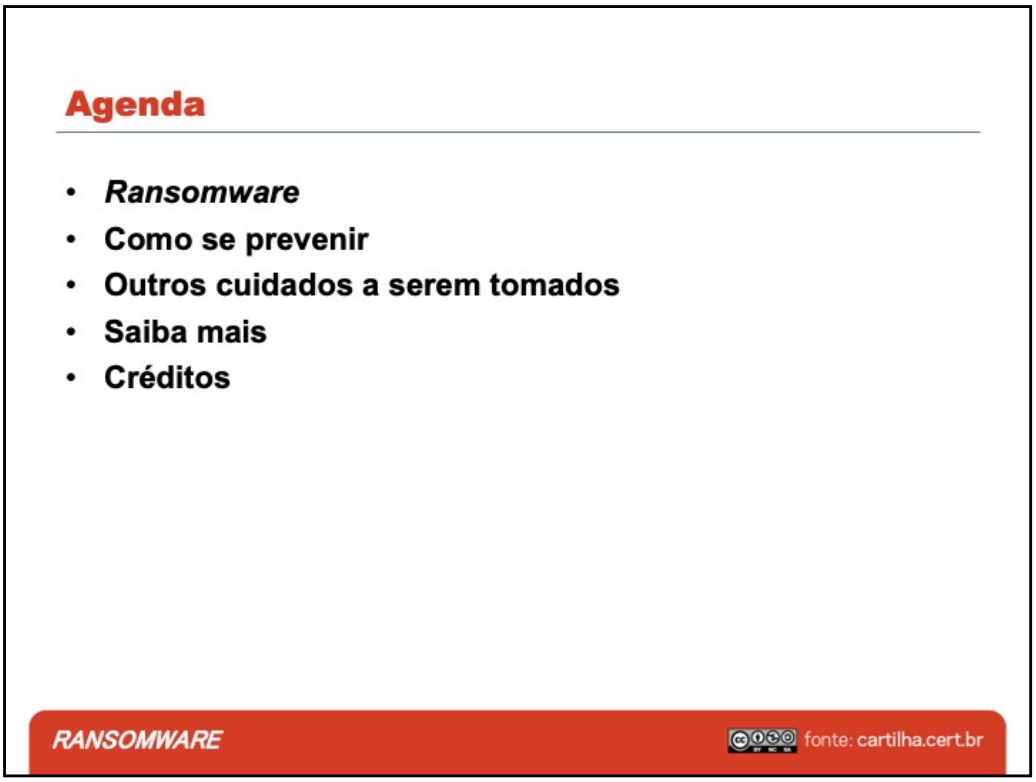
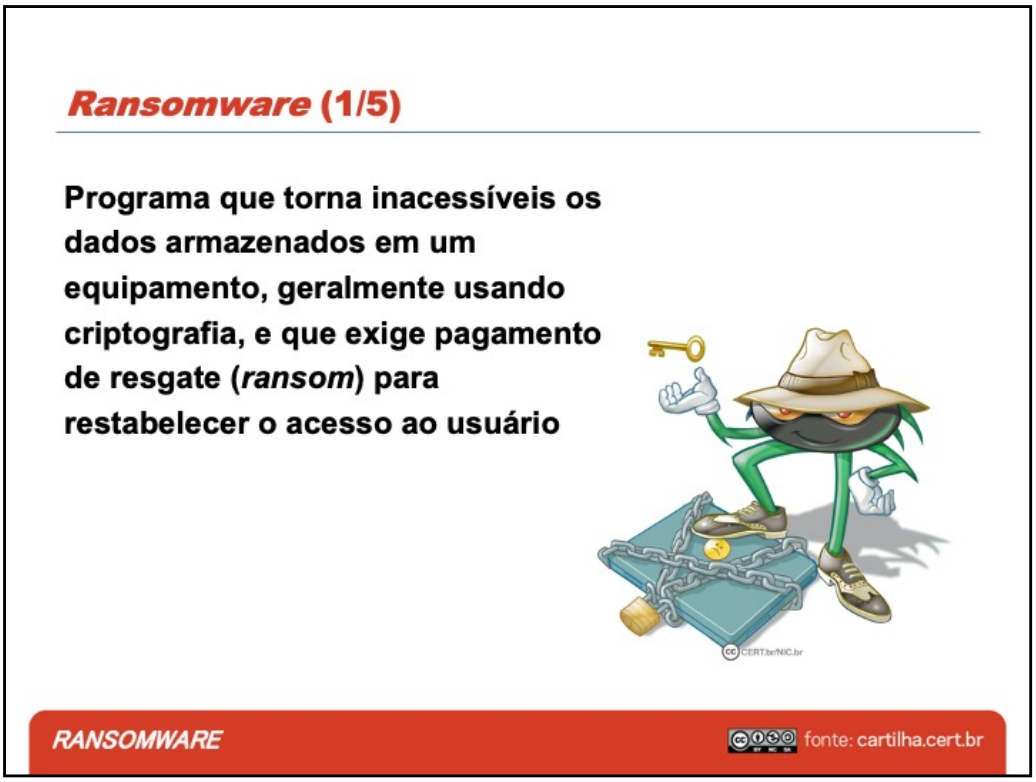


- ***Ransomware***: define o que é o *ransomware*.
- **Como se prevenir**: apresenta as principais medidas preventivas para evitar o *ransomware*.
- **Outros cuidados a serem tomados:** apresenta os cuidados extras a serem tomados para evitar que os equipamentos sejam infectados com *ransomware*.
- **Saiba 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*.

