Cartilha de Segurança para Internet

FASCÍCULO

COMÉRCIO ELETRÔNICO

Apoio de Divulgação:

UFPE

STI SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

Produção:

cert.br nic.br cgi.br

ATUALMENTE, GRAÇAS À INTERNET, É POSSÍVEL COMPRAR PRODUTOS SEM SAIR DE CASA OU DO TRABALHO, SEM SE PREOCUPAR COM HORÁRIOS E SEM ENFRENTAR FILAS

E ainda receber tudo em casa ou pedir para entregar diretamente onde desejar.

Infelizmente há golpistas que se aproveitam das facilidades do comércio eletrônico para cometer fraudes. Assim como existem lojas, *sites* e vendedores confiáveis, também existem aqueles cujo objetivo é lesar os consumidores, causar prejuízos e obter vantagens financeiras.

Os golpes envolvendo comércio eletrônico são aqueles que procuram explorar a relação de confiança existente entre as partes envolvidas na transação comercial.

Alguns exemplos de golpes deste tipo são:

- **Golpe do site falso (*phishing*):** um golpista pode criar um *site* falso, similar ao *site* original, e induzir os clientes a fornecerem dados pessoais e financeiros, achando que estão no *site* verdadeiro
- **Golpe do *site* de comércio eletrônico fraudulento:** um golpista pode criar um *site* fraudulento, com o objetivo de enganar os clientes que, após efetuarem os pagamentos, não recebem as mercadorias. Também pode anunciar promoções em *sites* de compras coletivas e, assim, conseguir grande quantidade de vítimas em um curto intervalo de tempo
- **Golpe do *site* de leilão e venda de produtos:** um golpista pode usar um *site* deste tipo para vender produtos que nunca serão entregues. Também pode usar os dados pessoais e financeiros envolvidos na transação para outros fins.

COMÉRCIO ELETRÔNICO: COMPRE COM SEGURANÇA

RISCOS PRINCIPAIS

Para aproveitar todo o conforto e as facilidades do comércio eletrônico de forma segura é importante, além de conhecer os golpes que são aplicados, estar ciente dos riscos que eles podem representar.

Alguns dos riscos que você pode enfrentar ao comprar pela Internet são:

- Não receber o produto
- Receber o produto, porém:
  - com atraso
  - totalmente ou parcialmente danificado
  - com características ou especificações diferentes do esperado
  - de origem ilícita ou criminosa, como contrabando ou roubo de carga
- Enfrentar dificuldades de contato com o *site*/loja, a fim de resolver problemas
- Ficar insatisfeito com a compra ("não era bem isso que eu imaginava")
- Ter os dados pessoais e financeiros indevidamente obtidos, por meio:
  - do uso de computadores invadidos ou infectados
  - do acesso a *sites* fraudulentos e falsos
  - da interceptação de tráfego, caso o *site*/loja não use conexão segura
- Ter a privacidade invadida, via o compartilhamento indevido de dados pessoais
- Ter os dados financeiros repassados para outras empresas e indevidamente usados para outros fins
- Recebimento de *spam*

CUIDADOS A SEREM TOMADOS

ANTES DE COMPRAR

» Utilize sempre um computador seguro
- com a versão mais recente de todos os programas instalados
- com todas as atualizações aplicadas
- com mecanismos de segurança instalados e atualizados, como *antimalware*, *antispam*, e *firewall* pessoal

» Evite usar computadores de terceiros

» Acesse o *site*/loja digitando o endereço diretamente no navegador *web*
- evite seguir ou clicar em *links* recebidos em mensagens
- não utilize *sites* de busca para localizar o *site*/loja de comércio eletrônico

» Seja cuidadoso ao elaborar suas senhas
- utilize
  - números aleatórios
  - grande quantidade de caracteres
  - diferentes tipos de caracteres
- não utilize
  - sequências de teclado
  - qualquer tipo de dado pessoal
  - a sua própria conta de usuário
  - palavras que façam parte de listas

