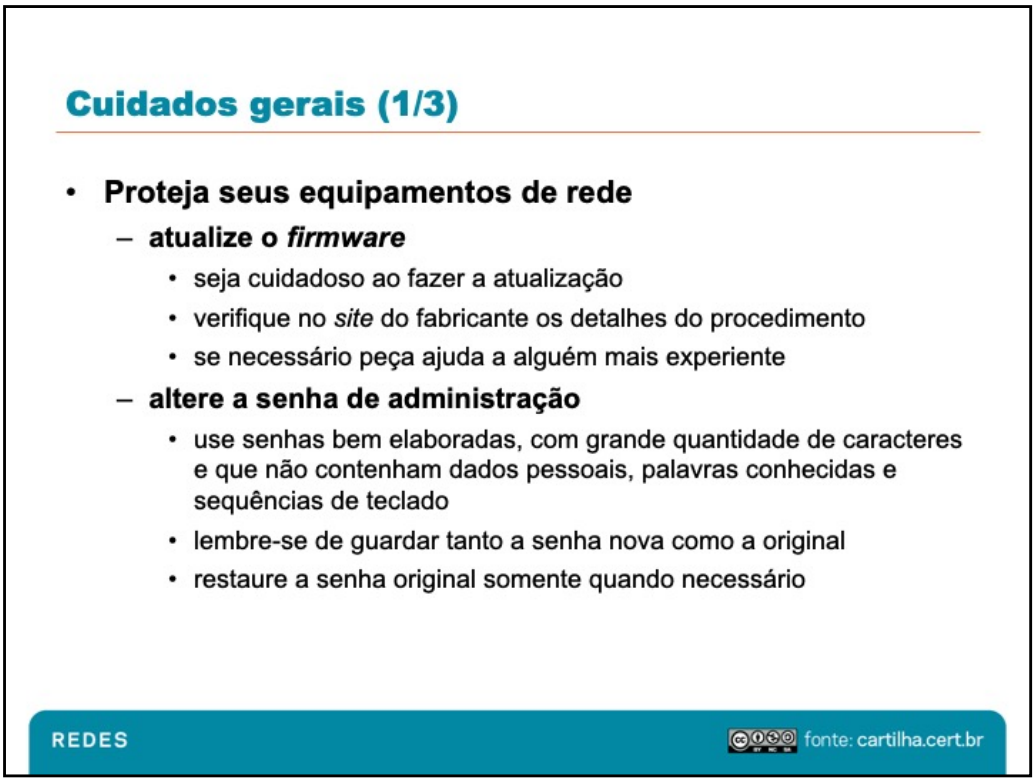


Interceptação de tráfego, ou *sniffing*, é uma técnica que consiste em inspecionar os dados trafegados em redes de computadores, por meio do uso de programas específicos chamados de *sniffers*. As informações capturadas por esta técnica são armazenadas na forma como trafegam, ou seja, informações que trafegam criptografadas apenas serão úteis ao atacante se ele conseguir decodificá-las.

Varredura em redes, ou *scan*, é uma técnica que consiste em efetuar buscas minuciosas em redes, com o objetivo de identificar computadores ativos e coletar informações sobre eles como, por exemplo, serviços disponibilizados e programas instalados. Com base nas informações coletadas é possível associar possíveis vulnerabilidades aos serviços disponibilizados e aos programas instalados nos computadores ativos detectados.

Negação de serviço, ou DoS (***D**enial **o**f **S**ervice*), é uma técnica pela qual um atacante utiliza **um computador** para tirar de operação um serviço, um computador ou uma rede conectada à Internet. Quando utilizada de forma coordenada e distribuída, ou seja, quando **um conjunto de computadores** é utilizado no ataque, recebe o nome de negação de serviço distribuído, ou DDoS (***D**istributed **D**enial of **S**ervice*).

Nos próximos *slides* são apresentados alguns dos principais tipos de cuidados que devem ser tomados para proteger seus dados, equipamentos de rede, computadores e dispositivos móveis.



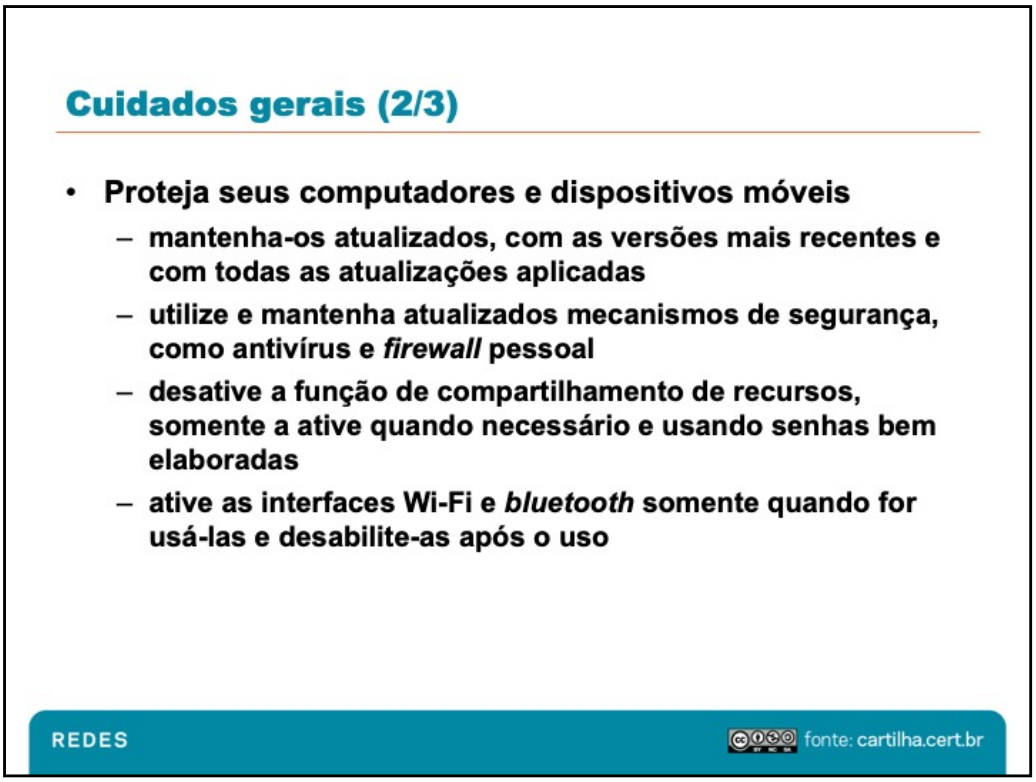
Fabricantes costumam lançar novas versões quando há recursos a serem adicionados e vulnerabilidades a serem corrigidas. Sempre que uma nova versão for lançada, ela deve ser prontamente instalada.

