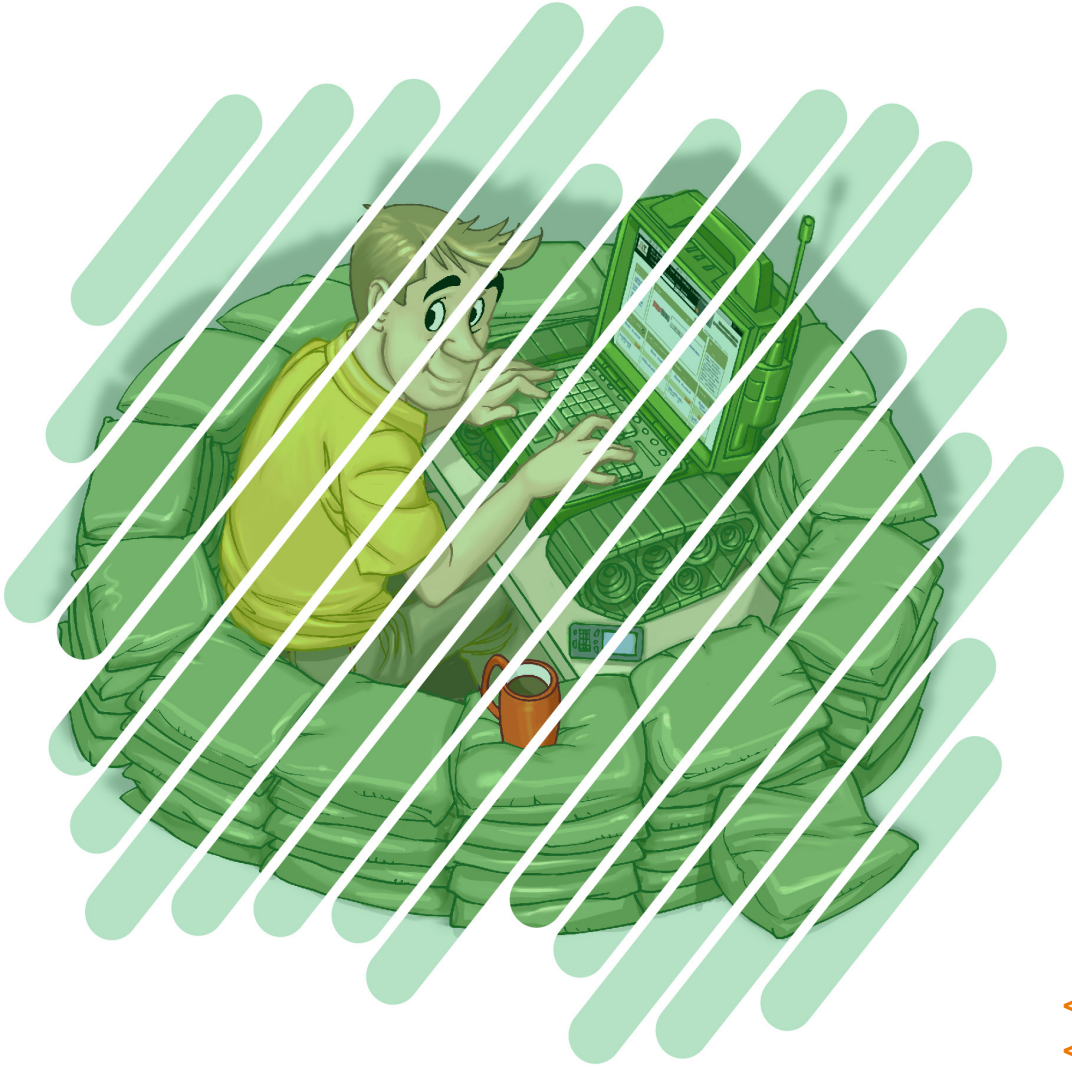


PROTEJA OS SEUS DADOS E OS DA SUA EMPRESA

<Nome do Palestrante>
<Instituição>
<e-mail>

fonte: cartilha.cert.br

Agenda

- A importância dos seus dados
- Como seus dados podem ser abusados
- Como se prevenir
- Reduza a quantidade de dados sobre você
- Informe-se sobre seus direitos
- Saiba mais
- Créditos

A importância dos seus dados (1/3)

- **Dados de cadastros, biográficos, profissionais, financeiros e de navegação são apenas alguns exemplos de dados referentes a você que, diariamente:**
  - **circulam por diversas redes**
  - **são armazenados em diferentes sistemas, dispositivos e mídias**
- **Infelizmente, há situações em que seus dados podem ser:**
  - **perdidos**
  - **indevidamente acessados**
  - **coletados e vendidos sem que você tenha ciência disso**

A importância dos seus dados (2/3)

- **Exemplos dessas situações incluem:**
  - **você perde o celular, computador ou mídia removível**
  - **seus dados são interceptados ao trafegarem na rede**
  - **há um vazamento envolvendo seus dados**
  - **suas contas de usuário e sistemas onde seus dados estão armazenados são invadidos**
  - **seus dados de navegação são coletados de forma não transparente e compartilhados sem seu consentimento**