» Verifique se o *site*/loja é confiável
- pesquise na Internet para ver a opinião de outros clientes
  - principalmente em redes sociais e *sites* de reclamações
- escolha *sites*/lojas que você conheça pessoalmente e/ou que tenha boas referências
- observe:
  - se há reclamações referentes à empresa e se elas foram tratadas adequadamente
  - se são disponibilizados canais de atendimento, como *e-mail*, *chat* e telefone

- se a empresa disponibiliza informações, como endereço, telefone e CNPJ
- as políticas de privacidade, garantia, troca, cancelamento, arrependimento e devolução

- procure validar os dados de cadastro da empresa no *site* da Receita Federal

» Verifique as condições de compra

- faça uma pesquisa de mercado e desconfie se o produto estiver muito barato
- observe:
  - as condições do produto (novo, usado, defeituoso)
  - a descrição detalhada ou especificação técnica
  - o prazo de entrega

» Verifique, quando disponível, a reputação/qualificação do vendedor

» Fique atento ao comprar em *sites* de compras coletivas

- procure não comprar por impulso
- seja cauteloso e faça pesquisas prévias
- verifique atentamente as condições da compra

» Não compre caso desconfie de algo

AO REALIZAR A COMPRA

» Verifique as opções de pagamento oferecidas e escolha aquela que considerar mais segura

» Ao fornecer dados sensíveis via *e-mail* certifique-se de criptografar a mensagem

» Guarde as informações da compra, como comprovantes e número de pedido

- documente também outros contatos que você venha a ter
- essas informações podem ser muito importantes caso haja problemas futuros

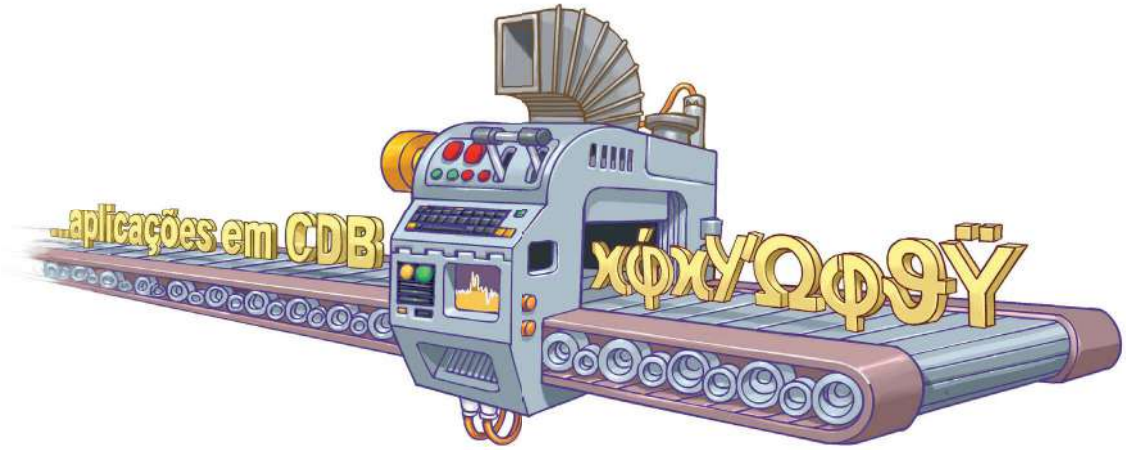
» Utilize sistemas de gerenciamento de pagamentos

- além de dificultarem a aplicação dos golpes, também podem impedir que seus dados pessoais e financeiros sejam enviados aos golpistas

» Certifique-se de usar conexões seguras. Alguns indícios são:

- o endereço do *site* 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/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 ele, são exibidos detalhes sobre a conexão/certificado digital em uso
- a barra de endereço e/ou o recorte são apresentados na cor verde e no recorte é colocado o nome da instituição dona do *site*

» Se tiver dúvidas entre em contato com a central de relacionamento da empresa



AO RECEBER O PRODUTO

» Marque encontros em locais públicos caso a entrega seja feita pessoalmente

» Mesmo que o vendedor lhe envie o código de rastreamento fornecido pelos Correios, não use esta informação para comprovar o envio e liberar o pagamento