Alguns elementos que você **não deve** usar na elaboração de suas senhas são:

- **Qualquer tipo de dado pessoal**: evite nomes, sobrenomes, contas de usuário, números de documentos, placas de carros, números de telefones e datas.
- **Sequências de teclado**: evite senhas associadas à proximidade entre os caracteres no teclado, como "1qaz2wsx" e "QwerTAsdfG".
- **Palavras que façam parte de listas**: evite palavras presentes em listas publicamente conhecidas, como nomes de músicas, times de futebol, etc.

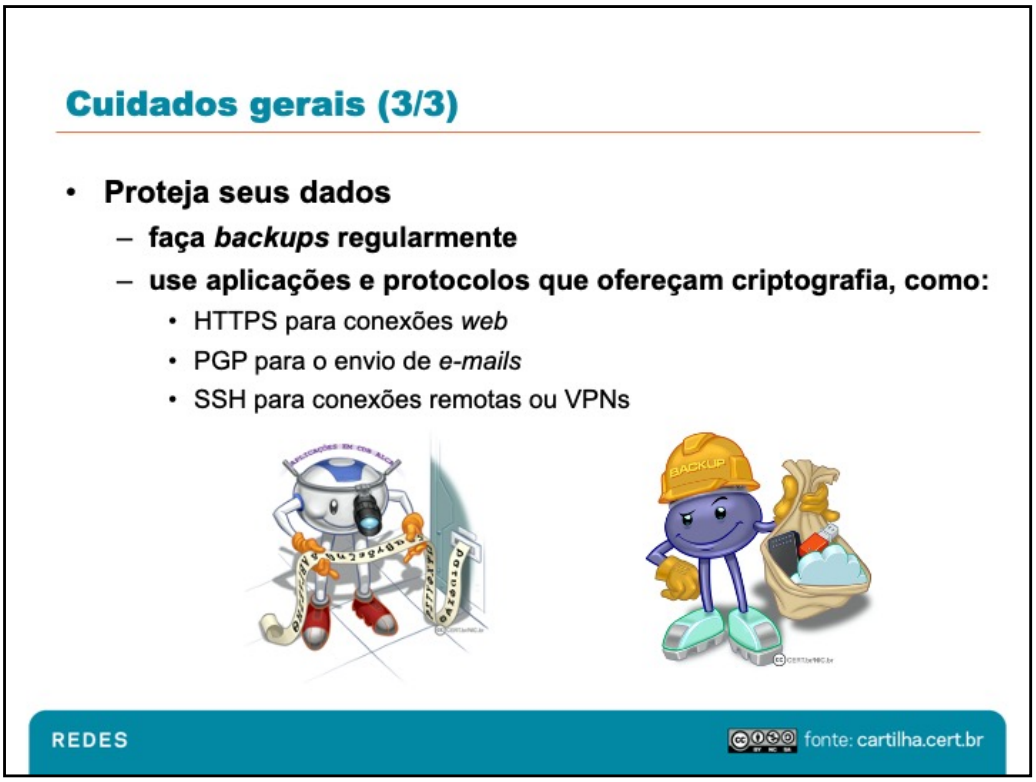
Alguns elementos que você **deve** usar na elaboração de suas senhas são:

- **Números aleatórios**: quanto mais ao acaso forem os números usados melhor, principalmente em sistemas que aceitem exclusivamente caracteres numéricos.
- **Grande quantidade de caracteres**: quanto mais longa for a senha mais difícil será descobri-la.
- **Diferentes tipos de caracteres**: quanto mais "bagunçada" for a senha mais difícil será descobri-la.

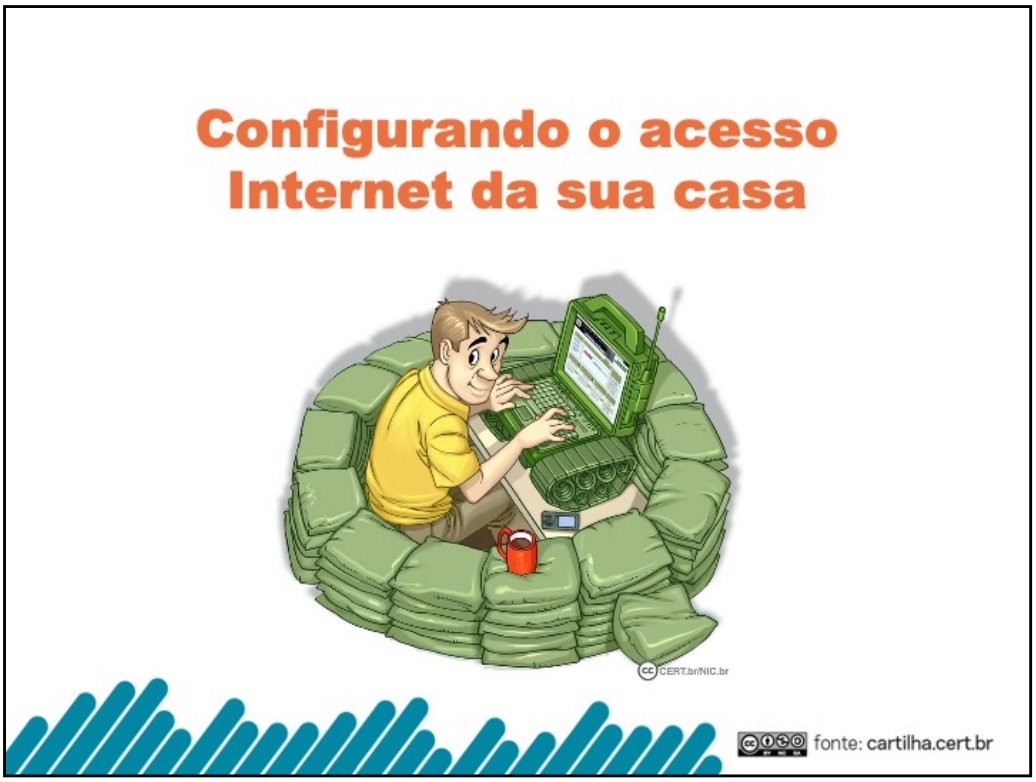


Quando vulnerabilidades são descobertas, certos fabricantes costumam lançar atualizações específicas, chamadas de *patches*, *hot fixes* ou *service packs*. Portanto, para manter os programas instalados livres de vulnerabilidades, além de manter as versões mais recentes, é importante que sejam aplicadas todas as atualizações disponíveis.