A importância dos seus dados (3/3)

- **Para proteger seus dados e assegurar que eles sejam tratados de forma adequada há um conjunto de mecanismos de segurança que podem ser usados**
  - exemplo: o uso de senhas fortes impede o acesso indevido às contas, a criptografia dificulta que seus dados sejam acessados e alterados indevidamente
- **Há situações em que os mecanismos de segurança sozinhos não protegem seus dados**
  - exemplo: quando eles são passados deliberadamente a outros sem sua autorização ou coletados sem necessidade
- **Adotar uma postura preventiva, tentando reduzir a quantidade de dados fornecida por você, é essencial**
- **Para coibir abusos, garantir seus direitos e agir adequadamente é importante conhecer a legislação vigente**

Como seus dados podem ser abusados

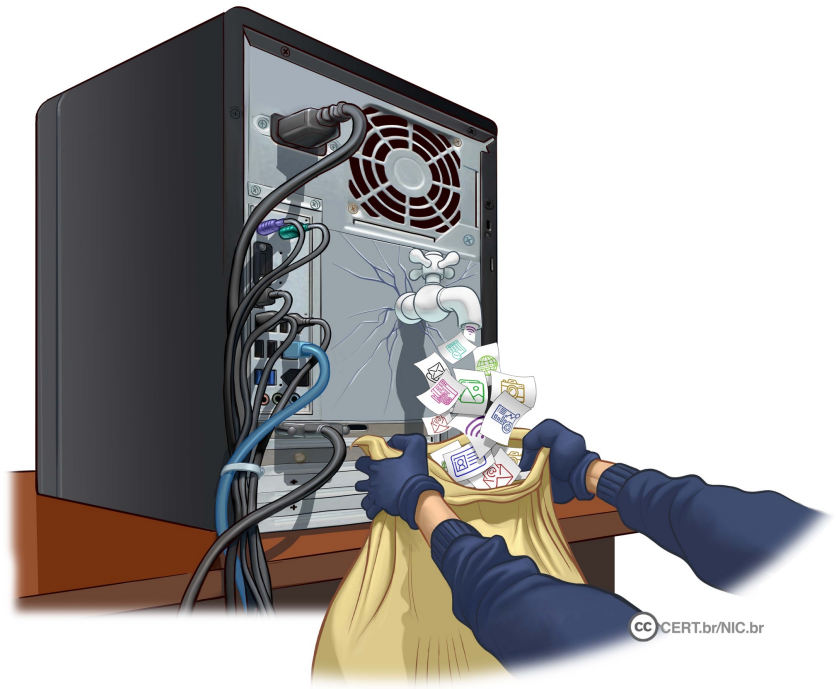
Como seus dados podem ser abusados

- **Pode ocorrer de diversas formas:**
  - **acesso indevido**
  - **perda de dados**
  - **invasão de contas e golpes**
  - **coleta excessiva**

- **O abuso de seus dados pode acarretar:**
  - **prejuízos financeiros**
  - **restrição a direitos ou benefícios**
  - **invasão de privacidade**

Acesso indevido

- **Seus dados podem ser indevidamente acessados:**
  - **por aplicativos e *sites***
    - que processem seus dados além das finalidades informadas
  - **por atacantes ou códigos maliciosos**
    - que consigam acesso às suas contas, equipamentos ou mídias
  - **em casos de vazamentos de dados**



Perda de dados

- **Seus dados podem ser perdidos:**
  - **pela ação de códigos maliciosos, como *ransomware***
  - **pela ação de atacantes que consigam invadir seus equipamentos e mídias e venham a apagá-los**