- até ter o produto em mãos não há nenhuma garantia de que ele foi realmente enviado

» Antes de abrir a embalagem verifique se ela não está danificada

» Certifique-se de que o produto está de acordo com o que foi comprado

» Comente sobre a compra no *site*

EM CASO DE PROBLEMAS

» Entre em contato com a empresa e verifique o ocorrido

» Se houver problemas de contato com o *site*/loja utilize *sites* de reclamações

» Utilize o Código de Defesa do Consumidor

- denuncie o ocorrido ao PROCON da sua cidade, que poderá orientá-lo sobre a forma correta de agir

PROTEJA SEUS DADOS

» Cuidado com telefonemas solicitando informações pessoais

» Não responda mensagens de instituições com as quais você não se relacione

» Procure reduzir a quantidade de informações que possam ser obtidas sobre você

- isso pode impedir, por exemplo, a criação de contas fantasma em seu nome

» Verifique periodicamente seu extrato bancário e do seu cartão de crédito

- entre em contato imediatamente com o seu banco ou com a operadora do seu cartão de crédito caso detecte algum lançamento suspeito

SAIBA MAIS

» Para mais detalhes sobre este e outros assuntos relacionados com cuidados na Internet, consulte os demais Fascículos da Cartilha de Segurança e o Livro Segurança na Internet, disponíveis em: **cartilha.cert.br**

» Procurando material para conversar sobre segurança com diferentes públicos? O Portal Internet Segura apresenta uma série de materiais focados em crianças, adolescentes, pais, responsáveis e educadores, confira em: **internetsegura.br**

cert.br

O CERT.br é o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Desde 1997, o grupo é responsável por tratar incidentes de segurança envolvendo redes conectadas à Internet no Brasil. O Centro também desenvolve atividades de análise de tendências, treinamento e conscientização, com o objetivo de aumentar os níveis de segurança e de capacidade de tratamento de incidentes no Brasil. Mais informações em **www.cert.br.**

nic.br

O Núcleo de Informação e Coordenação do Ponto BR — NIC.br (**www.nic.br**) é uma entidade civil, de direito privado e sem fins de lucro, que além de implementar as decisões e projetos do Comitê Gestor da Internet no Brasil, tem entre suas atribuições: coordenar o registro de nomes de domínio — Registro.br (**www.registro.br**), estudar, responder e tratar incidentes de segurança no Brasil — CERT.br (**www.cert.br**), estudar e pesquisar tecnologias de redes e operações — Ceptro.br (**www.ceptro.br**), produzir indicadores sobre as tecnologias da informação e da comunicação — Cetic.br (**www.cetic.br**), implementar e operar os Pontos de Troca de Tráfego — IX.br (**www.ix.br**), viabilizar a participação da comunidade brasileira no desenvolvimento global da Web e subsidiar a formulação de políticas públicas — Ceweb.br (**www.ceweb.br**), e abrigar o escritório do W3C no Brasil (**www.w3c.br**).