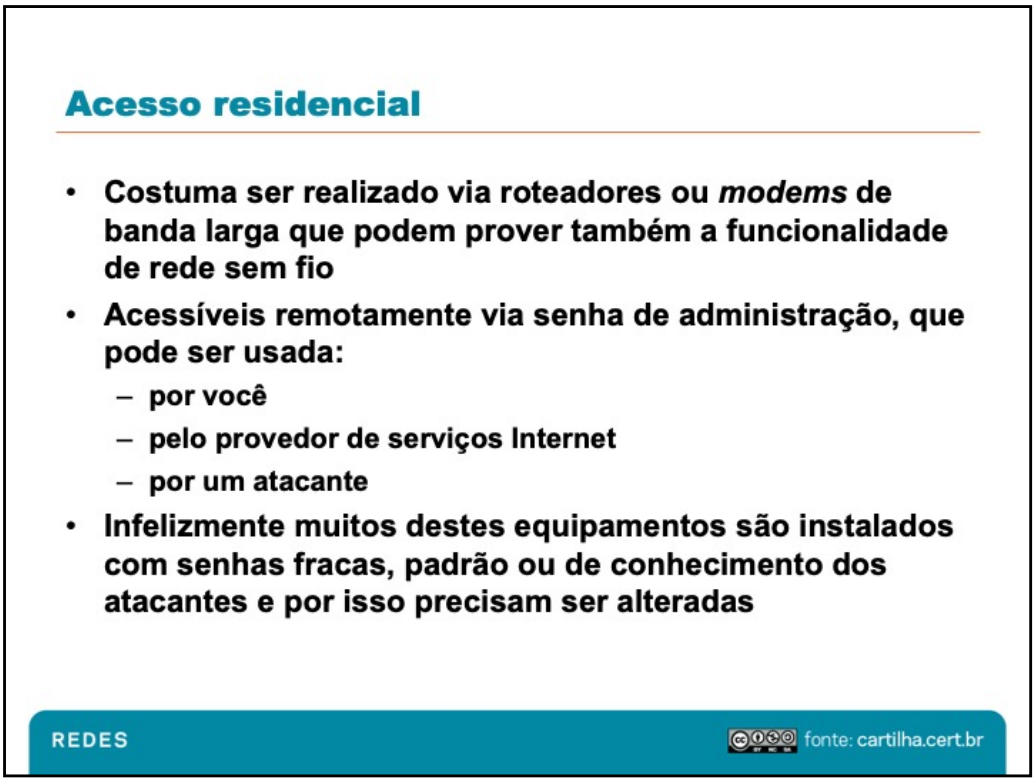
- Configure, quando possível, para que os programas sejam atualizados automaticamente;
- programe as atualizações automáticas para serem baixadas e aplicadas em horários em que seu computador esteja ligado e conectado à Internet. Alguns programas, por padrão, são configurados para que as atualizações sejam feitas de madrugada, período no qual grande parte dos computadores está desligada (as atualizações que não foram feitas no horário programado podem não ser feitas quando ele for novamente ligado);
- no caso de programas que não possuam o recurso de atualização automática, ou caso você opte por não utilizar este recurso, é importante visitar constantemente os *sites* dos fabricantes para verificar a existência de novas atualizações;
- utilize programas para verificação de vulnerabilidades.

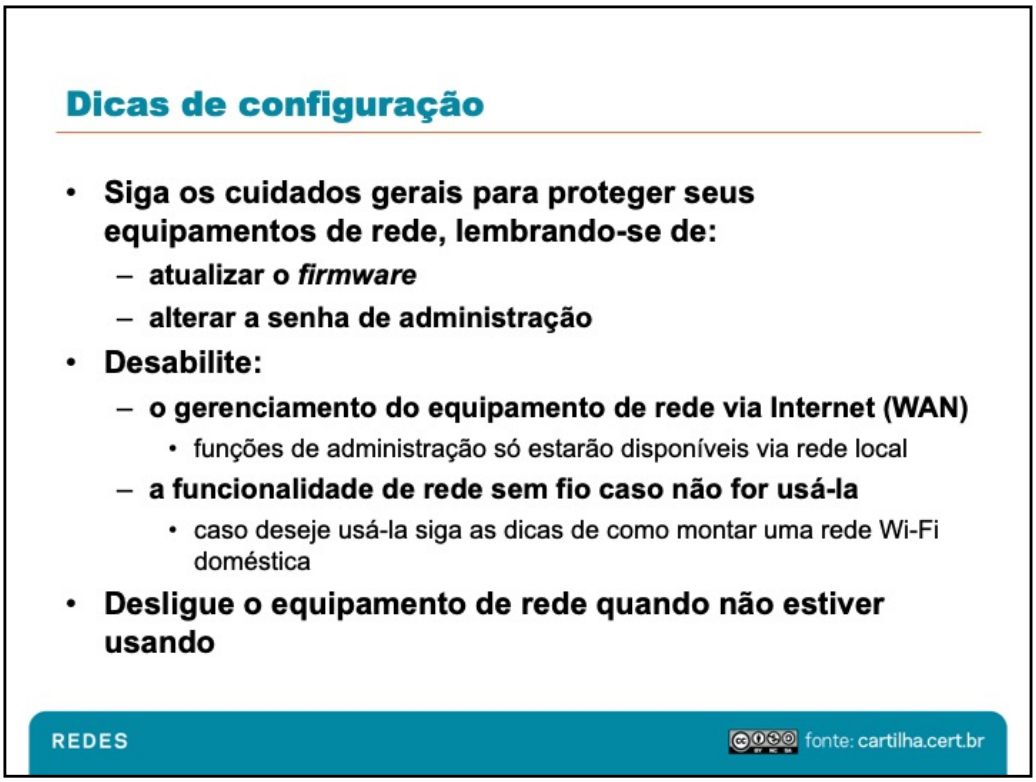


Faça regularmente *backup* dos seus dados. Para evitar que eles sejam perdidos em caso de furto ou mau funcionamento do computador (por exemplo, invasão, infecção por códigos maliciosos ou problemas de *hardware.*



Nos próximos *slides* são apresentadas algumas dicas de configuração segura de acesso Internet residencial.


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
REDES
fonte: cartilha.cert.br