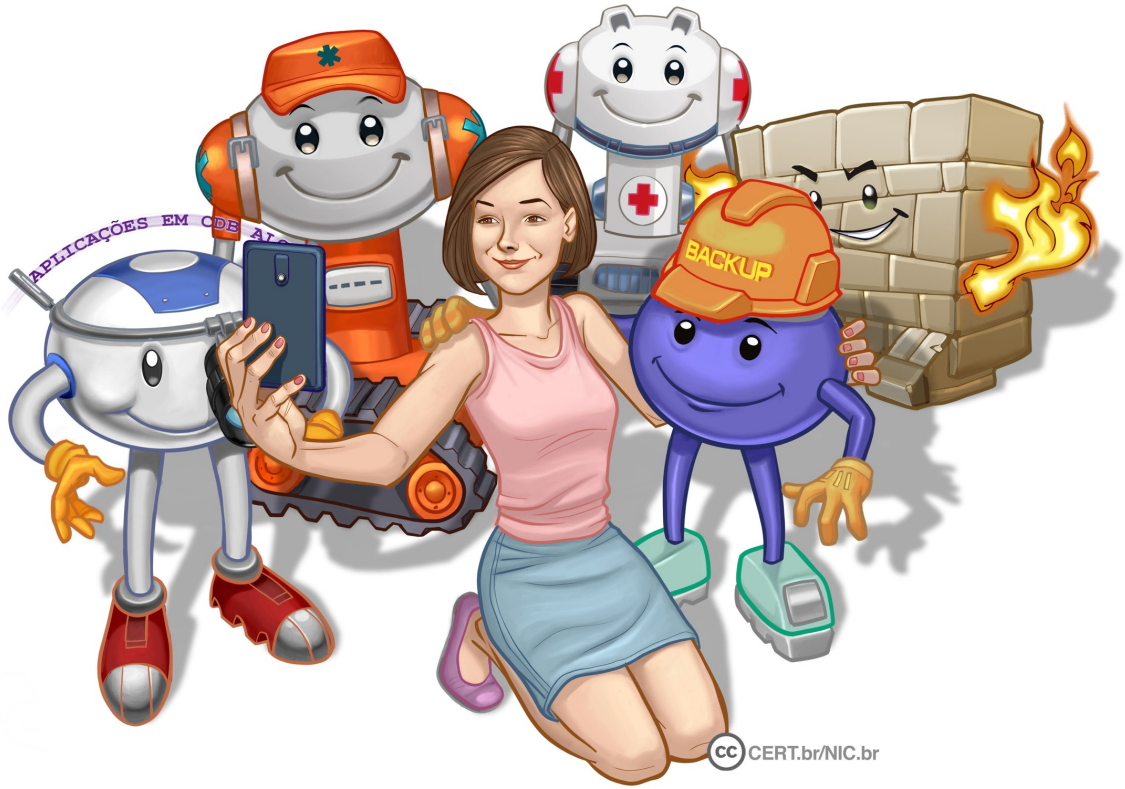
Invasão de contas e golpes

- **Seus dados podem ser usados:**
  - **para adivinhar suas senhas e responder perguntas de segurança**
  - **em tentativas de golpes, como:**
    - *phishing* direcionado e personalizado (*spear phishing*)
    - furto de identidade
    - extorsão

Coleta excessiva

- **Muitos aplicativos e *sites* coletam dados extras sem o seu conhecimento e os utilizam para a elaboração de perfis de comportamento (*profiling*)**
- **Seu perfil pode, então, ser usado sem o seu consentimento:**
  - **de forma discriminatória**
  - **para fins como propagandas**

Como se prevenir



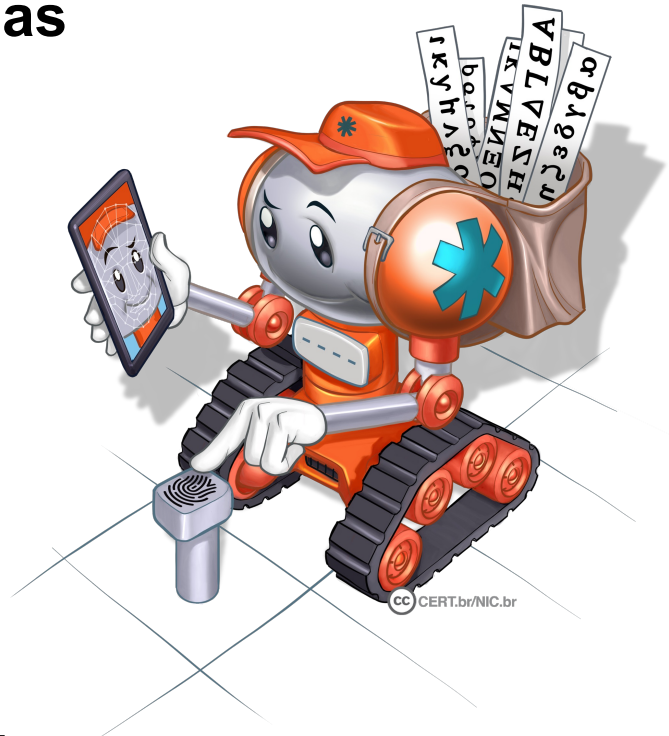
Como se prevenir

Nos próximos *slides* veremos dicas sobre vários aspectos que podem prevenir a perda e o vazamento de dados.

- **Autenticação forte**
  - **Contas e senhas**
  - **Verificação em duas etapas**
    - Código de verificação
    - *Token* gerador de senhas
    - Cartão de segurança
    - Dispositivo confiável
    - Lista de códigos reserva/*backup*
    - Chave de recuperação
- **Cuidados no uso da tecnologia**
  - ***E-mails* e mensagens eletrônicas**
  - **Aplicativos**
  - **Equipamentos e mídias**
  - ***Backups***
  - **Criptografia**

Contas e senhas

- **Crie senhas fortes e não repita senhas**
- **Habilite:**
  - **verificação em duas etapas**
    - especialmente em sistemas de armazenamento em nuvem
  - **notificações de *login***
    - para ser mais fácil perceber acessos indevidos
  - **configurações de privacidade e segurança**
- **Ao usar equipamentos compartilhados:**
  - **lembre-se de sair de suas contas (*logout*)**



Contas e senhas

Use:

- **números aleatórios**
  - quanto mais ao acaso forem os números melhor
- **grande quantidade de caracteres e palavras**
  - quanto mais longa for a sua senha melhor
- **diferentes tipos de caracteres**
  - quanto mais “bagunçada” for a sua senha melhor