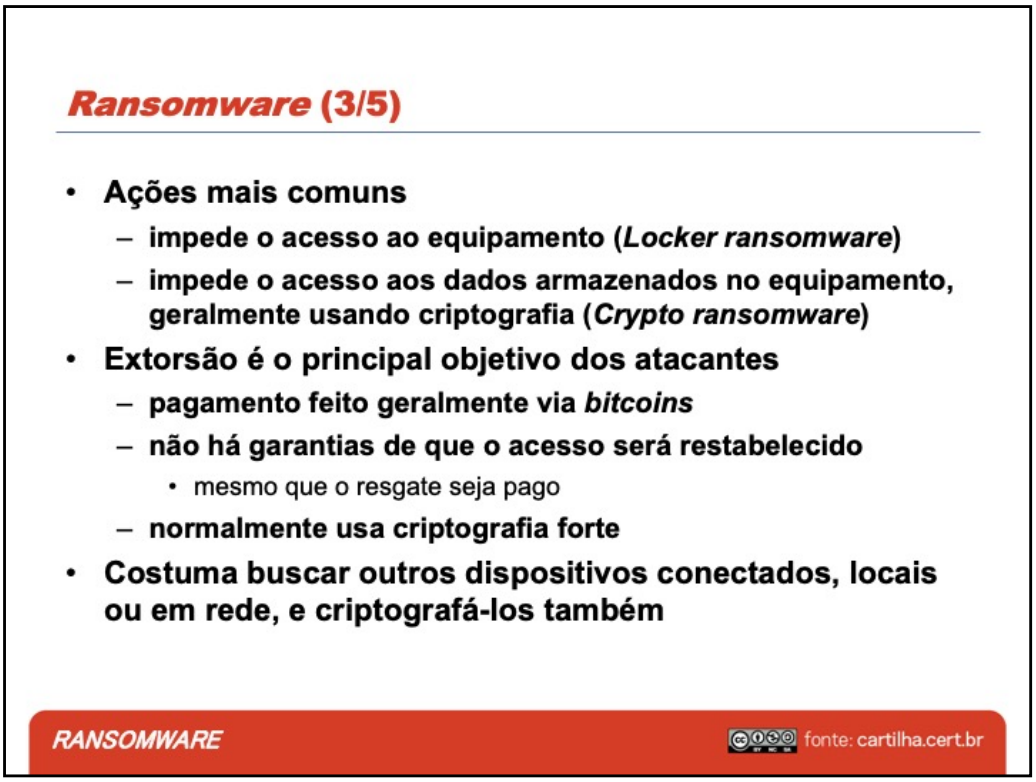


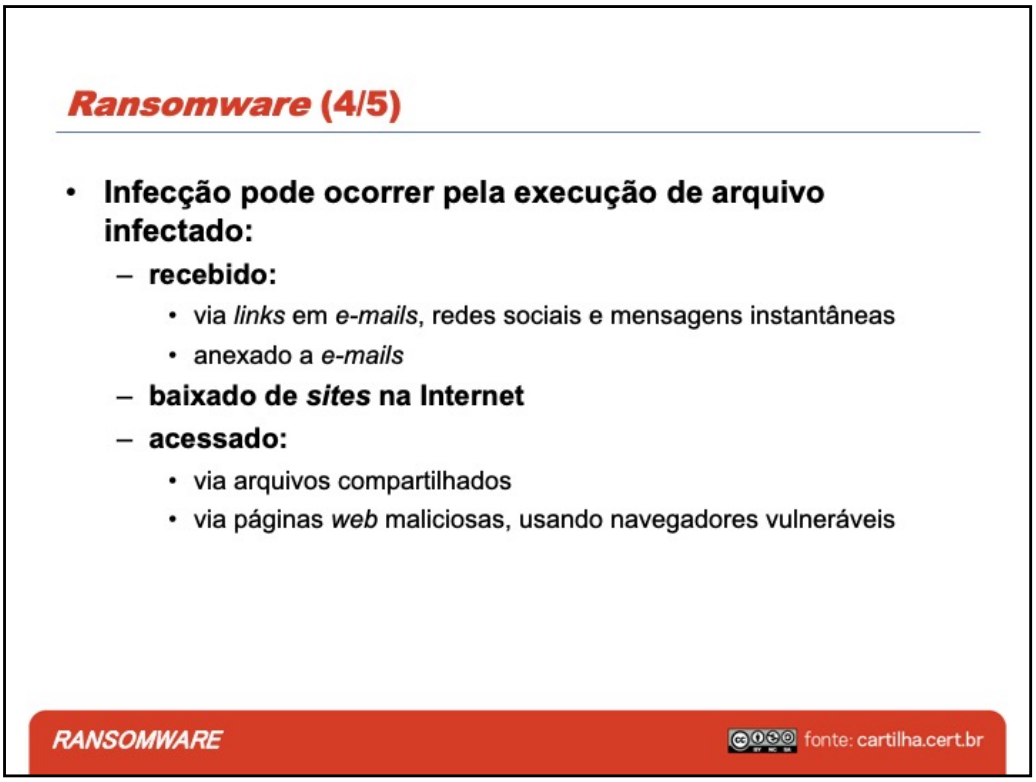
Definir e identificar as características dos diferentes tipos de códigos maliciosos têm se tornado tarefas cada vez mais difíceis, devido às diferentes classificações adotadas pelos fabricantes de antivírus e ao surgimento de variantes que mesclam características dos demais códigos. Dessa forma, as definições apresentadas nestes *slides* baseiam-se no entendimento dos autores da Cartilha de Segurança para Internet e, portanto, não são definitivas e podem ser diferentes de outras fontes de consulta.