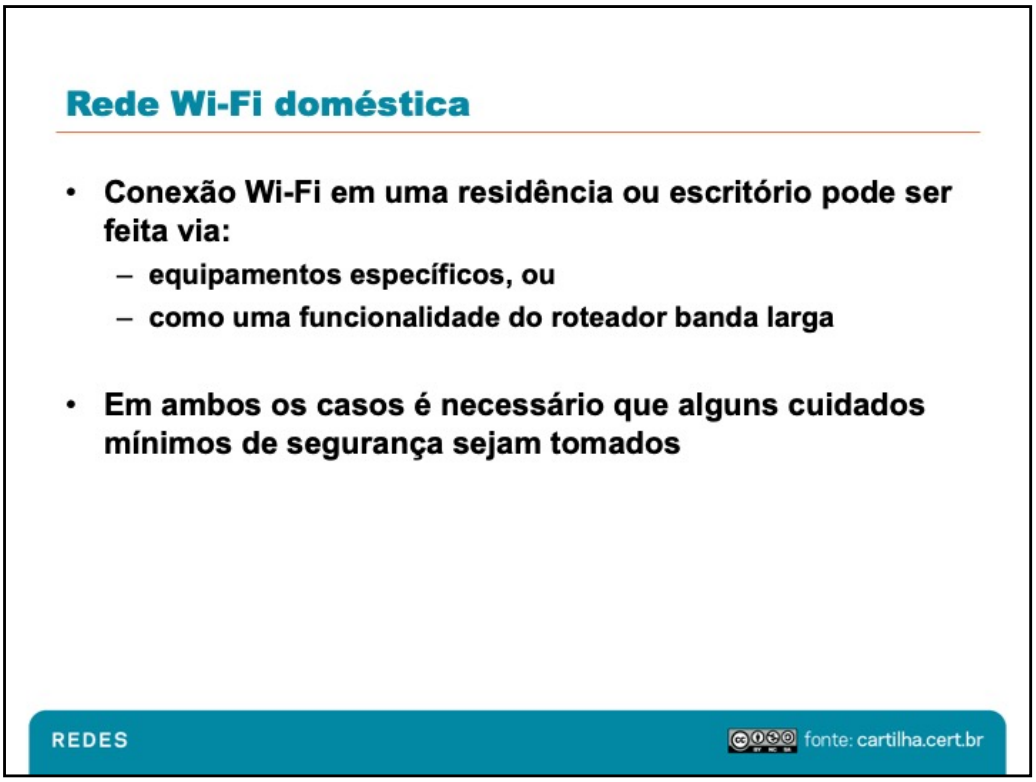

Dicas de configuração
• Siga os cuidados gerais para proteger seus equipamentos de rede, lembrando-se de:
– atualizar o *firmware*
– alterar a senha de administração
• Desabilite:
– o gerenciamento do equipamento de rede via Internet (WAN)
• funções de administração só estarão disponíveis via rede local
– 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
REDES
fonte: cartilha.cert.br

Wi-Fi (***Wi**reless **Fi**delity*) é um tipo de rede local que utiliza sinais de rádio para comunicação. Possui dois modos básicos de operação:

- **Infraestrutura:** normalmente o mais encontrado, utiliza um concentrador de acesso (*Access Point* - AP) ou um roteador *wireless*.
- **Ponto a ponto (*ad-hoc*):** permite que um pequeno grupo de máquinas se comunique diretamente, sem a necessidade de um AP.

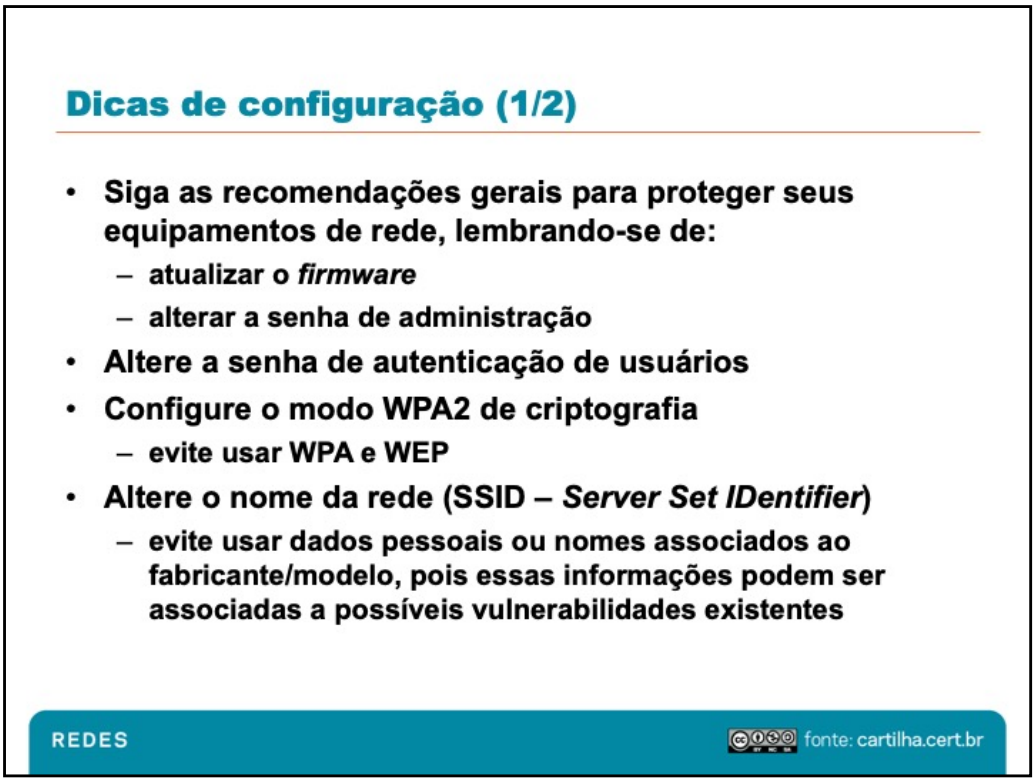
Redes Wi-Fi se tornaram populares pela mobilidade que oferecem e pela facilidade de instalação e de uso em diferentes tipos de ambientes.

Nos próximos *slides* são apresentadas algumas dicas de configuração segura de uma rede Wi-Fi doméstica.



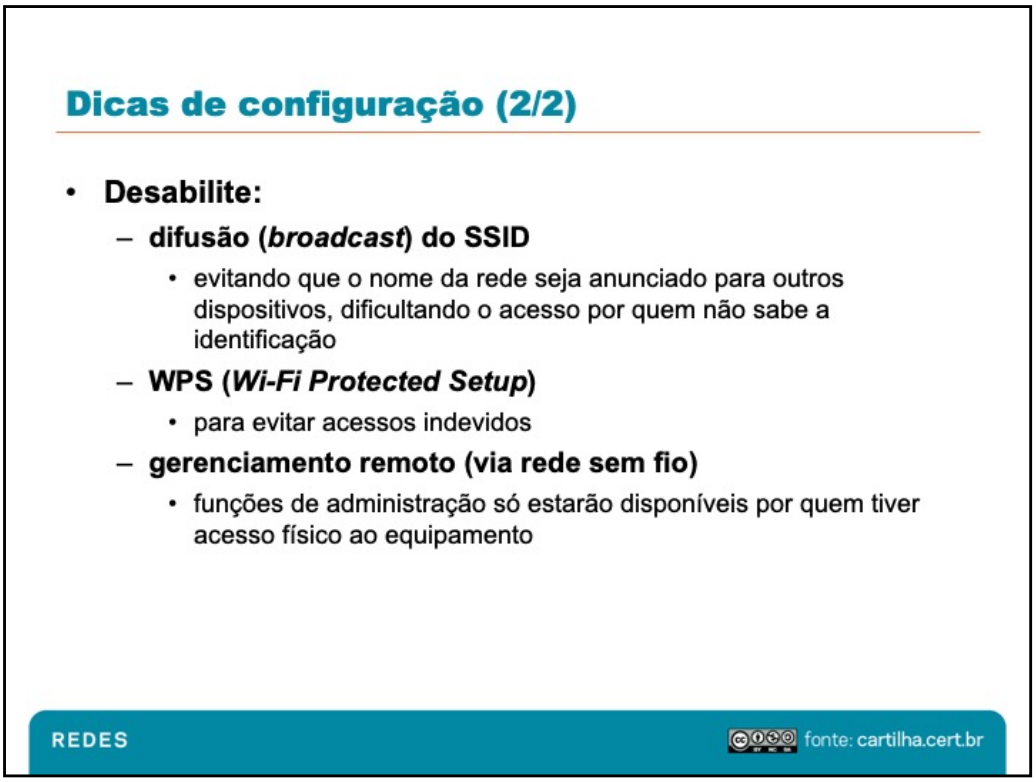
Embora sejam bastante convenientes, há alguns riscos que você deve considerar ao usar redes Wi-Fi, como:

- por se comunicarem por meio de sinais de rádio, não há a necessidade de acesso físico a um ambiente restrito, como ocorre com as redes cabeadas. Devido a isto, os dados transmitidos por clientes legítimos podem ser interceptados por qualquer pessoa próxima com um mínimo de equipamento (por exemplo, um *notebook* ou *tablet*);
- por terem instalação bastante simples, muitas pessoas as instalam em casa (ou mesmo em empresas, sem o conhecimento dos administradores de rede), sem qualquer cuidado com configurações mínimas de segurança, e podem vir a ser abusadas por atacantes, por meio de uso não autorizado ou de "sequestro";
- em uma rede Wi-Fi pública (como as disponibilizadas em aeroportos, hotéis e conferências) os dados que não estiverem criptografados podem ser indevidamente coletados por atacantes;
- uma rede Wi-Fi aberta pode ser propositadamente disponibilizada por atacantes para atrair usuários, a fim de interceptar o tráfego (e coletar dados pessoais) ou desviar a navegação para *sites* falsos.



Para resolver alguns dos riscos associados ao uso de redes Wi-Fi foram desenvolvidos mecanismos de segurança, como:

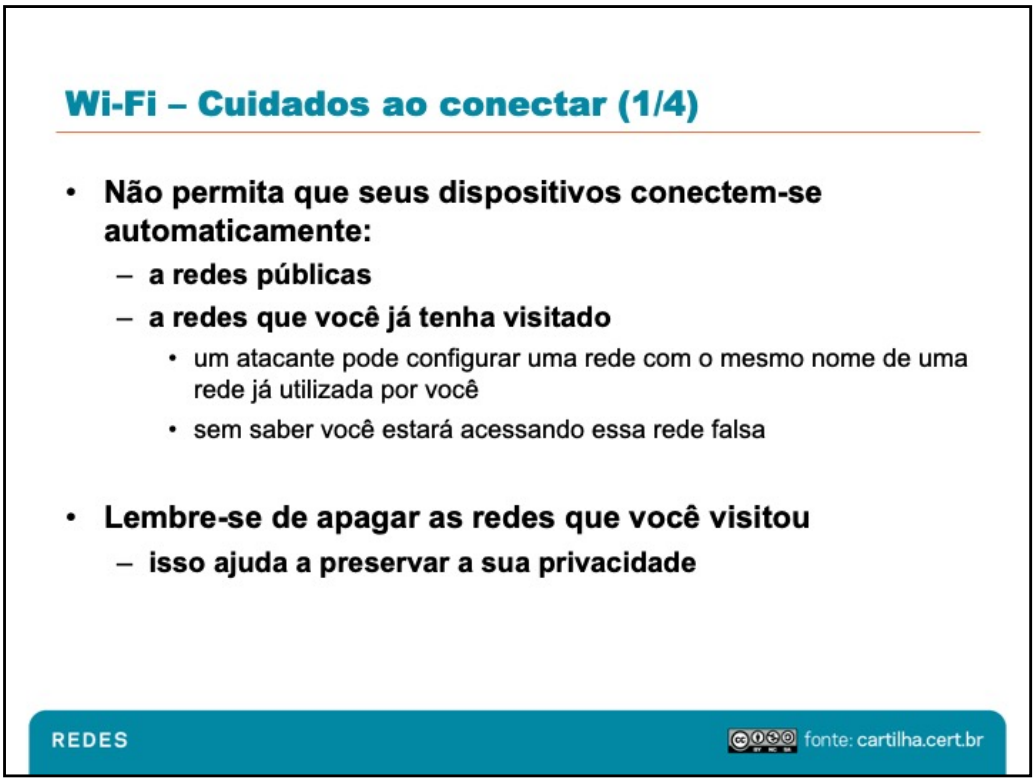
- **WEP (*Wired Equivalent Privacy*):** primeiro mecanismo de segurança a ser lançado. É considerado frágil e, por isto, o uso deve ser evitado.
- **WPA (*Wi-Fi Protected Access*):** mecanismo desenvolvido para resolver algumas das fragilidades do WEP. É o nível mínimo de segurança que é recomendado.
- **WPA-2**: similar ao WPA, mas com criptografia considerada mais forte. É o mecanismo mais recomendado.