Evite usar:

- **dados pessoais**
  - nome, sobrenome
  - contas de usuário, datas
  - números de documentos, de telefones ou de placas de carros
- **dados disponíveis em redes sociais e páginas *web***
- **sequências de teclado**
  - “1qaz2wsx”, “QwerTAsdfG”
- **palavras presentes em listas publicamente conhecidas**
  - músicas, times de futebol
  - personagens de filmes
  - dicionários de diferentes idiomas

Dicas práticas para elaborar boas senhas

- **Escolha uma frase e selecione a primeira, a segunda ou a última letra de cada palavra**

  Frase: “O Cravo brigou com a Rosa debaixo de uma sacada”

  Senha: “?OCbcaRddus”

- **Escolha uma frase longa, fácil de ser memorizada e com diferentes tipos de caracteres**

  Senha: “1 dia ainda verei os aneis de Saturno!!!”

- **Invente um padrão de substituição próprio**

  Padrão: substituir “o” por “0” e duplicar as letras “s” e “r”

  Frase: “Sol, astro-rei do Sistema Solar”

  Senha: “SS0l, asstrr0-rrei d0 SSisstema SS0larr”

Contas e senhas

- **Não exponha suas senhas**
  - **certifique-se de não estar sendo observado ao digitá-las**
  - **não as deixe anotadas em locais onde outros possam ver**
    - um papel sobre sua mesa ou colado em seu monitor
  - **evite digitá-las em computadores e dispositivos móveis de terceiros**
- **Não forneça suas senhas para outras pessoas**
  - **cuidado com *e-mails*/telefonemas pedindo dados pessoais**
- **Use conexões seguras quando o acesso envolver senhas**

Contas e senhas

- **Evite:**
  - **salvar as suas senhas no navegador *web***
  - **usar opções, como:**
    - "Lembre-se de mim"
    - "Continuar conectado"
  - **usar a mesma senha para todos os serviços que acessa**
    - basta ao atacante conseguir uma senha para ser capaz de acessar as demais contas onde ela seja usada
- **Não use senhas de acesso profissional para acessar assuntos pessoais (e vice-versa)**
  - **respeite os contextos**

Contas e senhas

- **Crie grupos de senhas, de acordo com o risco envolvido**
  - **crie senhas:**
    - únicas, fortes, e use-as onde haja recursos valiosos envolvidos
    - únicas, um pouco mais simples, e use-as onde o valor dos recursos protegidos é inferior
    - simples e reutilize-as para acessos sem risco
- **Armazene suas senhas de forma segura:**
  - **use programas gerenciadores de contas/senhas**
  - **anote-as em um papel e guarde-o em local seguro**
  - **grave-as em um arquivo criptografado**

Contas e senhas

- **Altere suas senhas:**
  - **imediatamente: se desconfiar que tenham sido descobertas ou usadas em computadores invadidos ou infectados**
  - **rapidamente:**
    - se perder um computador onde elas estejam gravadas
    - se usar:
      - um padrão de formação e desconfiar que alguma tenha sido descoberta
      - uma mesma senha em mais de um lugar e desconfiar que ela tenha sido descoberta em algum deles
    - ao adquirir equipamentos acessíveis via rede
      - eles podem estar configurados com senha padrão

Contas e senhas

- **Configure opções de recuperação de senhas:**
  - **endereço de *e-mail* alternativo, pergunta de segurança, dica de segurança, número de telefone celular**
- **Ao usar perguntas de segurança:**
  - **evite escolher questões cujas respostas sejam facilmente adivinhadas**
  - **procure criar suas próprias questões**
- **Ao usar dicas de segurança, escolha aquelas que sejam:**
  - **vagas o suficiente para que ninguém consiga descobri-las, e**
  - **claras o bastante para que você consiga entendê-las**
- **Ao solicitar o envio de suas senhas por *e-mail*:**
  - **procure alterá-las o mais rápido possível**
  - **cadastre um *e-mail* que você acesse regularmente**
    - para não esquecer a senha desta conta também

Verificação em duas etapas

- Também chamada de:
  - *two-factor authentication*
  - verificação ou autenticação em dois fatores
  - aprovação de *login*
  - verificação ou autenticação em dois passos
- Recurso opcional oferecido por diversos serviços:
  - *webmail,* redes sociais, *Internet Banking,* serviços em nuvem
  - ao ser habilitada aumenta a segurança de sua conta
  - pode ser desabilitada

Verificação em duas etapas

- **Dificulta o acesso indevido de contas de usuário**
- **Para que o acesso ocorra é necessário que o atacante realize com sucesso duas etapas**
  - **primeira etapa: geralmente a senha do usuário**
  - **segunda etapa: informações adicionais**
- **Segunda etapa pode envolver:**
  - **algo que apenas você sabe**
    - outra senha, perguntas de segurança, número PIN, alguma informação pessoal
  - **algo que apenas você possui**
    - código de verificação, cartão de senhas bancárias, *token* gerador de senhas, acesso a determinado computador ou dispositivo móvel
  - **algo que você é**
    - informações biométricas: impressão digital, palma da mão, rosto