cgi.br

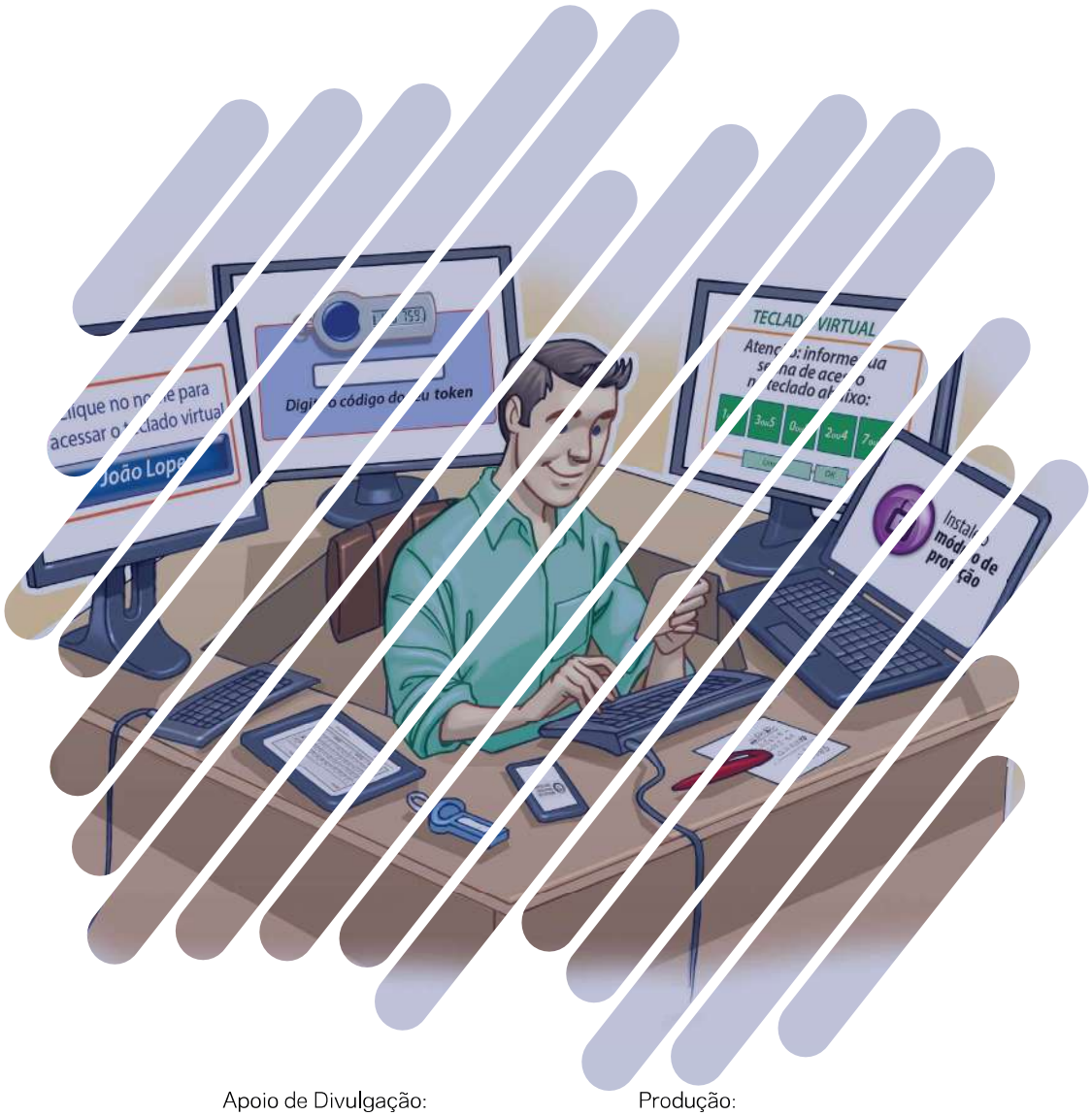
O Comitê Gestor da Internet no Brasil, responsável por estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil, coordena e integra todas as iniciativas de serviços Internet no País, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados. Com base nos princípios do multissetorialismo e transparência, o CGI.br representa um modelo de governança da Internet democrático, elogiado internacionalmente, em que todos os setores da sociedade são partícipes de forma equânime de suas decisões. Uma de suas formulações são os 10 Princípios para a Governança e Uso da Internet (**www.cgi.br/principios**). Mais informações em **www.cgi.br**.

outubro / 2020

Cartilha de Segurança para Internet

FASCÍCULO

INTERNET BANKING



Apoio de Divulgação:

UFPE

STI SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

Produção:

cert.br nic.br cgi.br

VIA *INTERNET BANKING* VOCÊ REALIZA AS MESMAS AÇÕES DISPONÍVEIS NAS AGÊNCIAS BANCÁRIAS, SEM FILAS OU RESTRIÇÃO DE HORÁRIOS

Realizar transações bancárias via Internet pode apresentar riscos caso você não tome alguns cuidados.