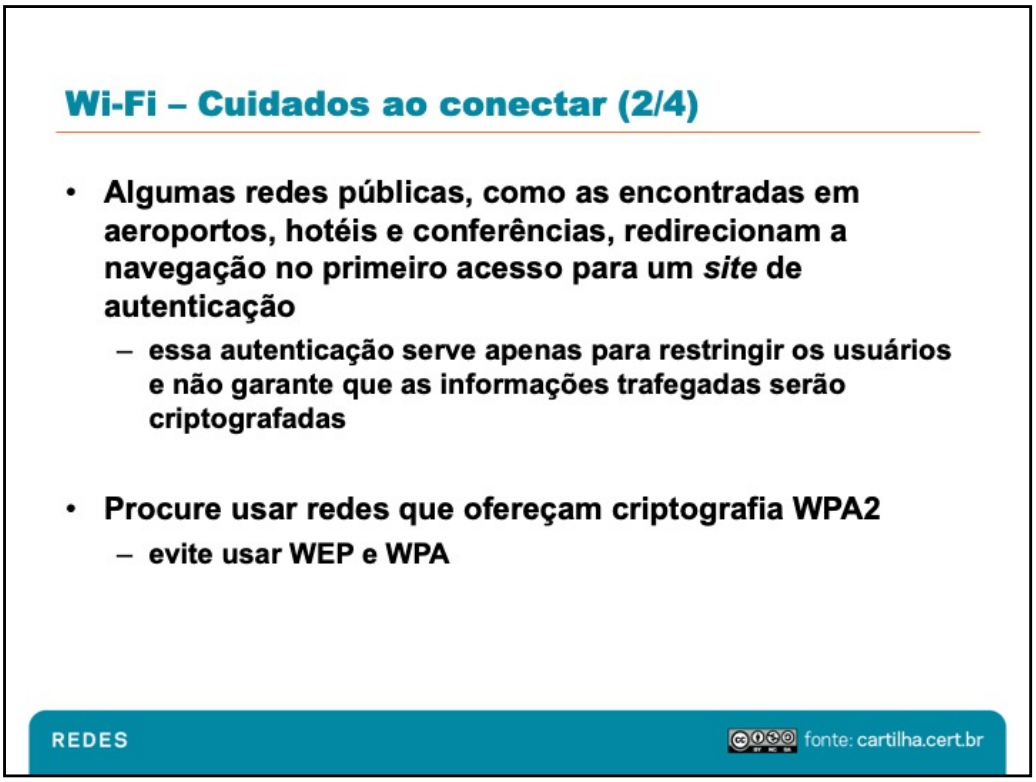


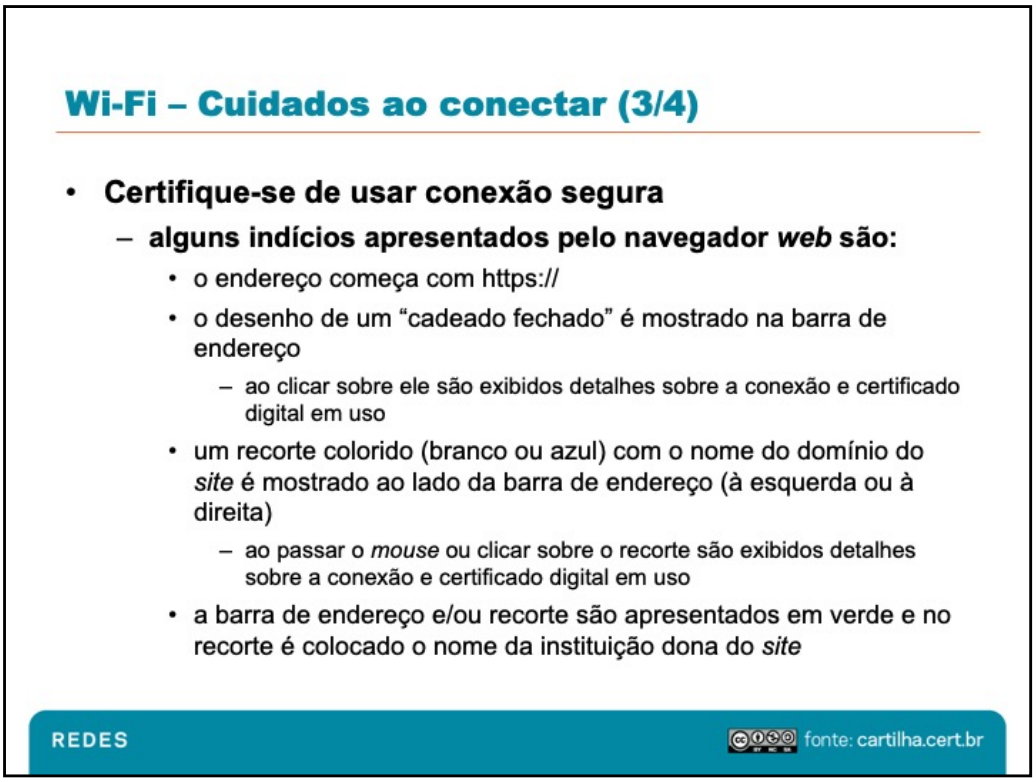
Altere as configurações padrão que acompanham o seu equipamento de rede. Alguns exemplos são:

- altere as senhas originais, tanto de administração como de autenticação de usuários;
- assegure-se de utilizar senhas bem elaboradas e difíceis de serem descobertas;
- altere o SSID (***S**erver **S**et **ID**entifier*);
- ao configurar o SSID procure não usar dados pessoais e nem nomes associados ao fabricante ou modelo, pois isto facilita a identificação de características técnicas do equipamento e pode permitir que essas informações sejam associadas a possíveis vulnerabilidades existentes;
- desabilite a difusão (*broadcast*) do SSID, evitando que o nome da rede seja anunciado para outros dispositivos;
- desabilite o gerenciamento do equipamento via rede sem fio, de tal forma que, para acessar funções de administração, seja necessário conectar-se diretamente a ele usando uma rede cabeada. Desta maneira, um possível atacante externo (via rede sem fio) não será capaz de acessar o AP para promover mudanças na configuração.

Nos próximos *slides* são apresentados alguns cuidados que devem ser tomados 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
REDES
fonte: cartilha.cert.br

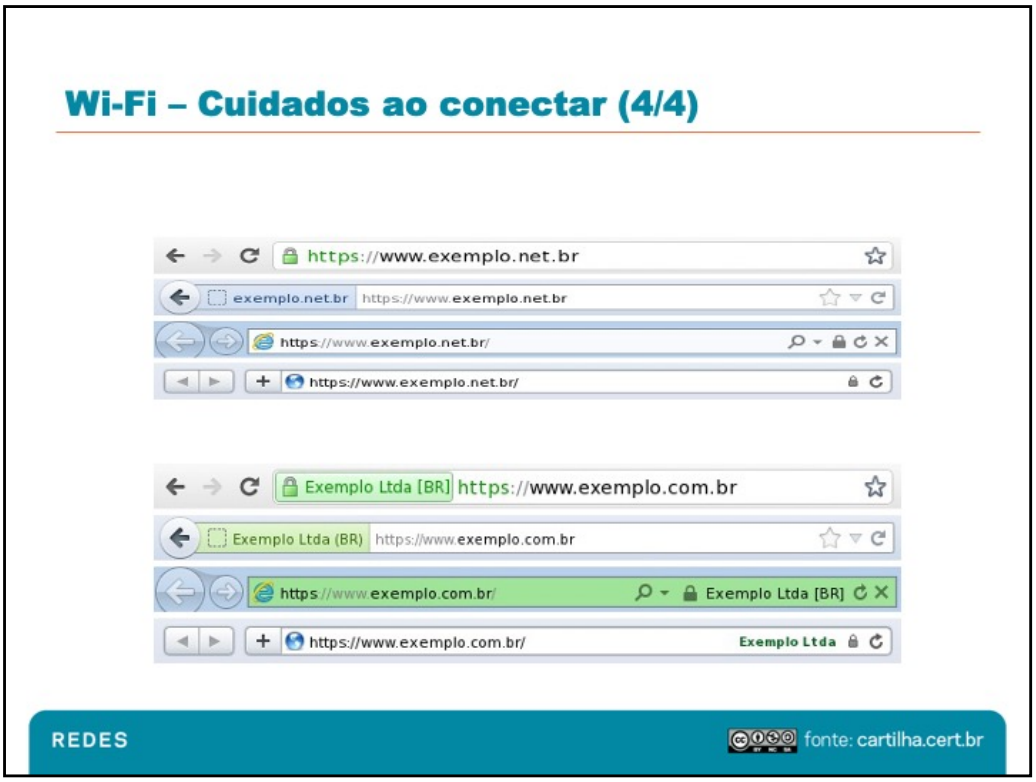

Wi-Fi – Cuidados ao conectar (2/4)
• Algumas redes públicas, como as encontradas em aeroportos, hotéis e conferências, redirecionam a navegação no primeiro acesso para um *site* de autenticação
– essa autenticação serve apenas para restringir os usuários e não garante que as informações trafegadas serão criptografadas
• Procure usar redes que ofereçam criptografia WPA2
– evite usar WEP e WPA
REDES
fonte: cartilha.cert.br



Conexão segura é a que deve ser utilizada quando dados sensíveis são transmitidos. Provê autenticação, integridade e confidencialidade, como requisitos de segurança.