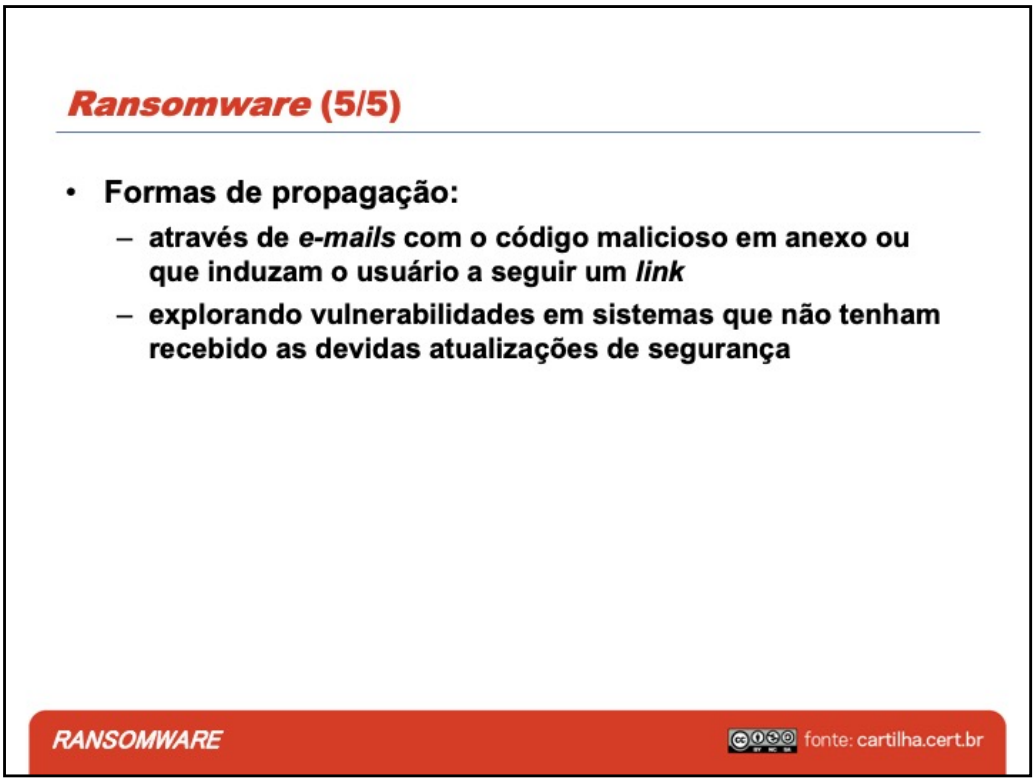
***Ransomware* (2/5)**

- **Tipo de código malicioso**
  - **assim como vírus, *trojan*, *backdoor*, *worm*, *bot* e *spyware***
- **Pode infectar:**
  - **computadores**
    - como *desktop*, *notebook* e servidores
  - **equipamentos de rede**
    - como *modems*, *switches* e roteadores
  - **dispositivos móveis**
    - como *tablets*, celulares e *smartphones*

RANSOMWARE fonte: cartilha.cert.br


Ransomware (3/5)
• Ações mais comuns
– impede o acesso ao equipamento (Locker ransomware)
– impede o acesso aos dados armazenados no equipamento, geralmente usando criptografia (Crypto ransomware)
• Extorsão é o principal objetivo dos atacantes
– pagamento feito geralmente via bitcoins
– não há garantias de que o acesso será restabelecido
• mesmo que o resgate seja pago
– normalmente usa criptografia forte
• Costuma buscar outros dispositivos conectados, locais ou em rede, e criptografá-los também
RANSOMWARE
fonte: cartilha.cert.br

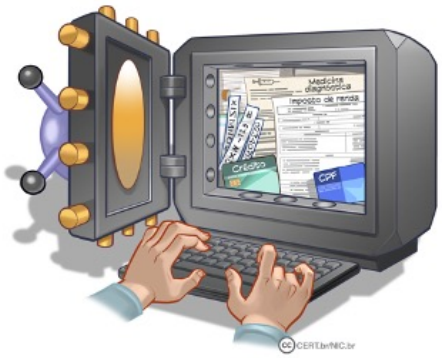

Ransomware (4/5)
• Infecção pode ocorrer pela execução de arquivo infectado:
– recebido:
• via links em e-mails, redes sociais e mensagens instantâneas
• anexado a e-mails
– baixado de sites na Internet
– acessado:
• via arquivos compartilhados
• via páginas web maliciosas, usando navegadores vulneráveis
RANSOMWARE
fonte: cartilha.cert.br