Verificação em duas etapas: Código de verificação

- **Código individual**
  - **criado pelo serviço e enviado de forma que apenas você possa recebê-lo**
    - por *e-mail,* chamada de voz, mensagem SMS
    - pode ser gerado por um aplicativo autenticador instalado em seu dispositivo móvel

Cuidados a serem tomados:

- **mantenha atualizados seus dados para recebimento**
  - números de telefones celulares alternativos podem ser cadastrados, caso o seu principal não esteja disponível
- **certifique-se de estar com seu telefone celular, caso tenha configurado:**
  - o envio via SMS ou o uso do aplicativo autenticador
  - aplicativo autenticador deve ser usado em casos onde não é possível receber mensagens SMS

Verificação em duas etapas: *Token* gerador de senhas

- **Chave eletrônica**
  - **tipo de dispositivo eletrônico que gera códigos usados na verificação da sua identidade**
- **Cada código é válido por um determinado período**
  - **geralmente alguns segundos, após esse tempo um novo código é gerado**
  - **código pode ser gerado automaticamente ou necessitar que você clique em um botão para ativá-lo**

Cuidados a serem tomados:

- **guarde seu *token* em um local seguro**
- **não informe o código mostrado no *token* por *e-mail* ou telefone**
- **caso perca seu *token* ou ele seja furtado:**
  - avise imediatamente o responsável pelo serviço no qual ele é usado

Verificação em duas etapas: Cartão de segurança

- **Cartão com diversos códigos numerados e que são solicitados quando você acessa a sua conta**

Cuidados a serem tomados:

- **guarde seu cartão em um local seguro**
- **nunca forneça os códigos do cartão por *e-mail* ou telefone**
- **forneça apenas uma posição do seu cartão a cada acesso**
- **verifique se o número de identificação do cartão apresentado pelo serviço corresponde ao que está no seu cartão**
  - caso sejam diferentes entre em contato com o serviço
- **desconfie caso, em um mesmo acesso, seja solicitada mais de uma posição do cartão**

Verificação em duas etapas: Dispositivo confiável

- Computador ou dispositivo móvel usado para acessar suas contas
- No primeiro acesso:
  - pode ser necessário inserir um código de segurança
  - ele não será necessário nos demais acessos, pois seu dispositivo será "lembrado", caso você assim o configure

Cuidados a serem tomados:

- não esqueça de excluir seus dispositivos confiáveis caso eles sejam trocados ou você perca o acesso a eles
- pode ser necessário habilitar a opção de *cookies* em seu navegador *web* para que seu dispositivo seja memorizado

Verificação em duas etapas: Lista de códigos reserva/*backup*

- **Lista de códigos que devem ser usados de forma sequencial e uma única vez**

Cuidados a serem tomados:

- **anote ou imprima a lista e a mantenha em um local seguro**
- **não a armazene em seu dispositivo confiável pois ela poderá vir a ser acessada por atacantes**
  - caso não esteja criptografada
- **caso perca a lista ou desconfie que alguém a acessou você deve gerá-la novamente ou revogá-la**
  - anulando assim a anterior

Verificação em duas etapas: Chave de recuperação

- **Número gerado pelo serviço quando você ativa a verificação em duas etapas**
- **Permite que você acesse o serviço mesmo que perca sua senha ou seus dispositivos confiáveis**

Cuidados a serem tomados:

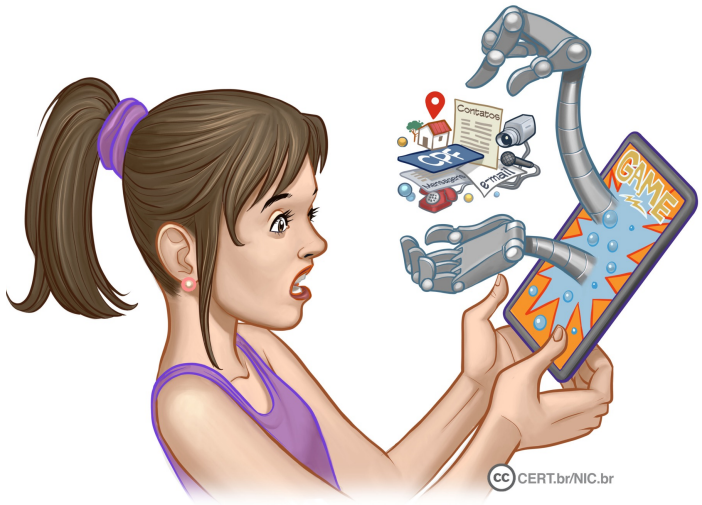
- **anote ou imprima a chave e a mantenha em um local seguro**
- **não a deixe anotada em seu dispositivo confiável pois ela poderá vir a ser acessada por atacantes**
  - caso não esteja criptografada
- **caso perca ou desconfie que alguém acessou a sua chave você deve gerá-la novamente**
  - substituindo assim a anterior