Como não é uma tarefa simples fraudar dados em um servidor de uma instituição bancária ou comercial, os golpistas procuram enganar e persuadir as potenciais vítimas a fornecerem informações sensíveis ou a realizarem ações, como executar códigos maliciosos e acessar páginas falsas (*phishing*). Para isso costumam utilizar temas como:

- atualização de cadastro e de cartão de senhas
- sincronização de *tokens*
- lançamento e atualização de módulos de proteção
- comprovante de transferência e depósito
- novas campanhas, como lançamento de produtos e unificação de bancos e contas
- cadastro/recadastro de computadores
- suspensão de acesso.

Outras formas de golpes usadas são:

- disponibilizar aplicativos maliciosos que, se instalados, podem coletar seus dados
- efetuar ligações telefônicas tentando se passar, por exemplo, pelo gerente do seu banco e solicitar seus dados
- explorar possíveis vulnerabilidades em seu computador ou dispositivo móvel para instalar códigos maliciosos
- explorar possíveis vulnerabilidades em equipamentos de rede, como senhas fracas ou padrão
- coletar informações sensíveis que estiverem trafegando na rede sem criptografia.

INTERNET BANKING: PROTEJA SUAS TRANSAÇÕES BANCÁRIAS

RISCOS PRINCIPAIS

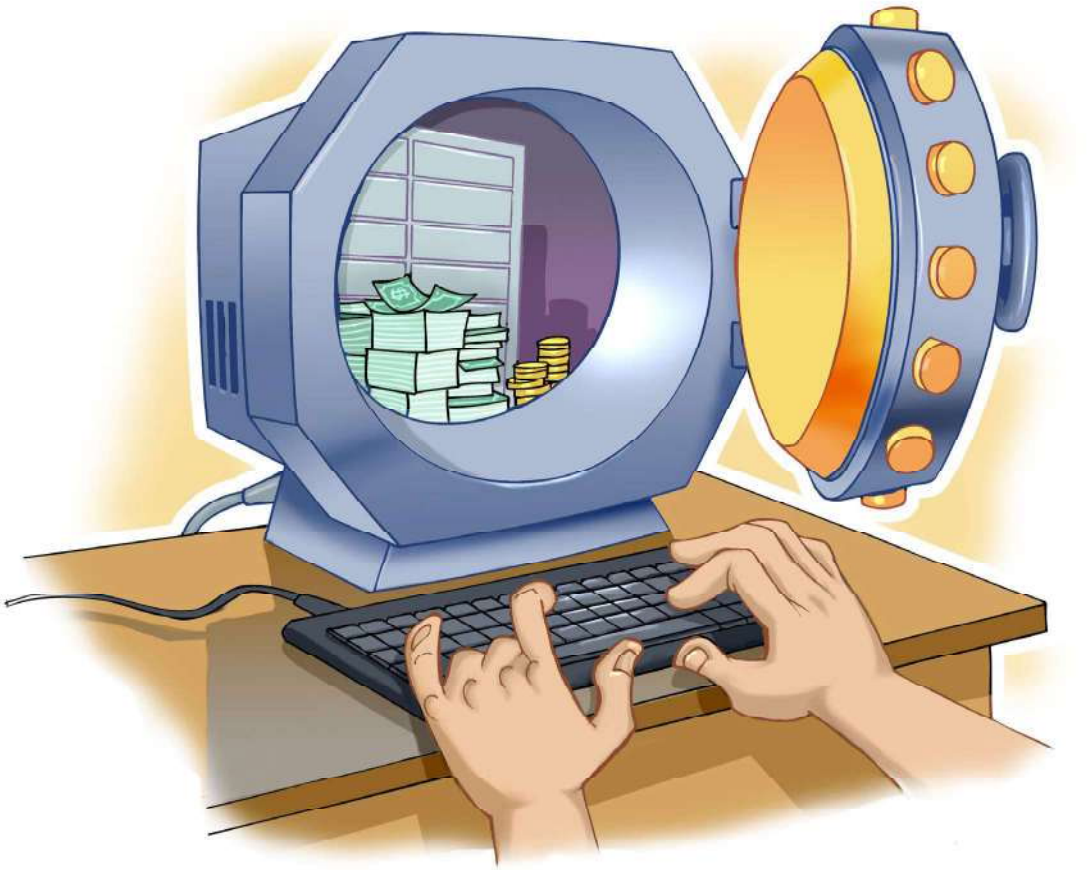
Caso não tome os devidos cuidados ao usar seu computador ou dispositivo móvel, os principais riscos aos quais você está exposto ao realizar transações bancárias via Internet são:

» Perdas financeiras
- sua conta bancária pode ser usada para ações maliciosas, como transferências indevidas de dinheiro e pagamentos de contas de outras pessoas

» Violação de sigilo bancário
- o sigilo bancário é um direito seu, que pode ser violado caso alguém acesse indevidamente sua conta

» Invasão de privacidade
- alguém que tenha acesso indevido a sua conta pode obter informações pessoais sobre suas transações bancárias e assim expor sua privacidade

» Participação em esquemas de fraude
- sua conta bancária pode ser usada como intermediária para aplicar golpes e cometer fraudes



CUIDADOS A SEREM TOMADOS

AO ACESSAR O *SITE* BANCÁRIO

» Certifique-se de usar computadores e dispositivos móveis seguros

» Digite o endereço do *site* bancário diretamente no navegador *web*

- evite seguir ou clicar em *links* recebidos via mensagens eletrônicas (*e-mails*, mensagens SMS, redes sociais, etc.)
- não utilize *sites* de busca para localizar o *site* bancário
  - geralmente o endereço é bastante conhecido

» Sempre acesse sua conta usando a página ou o aplicativo fornecido pelo próprio banco

» Antes de instalar um módulo de proteção, certifique-se de que o autor do módulo é realmente a instituição em questão

» Evite usar dispositivos móveis e computadores de terceiros (como *lan houses* e Internet cafés)

- não há garantias de que os equipamentos estejam seguros

» Evite usar redes Wi-Fi públicas

» Utilize um endereço terminado em "b.br", caso seu banco ofereça essa opção

- domínios terminados em "b.br", além de serem de uso exclusivo de instituições bancárias, também oferecem recursos adicionais de segurança

» Certifique-se de usar conexões seguras. Alguns indícios desse tipo de conexão são:

- o endereço do *site* 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/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 ele, são exibidos detalhes sobre conexão/certificado digital em uso
- a barra de endereço e/ou o recorte são apresentados na cor verde e no recorte é colocado o nome da instituição dona do *site*

» Existem casos em que a instituição bancária utiliza uma conexão mista, ou seja, parte da conexão é segura e parte não é. Nesse caso, verifique com seu banco se o tipo de conexão é realmente mista ou se poderia ser um *site* falso

OUTROS CUIDADOS

» Forneça apenas uma posição do seu cartão de segurança
  - desconfie caso, em um mesmo acesso, seja solicitada mais de uma posição

» Mantenha o número do seu celular atualizado, caso o tenha cadastrado
  - ele é utilizado para o envio de mensagens de confirmação e códigos de liberação de transações

» Use sempre a opção de "sair" quando deixar de utilizar seu *Internet Banking*

» Seja cuidadoso com mensagens sobre promoções

» Evite acessar a central de atendimento do seu banco por meio de celulares de terceiros
  - os dados digitados, como número da sua conta bancária e sua senha, podem ficar armazenados

» A maioria dos bancos não envia *e-mails* sem autorização prévia
  - desconsidere mensagens que receber, caso não tenha autorizado previamente o envio e principalmente de instituições com as quais você não tenha relação

» Verifique periodicamente o extrato da sua conta bancária e do seu cartão de crédito