Ransomware (5/5)
• Formas de propagação:
– através de e-mails com o código malicioso em anexo ou que induzam o usuário a seguir um link
– explorando vulnerabilidades em sistemas que não tenham recebido as devidas atualizações de segurança
RANSOMWARE
fonte: cartilha.cert.br


Como
se prevenir
BACKUP
CERT.br/NIC.br
fonte: cartilha.cert.br

Não deixe que a infecção ocorra

- **A melhor prevenção é impedir a infecção inicial**
- **Nem sempre é possível reverter as ações danosas já feitas ou recuperar totalmente os dados**

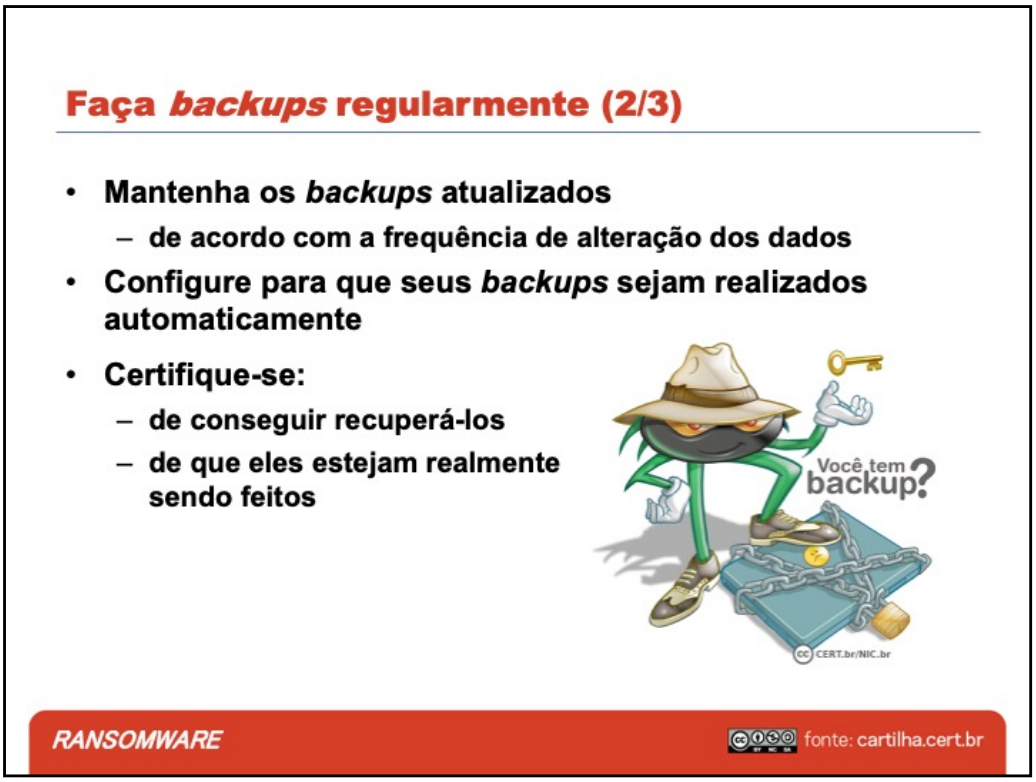


RANSOMWARE fonte: cartilha.cert.br

Faça *backups* regularmente (1/3)

Backup* é a solução mais efetiva contra *ransomware

RANSOMWARE fonte: cartilha.cert.br



- Mantenha *backups* em locais seguros, bem condicionados e com acesso restrito;
- além dos *backups* periódicos, sempre faça *backups* antes de efetuar grandes alterações no sistema e de enviar o equipamento para manutenção;
- armazene dados sensíveis em formato criptografado;
- cuidado com mídias obsoletas;
- assegure-se de conseguir recuperar seus *backups*;
- mantenha seus *backups* organizados e identificados;
- copie dados que você considere importantes e evite aqueles que podem ser obtidos de fontes externas confiáveis, como os referentes ao sistema operacional ou aos programas instalados.