E-mails e mensagens eletrônicas

- **Desconfie de *links* ou pedidos de pagamentos recebidos via mensagens eletrônicas**
  - **mesmo que vindos de pessoas conhecidas**
  - **podem ter sido enviadas de perfis falsos ou invadidos**
- **Evite:**
  - **clicar/seguir *links* recebidos via mensagens eletrônicas**
    - procure digitar a URL diretamente no navegador
  - **usar *sites* de busca para acessar serviços que requeiram senhas, como seu *webmail* e sua rede social**
- **Seja cuidadoso ao acessar *links* reduzidos:**
  - **use complementos que permitam expandir o *link* antes de clicar sobre ele**

Aplicativos

- **Instale aplicativos somente de fontes e lojas oficiais**
  - **antes de instalar, verifique as telas e o nome do aplicativo**
  - **muitos falsos aplicativos se assemelham aos oficiais**



- **Observe:**
  - **se o desenvolvedor é confiável**
  - **quantas pessoas instalaram o aplicativo**
  - **qual a opinião delas sobre o aplicativo**
- **Fique atento às permissões:**
  - **forneça apenas as que considerar necessárias**
  - **limite quais aplicativos podem acessar o microfone, a câmera, seus contatos e sua localização**
- **Apague os aplicativos que não usa mais**

Equipamentos e mídias

- **Atualize o sistema e os aplicativos**
- **Utilize mecanismos de segurança**
- **Cuidado para não perder *pen drives* e discos externos**
- **Antes de se desfazer de seus equipamentos e mídias apague os dados armazenados**
- **Ao enviar equipamentos para manutenção escolha empresas com boa reputação**
- **Seja cuidadoso ao usar equipamentos de terceiros ou potencialmente infectados**

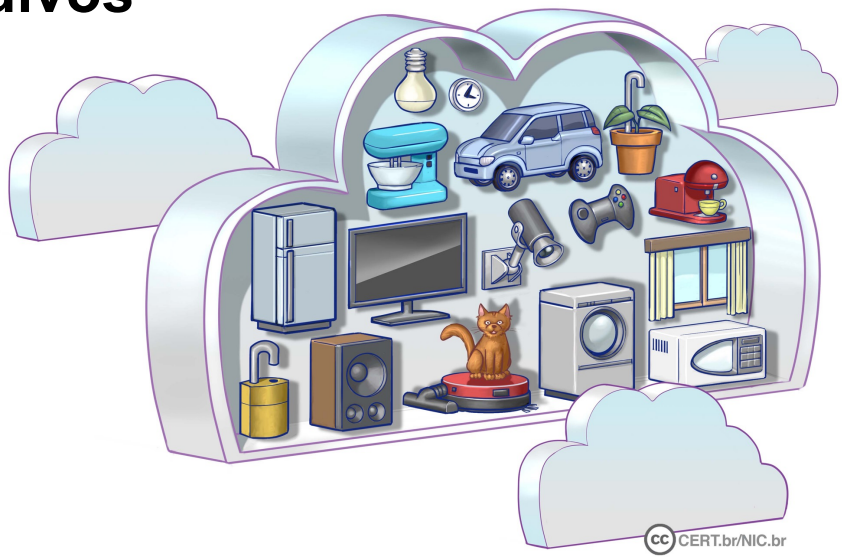
Backups

Backups* protegem seus dados em caso de mau funcionamento de equipamentos, da perda de dispositivos e da ação de códigos maliciosos, especialmente *ransomware

- **Faça regularmente *backup* dos seus dados**
- **Programe seus *backups* para serem feitos automaticamente**
- **Teste periodicamente seus *backups***
  - **para ter certeza de que estão sendo feitos corretamente**
- **Mantenha pelo menos um *backup off-line***

Arquivos

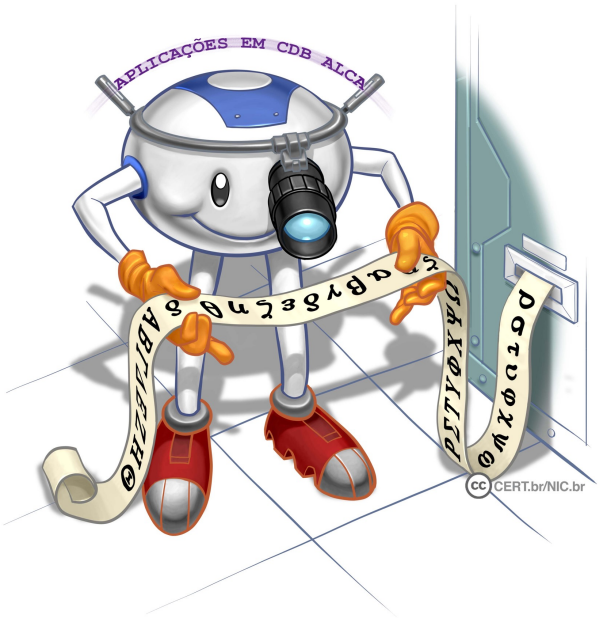
- Evite colocar na nuvem arquivos contendo dados confidenciais ou que considere privados
- Crie uma partição criptografada ou use outros recursos de criptografia para armazenar seus arquivos de forma segura
- Seja cuidadoso ao abrir arquivos enviados por terceiros