Alguns indícios de conexão segura apresentados pela navegador *web* são:

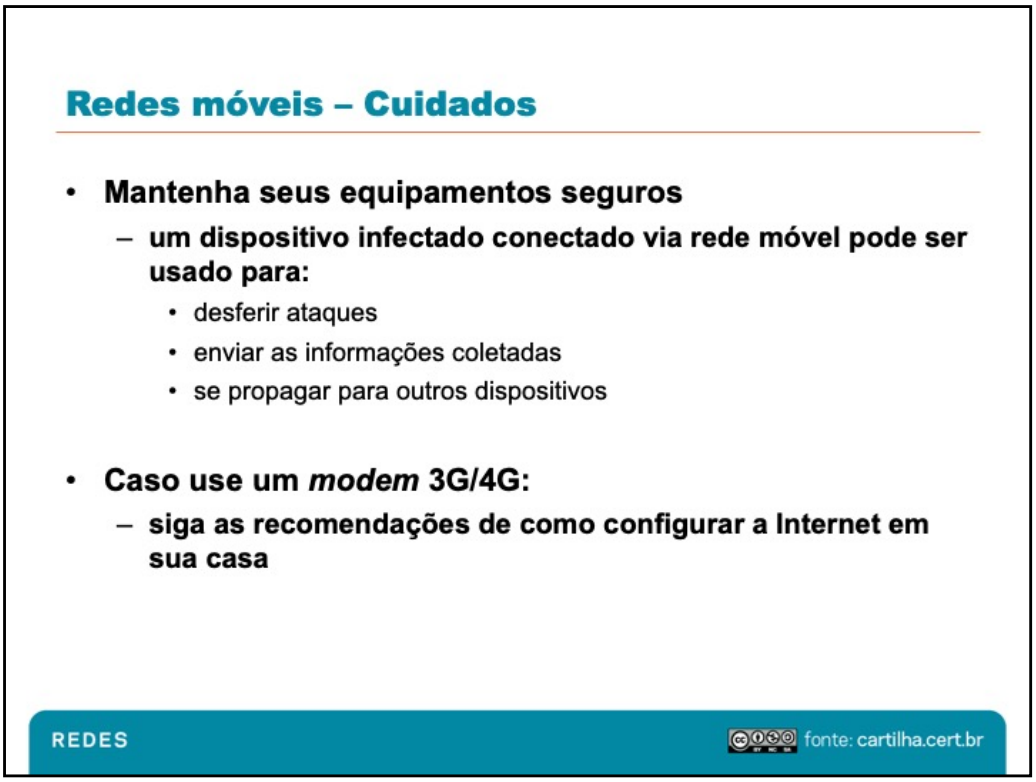
- o endereço começa com https://;
- o desenho de um cadeado fechado é mostrado na barra de endereços. Ao clicar sobre ele, detalhes sobre a conexão e sobre o certificado digital em uso são exibidos;
- um recorte colorido (branco ou azul) com o nome do domínio do *site* é mostrado ao lado da barra de 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.*



Este *slide* apresenta exemplos de:

- conexão segura em diversos navegadores;
- conexão segura usando EV SSL em diversos navegadores.

Nos próximos *slides* são apresentados alguns cuidados que se deve ter ao usar redes móveis (3G/4G).



A banda larga móvel refere-se às tecnologias de acesso sem fio, de longa distância, por meio da rede de telefonia móvel, especialmente 3G e 4G.

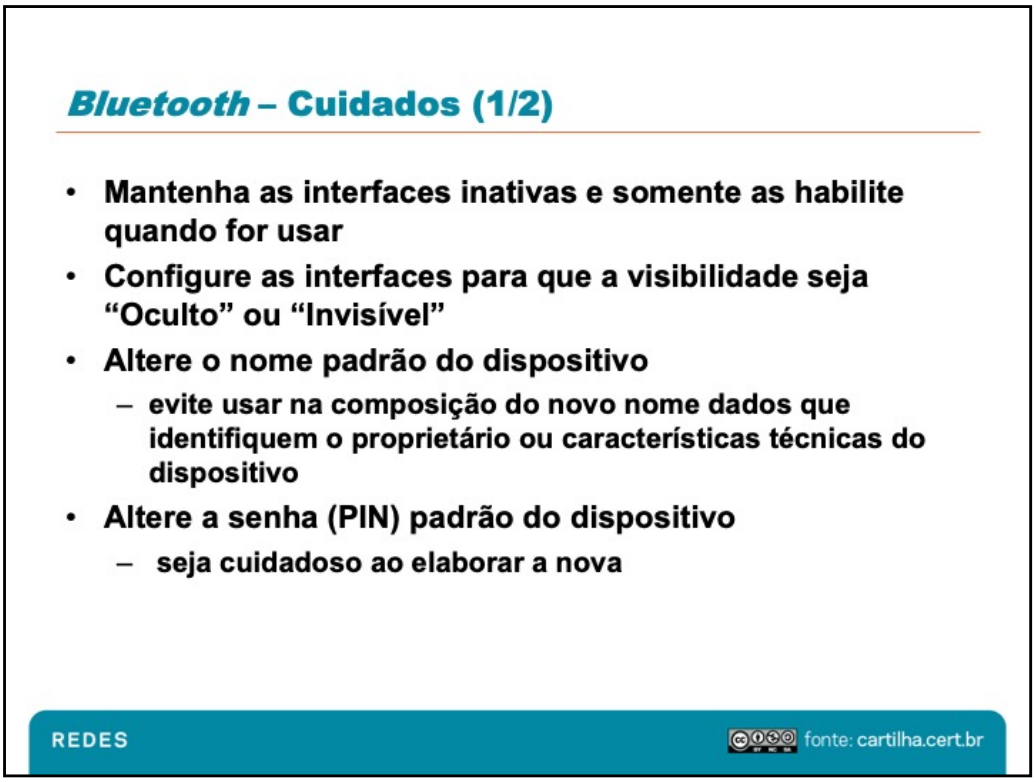
Este tipo de tecnologia está disponível em grande quantidade de dispositivos móveis (como celulares, *smartphones* e *tablets*) e é uma das responsáveis pela popularização destes dispositivos e das redes sociais. Além disto, também pode ser adicionada a computadores e dispositivos móveis que ainda não tenham esta capacidade, por meio do uso de *modems* específicos.