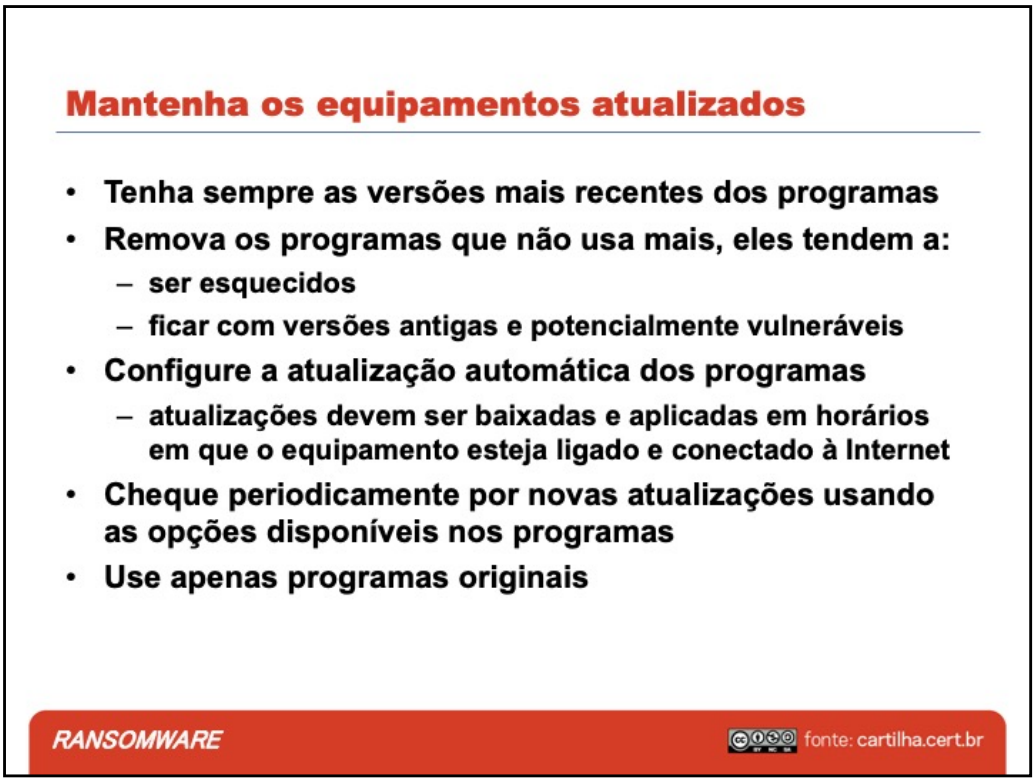
Faça *backups* regularmente (3/3)

- **Nunca recupere um *backup* se desconfiar que ele contém dados não confiáveis**
- **Mantenha os *backups* desconectados do sistema**
  - **para que não sejam também criptografados**
- **Faça cópias redundantes**
  - **para evitar perder seus dados:**
    - em incêndio, inundação, furto ou pelo uso de mídias defeituosas
    - caso uma das cópias seja infectada