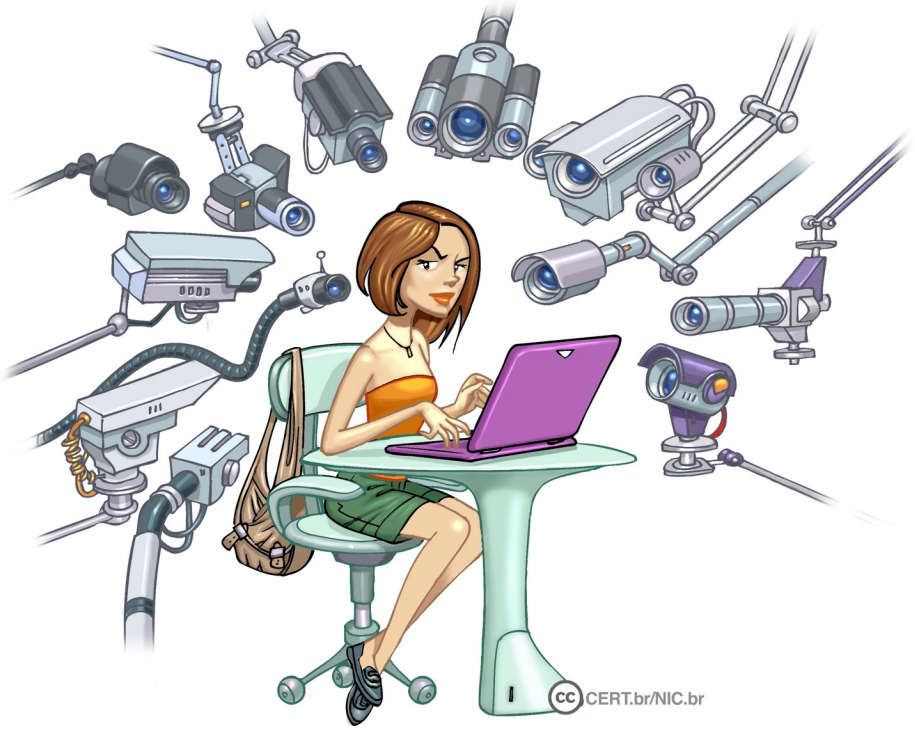
Criptografia

A criptografia ajuda a tornar as transmissões de dados mais seguras, detectar alterações em seus dados e impedir que sejam lidos indevidamente

- **Use criptografia para proteger os dados armazenados em seus equipamentos e mídias**
  - **em caso de perda ou furto será mais difícil deles serem acessados**
- **Ative as configurações de criptografia em seus discos e mídias**
  - **como *pen drive*s e discos externos**
- **Use conexões seguras**



Reduza a quantidade de dados sobre você



Rastros digitais

- **Você sabia que todas as vezes que acessa seus equipamentos e "entra na Internet" alguns de seus dados são de alguma forma fornecidos?**
- **Cada vez que acessa um *site*, assiste a um vídeo ou compra algo, deixa marcas de sua passagem**
  - **essas marcas são chamadas vestígios, rastros ou pegadas digitais**
  - **permitem criar sua reputação *online* e definir seu perfil comportamental**