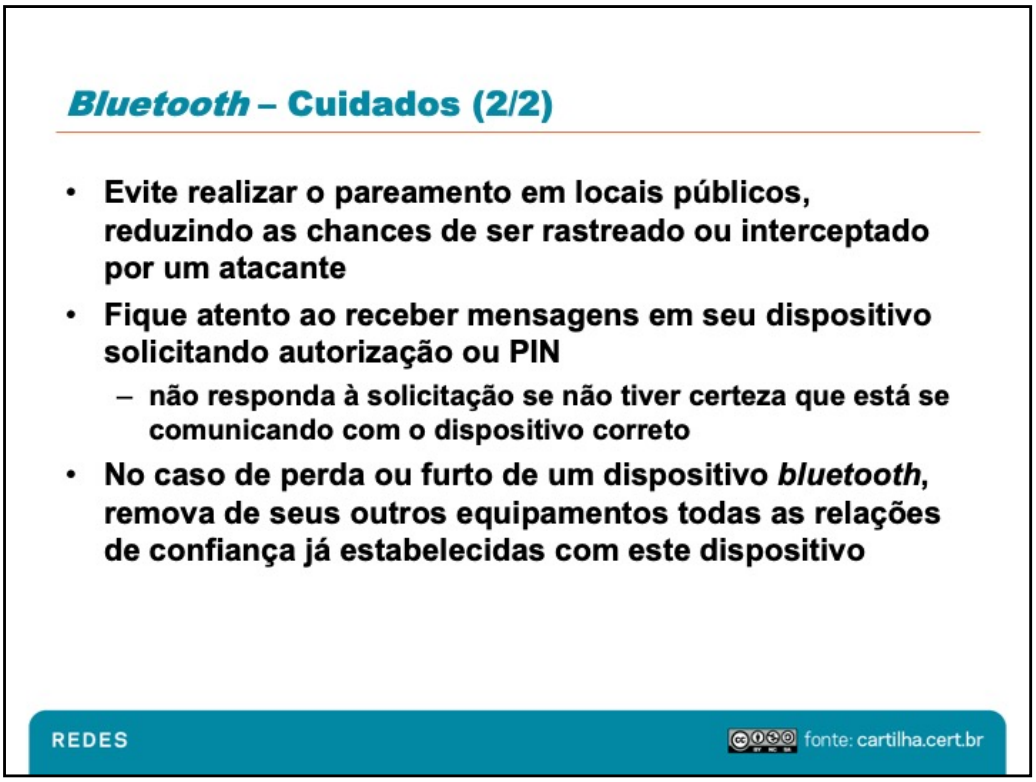
Assim como no caso da banda larga fixa, dispositivos com suporte a este tipo de tecnologia podem ficar conectados à Internet por longos períodos e permitem que o usuário esteja *online*, independente de localização. Por isto, são bastante visados por atacantes para a prática de atividades maliciosas.

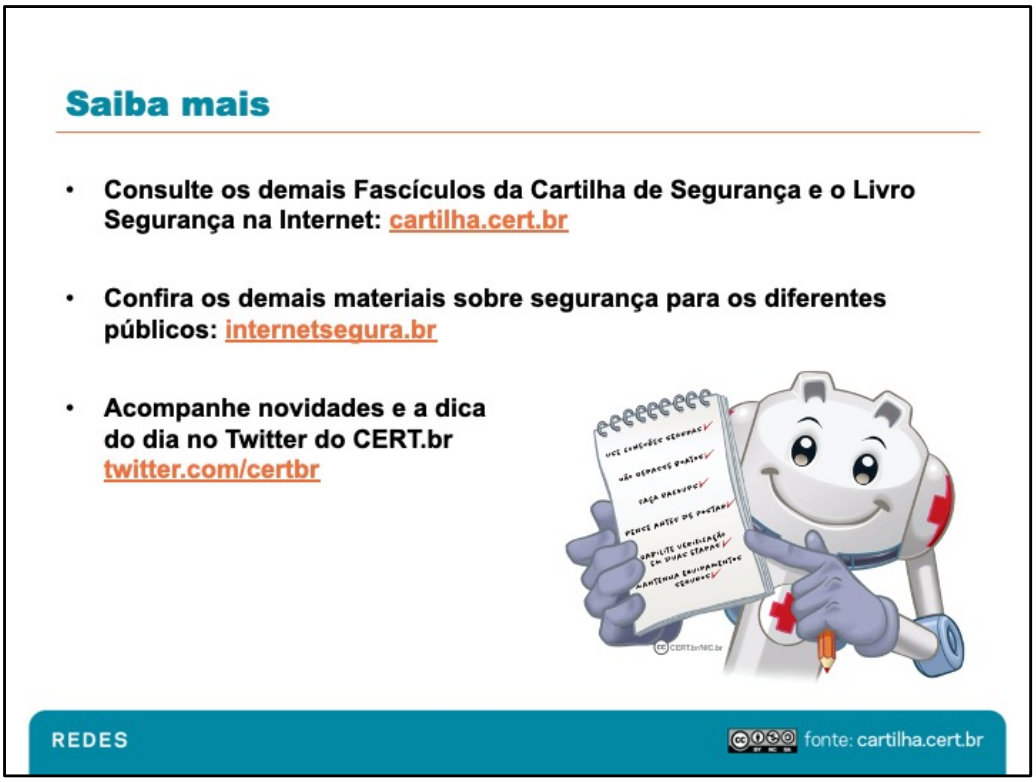
Bluetooth é um padrão para tecnologia de comunicação de dados e voz, baseado em radiofrequência e destinado à conexão de dispositivos em curtas distâncias, permitindo a formação de redes pessoais sem fio. Está disponível em uma extensa variedade de equipamentos, como dispositivos móveis, videogames, *mouses*, teclados, impressoras, sistemas de áudio, aparelhos de GPS e monitores de frequência cardíaca. A quantidade de aplicações também é vasta, incluindo sincronismo de dados entre dispositivos, comunicação entre computadores e periféricos e transferência de arquivos.

Embora traga muitos benefícios, o uso desta tecnologia traz também riscos, visto que está sujeita às várias ameaças que acompanham as redes em geral, como varredura, furto de dados, uso indevido de recursos, ataque de negação de serviço, interceptação de tráfego e ataque de força bruta.

Um agravante, que facilita a ação dos atacantes, é que muitos dispositivos vêm, por padrão, com o *bluetooth* ativo. Desta forma, muitos usuários não percebem que possuem este tipo de conexão ativa e não se preocupam em adotar uma postura preventiva.


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
REDES
fonte: cartilha.cert.br


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
REDES
fonte: cartilha.cert.br



Novidades e dicas diárias podem ser obtidas por meio do RSS da Cartilha e do Twitter do CERT.br:

- Twitter: https://twitter.com/certbr
- RSS: https://cartilha.cert.br/rss/cartilha-rss.xml

No *site* da Cartilha de Segurança para Internet (https://cartilha.cert.br/) você encontra diversos materiais, como dicas rápidas sobre vários assuntos e outros fascículos, com temas como Boatos, *Internet Banking*, Senhas e Verificação em Duas Etapas, entre outros.

No *site* Internet Segura (https://internetsegura.br/) você encontra materiais de interesse geral e para diversos públicos específicos, como crianças, adolescentes, pais, educadores, pessoas com mais de 60 anos e técnicos. Além dos materiais produzidos pelo NIC.br, há também iniciativas de outras entidades e instituições, com diversas informações sobre uso seguro da Internet.