RANSOMWARE fonte: cartilha.cert.br

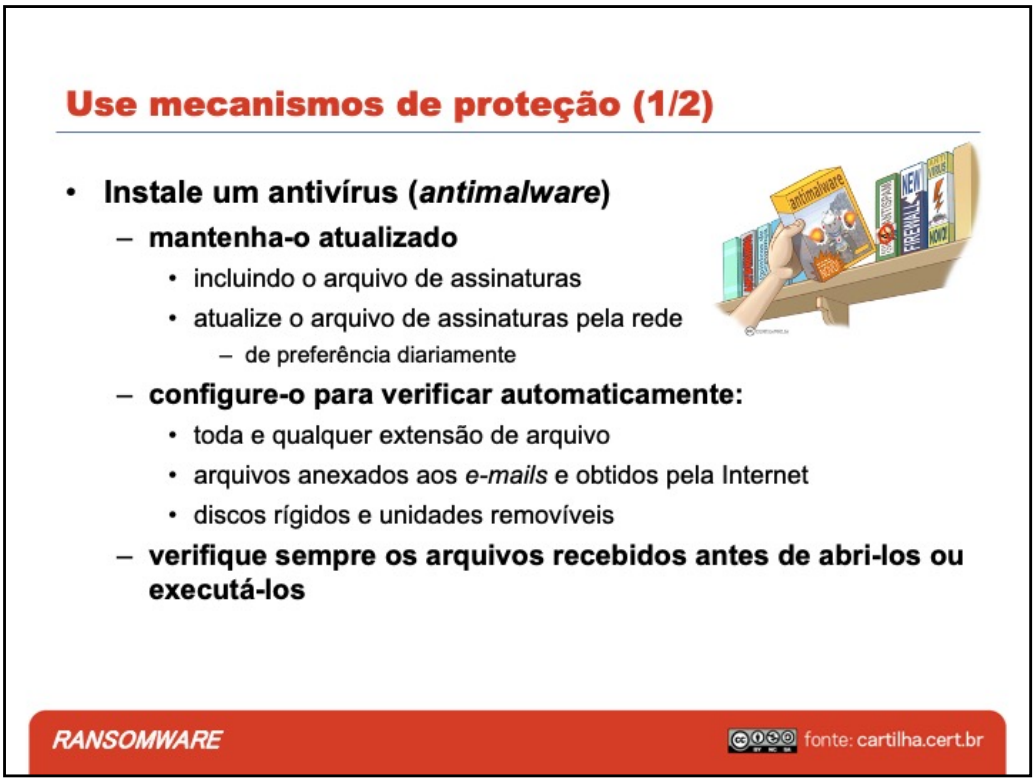
Outros cuidados a serem tomados

fonte: cartilha.cert.br



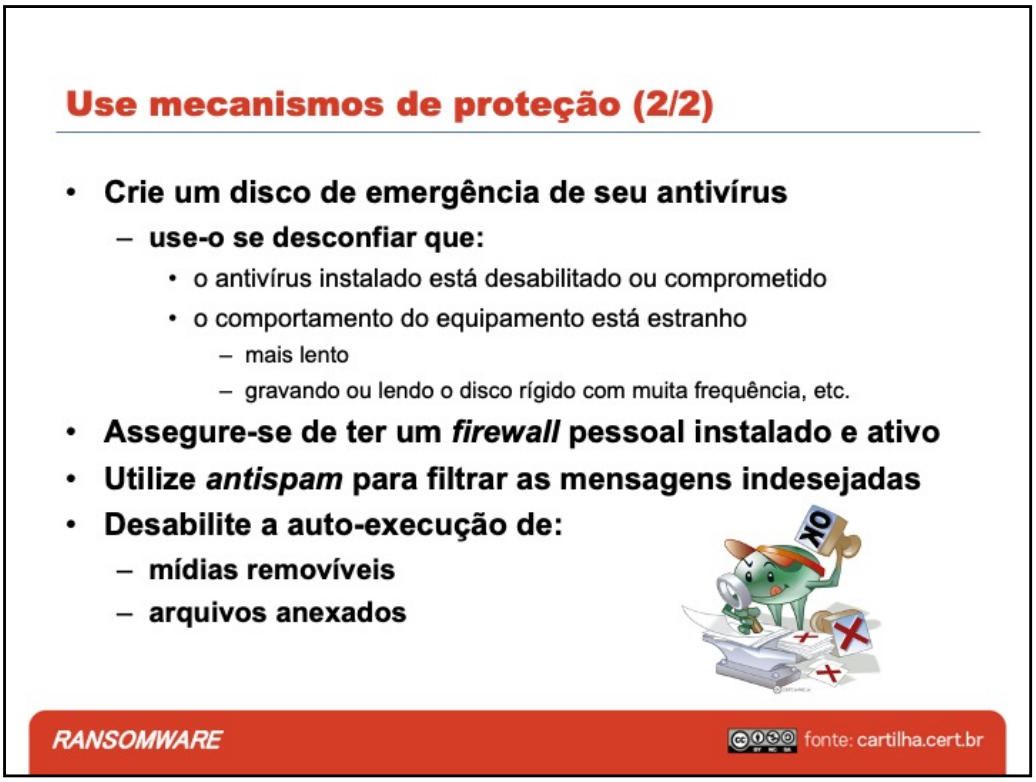
Fabricantes de programas (*software*) costumam lançar novas versões quando há recursos a serem adicionados e vulnerabilidades a serem corrigidas. Sempre que uma nova versão for lançada, ela deve ser prontamente instalada, pois isto pode ajudar a proteger seu equipamento da ação de atacantes e códigos maliciosos. Além disto, alguns fabricantes deixam de dar suporte e de desenvolver atualizações para versões antigas, o que significa que vulnerabilidades que possam vir a ser descobertas não serão corrigidas.

- Remova programas que você não utiliza mais. Programas não usados tendem a ser esquecidos e a ficar com versões antigas (e potencialmente vulneráveis);
- remova as versões antigas. Existem programas que permitem que duas ou mais versões estejam instaladas ao mesmo tempo. Nestes casos, você deve manter apenas a versão mais recente e remover as mais antigas;
- tenha o hábito de verificar a existência de novas versões, por meio de opções disponibilizadas pelos próprios programas ou acessando diretamente os *sites* dos fabricantes.



Ferramentas *antimalware (*antivírus, *antispyware*, *antirootkit* e *antitrojan)* são aquelas que procuram detectar e, então, anular ou remover os códigos maliciosos de um equipamento. Entre as diferentes ferramentas existentes, a que engloba a maior quantidade de funcionalidades é o antivírus.

Configure seu antivírus para verificar todos os formatos de arquivo pois, apesar de inicialmente algumas extensões terem sido mais usadas para a disseminação de códigos maliciosos, atualmente isso já não é mais válido.