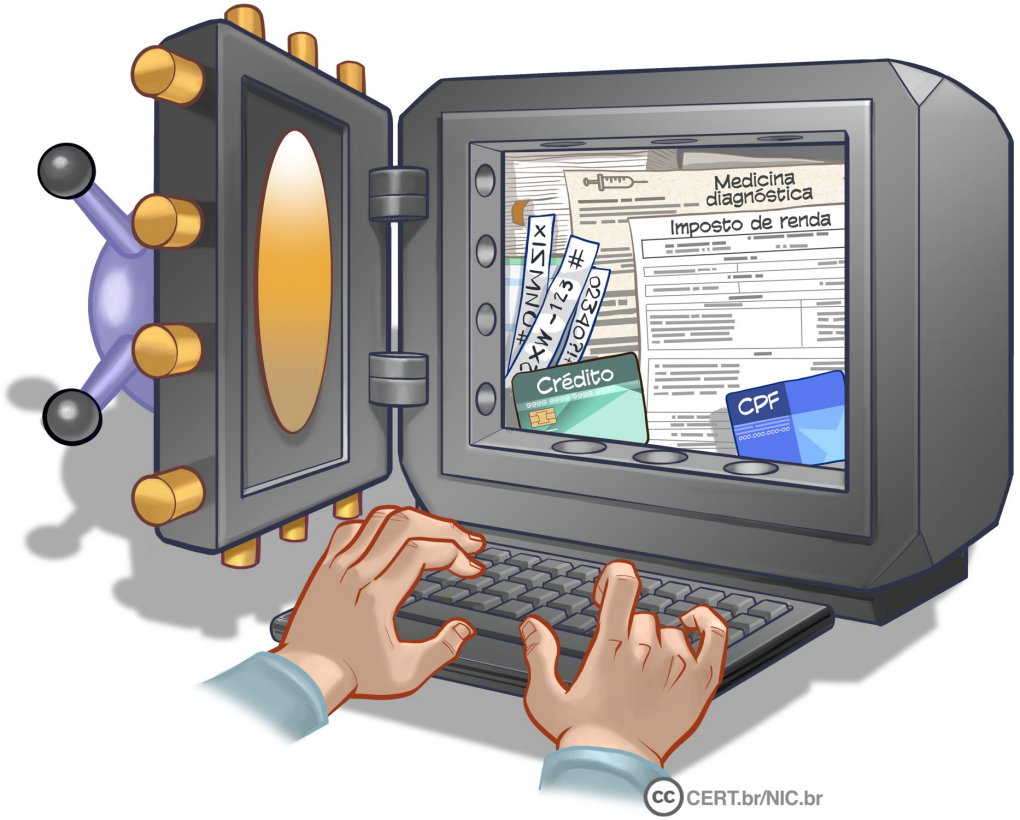
Dados que você divulga

- **Pense bem antes de divulgar algo**
  - **depois será difícil de excluir**
- **Seja seletivo ao aceitar seus contatos nas redes sociais**
- **Ao preencher cadastros questione-se sobre a necessidade:**
  - **de fornecer todos os dados solicitados**
  - **da instituição retê-los**

Dados coletados sobre você

- Use conexões seguras
- Seja seletivo ao baixar aplicativos
- Observe as configurações de privacidade de seus aplicativos e navegadores
- Ao acessar *sites*, procure limitar a coleta de dados por *cookies*
  - preferencialmente, autorize somente aqueles essenciais ao funcionamento da sessão
- Limpe frequentemente o histórico de navegação

Informe-se sobre os seus direitos



Lei Geral de Proteção de Dados (LGPD)

- **Criada para que:**
  - **o indivíduo tenha controle sobre seus dados pessoais**
  - **saiba como esses dados são tratados por organizações públicas, privadas e terceiros**
- **Dados pessoais, segundo a LGPD:**
  - **informações relacionadas a pessoa natural identificada ou identificável**
- **Como titular de dados pessoais você tem diversos direitos garantidos pela LGPD, como os definidos no art. 18**
- **Informe-se sobre a LGPD, conheça seus direitos e saiba como agir de forma adequada:**
  - **https://www.gov.br/anpd/pt-br/legislacao**

Benefícios e direitos trazidos pela LGPD (1/2)

- **A LGPD:**
  - **dá a você o direito de saber:**
    - como seus dados são exatamente tratados
    - quais dados são coletados
    - o porquê e com quem seus dados são compartilhados
  - **traz maior segurança jurídica**
    - ao fornecer mecanismos para que você tenha controle sobre quais dados seus são coletados e como são usados
- **Organizações públicas e privadas devem disponibilizar informações claras que o ajudem a compreender:**
  - **os termos de consentimento**
  - **as bases legais que apoiam o tratamento dos seus dados**

Benefícios e direitos trazidos pela LGPD (2/2)

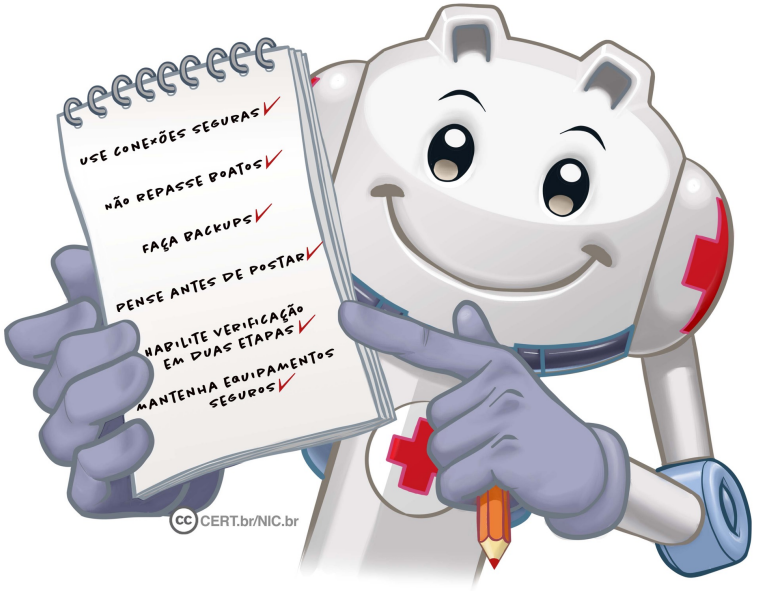
- **Caso a instituição responsável pelo tratamento de seus dados pessoais não atenda a um de seus direitos de titular sem uma justificativa legal:**
  - **você tem o direito de peticionar uma reclamação para a Autoridade Nacional de Proteção de Dados – ANPD**
  - **https://www.gov.br/anpd/pt-br/canais_atendimento**

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 Proteção de Dados
  - Fascículo Senhas
  - Fascículo Verificação em Duas Etapas

  cartilha.cert.br/guardiao

- **Livro Segurança na Internet**

  cartilha.cert.br/livro

Apoio de Divulgação:

GUARDIÃO CIBERNÉTICO

Produção:

cert.br nic.br cgi.br