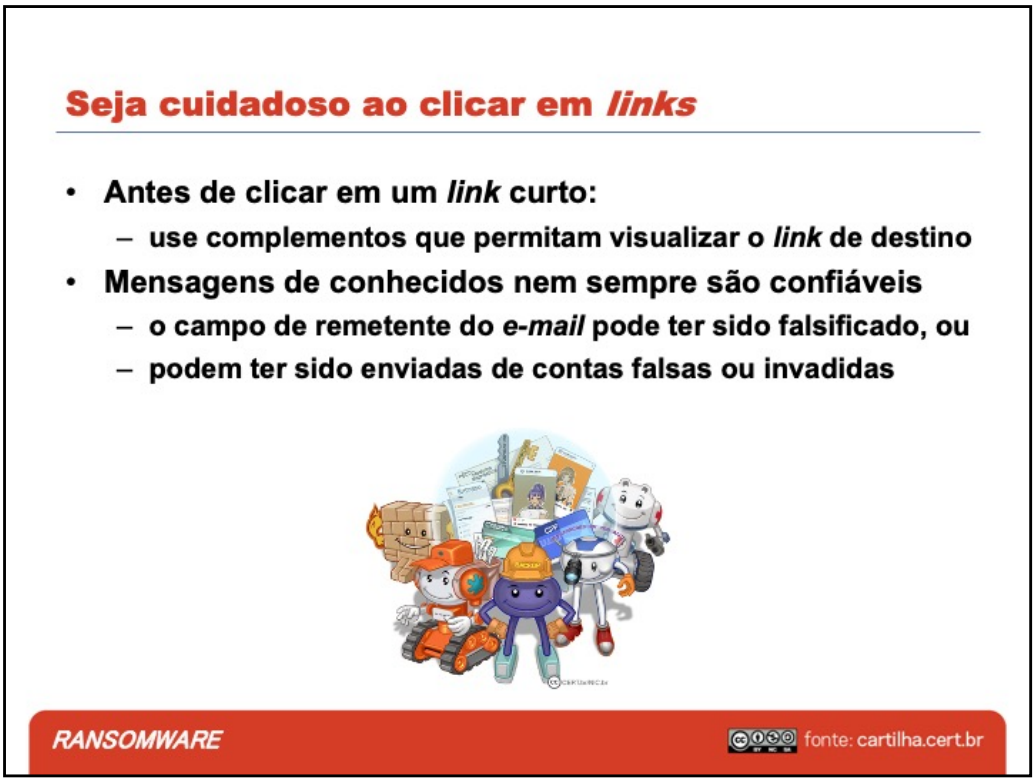


Firewall pessoal é um tipo específico de *firewall* que é utilizado para proteger um equipamento contra acessos não autorizados vindos da Internet. Os programas antivírus, apesar da grande quantidade de funcionalidades, não são capazes de impedir que um atacante tente explorar, via rede, alguma vulnerabilidade existente em seu equipamento e nem de evitar o acesso não autorizado. Devido a isto, além da instalação do antivírus, é necessário que você utilize um *firewall* pessoal.

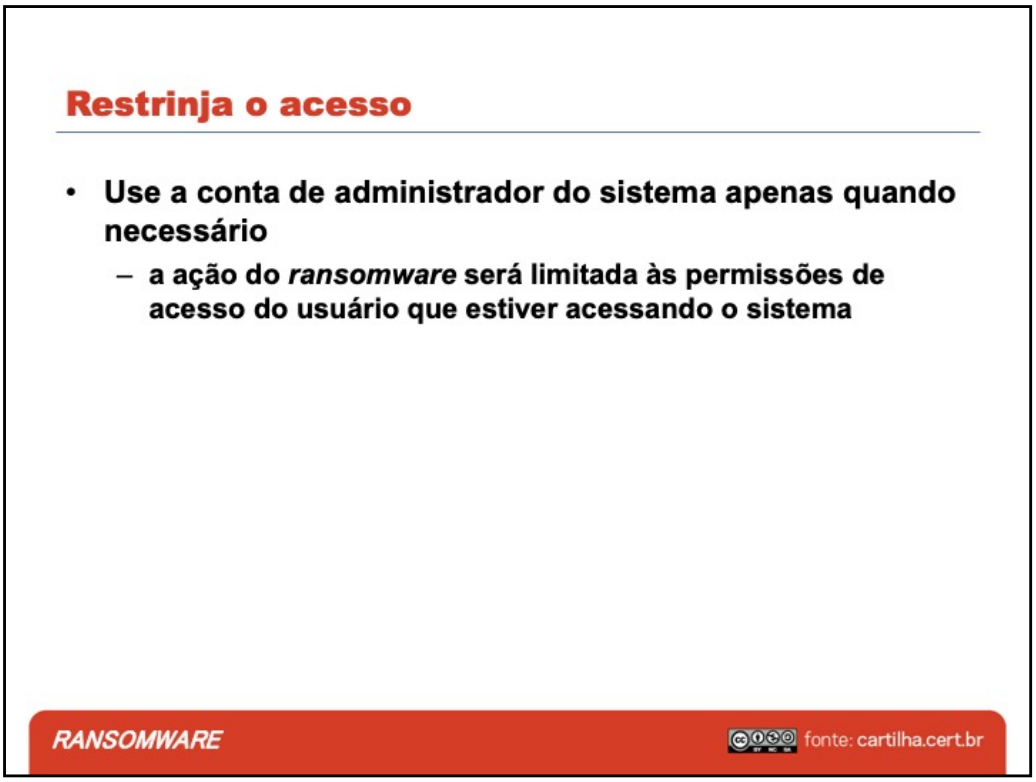
Verifique periodicamente os *logs* gerados pelo seu *firewall* pessoal, sistema operacional e antivírus (observe se há registros que possam indicar algum problema de segurança).

Plug-ins, complementos e extensões são programas geralmente desenvolvidos por terceiros e que podem prover funcionalidades extras. Costumam ser disponibilizados em repositórios, onde podem ser baixados livremente ou comprados. Alguns repositórios efetuam controle rígido antes de disponibilizá-los, outros utilizam classificações referentes ao tipo de revisão, enquanto outros não efetuam controle. Apesar de grande parte ser confiável, há a chance de existir programas especificamente criados para executar atividades maliciosas ou que, devido a erros de implementação, possam executar ações danosas em seu equipamento.

- Assegure-se de ter mecanismos de segurança instalados e atualizados, antes de instalar programas desenvolvidos por terceiros;
- mantenha os programas instalados sempre atualizados;
- procure obter arquivos apenas de fontes confiáveis;
- veja comentários de outros usuários sobre o programa, antes de instalá-lo;
- seja cuidadoso ao instalar programas que ainda estejam em processo de revisão;
- denuncie aos responsáveis pelo repositório caso identifique programas maliciosos.

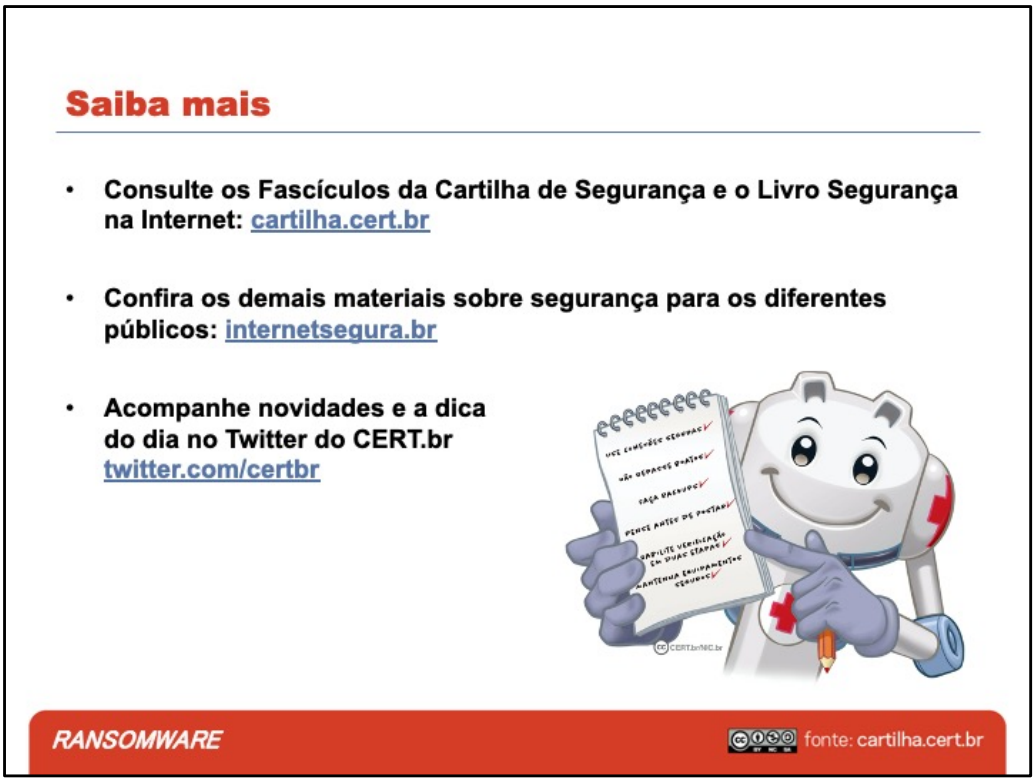


Alguns mecanismos, como os programas antivírus, são importantes para proteger seu equipamento contra ameaças já conhecidas, mas podem não servir para aquelas ainda não detectadas. Novos códigos maliciosos podem surgir, a velocidades nem sempre acompanhadas pela capacidade de atualização dos mecanismos de segurança e, por isto, adotar uma postura preventiva é tão importante quanto as outras medidas de segurança aplicadas.



Quando um programa é executado, ele herda as permissões da conta do usuário que o executou e pode realizar operações e acessar arquivos de acordo com estas permissões. Se o usuário em questão estiver utilizando a conta de administrador, então o programa poderá executar qualquer tipo de operação e acessar todo tipo de arquivo. A conta de administrador, portanto, deve ser usada apenas em situações nas quais uma conta padrão não tenha privilégios suficientes para realizar uma operação. E, sobretudo, pelo menor tempo possível. Muitas pessoas, entretanto, por questões de comodidade ou falta de conhecimento, utilizam esta conta para realizar todo tipo de atividade. Utilizar nas atividades cotidianas uma conta com privilégios de administrador é um hábito que deve ser evitado, pois você pode, por exemplo, apagar acidentalmente arquivos essenciais para o funcionamento do sistema operacional ou instalar inadvertidamente um código malicioso, que terá acesso irrestrito ao seu equipamento.

Tenha cuidado com extensões ocultas. Alguns sistemas possuem como configuração padrão ocultar a extensão de tipos de arquivos conhecidos. Exemplo: se um atacante renomear o arquivo "exemplo.scr" para "exemplo.txt.scr", ao ser visualizado o nome do arquivo será mostrado como "exemplo.txt", já que a extensão ".scr" não será mostrada.



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.

Créditos

- **Cartilha de Segurança para Internet**
  Fascículo Códigos Maliciosos
  Fascículo *Backup*
  cartilha.cert.br/fasciculos

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

cert.br nic.br cgi.br