EM CASO DE DÚVIDAS OU PROBLEMAS

» Entre imediatamente em contato com a central de relacionamento do seu banco, diretamente com o seu gerente ou com a operadora do seu cartão de crédito

PROTEJA SUAS SENHAS

» Seja cuidadoso ao elaborar as suas senhas
  - procure usar senhas com a maior quantidade de caracteres possível
  - procure usar diferentes tipos de caracteres para compor suas senhas
  - não utilize dados pessoais, como nome, sobrenome e datas
  - não utilize dados que possam ser facilmente obtidos sobre você

» Evite reutilizar suas senhas
  - não use a mesma senha de acesso ao seu *Internet Banking* para acessar outros *sites*

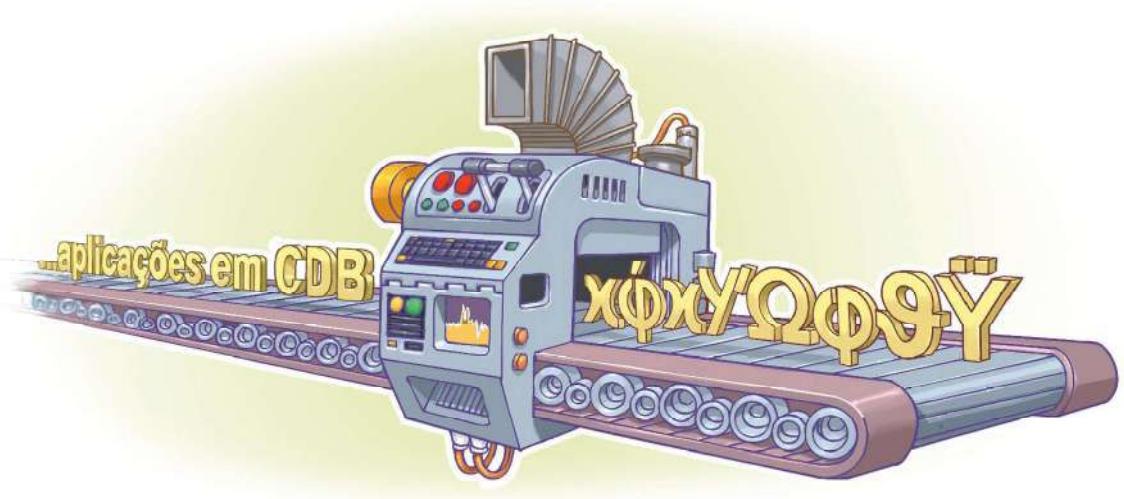
» Troque periodicamente suas senhas

» Não forneça informações bancárias, especialmente senhas, por meio de ligações telefônicas ou *e-mails*

PROTEJA SEU COMPUTADOR E SEUS DISPOSITIVOS MÓVEIS

» Mantenha seu computador e seus dispositivos móveis seguros
  - com as versões mais recentes de todos os programas instalados
  - com todas as atualizações aplicadas
  - com mecanismos de segurança instalados e atualizados, como *antimalware*, antivírus, *antispam* e *firewall* pessoal

» Ao instalar aplicativos desenvolvidos por terceiros
  - verifique se as permissões necessárias para a instalação e execução são coerentes
  - seja cuidadoso ao
    - permitir que os aplicativos acessem seus dados pessoais
    - selecionar os aplicativos, escolhendo aqueles bem avaliados e com grande quantidade de usuários



SAIBA MAIS

» Para mais detalhes sobre este e outros assuntos relacionados com cuidados na Internet, consulte os demais Fascículos da Cartilha de Segurança e o Livro Segurança na Internet, disponíveis em: **cartilha.cert.br**

» Procurando material para conversar sobre segurança com diferentes públicos? O Portal Internet Segura apresenta uma série de materiais focados em crianças, adolescentes, pais, responsáveis e educadores, confira em: **internetsegura.br**

cert.br

O CERT.br é o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Desde 1997, o grupo é responsável por tratar incidentes de segurança envolvendo redes conectadas à Internet no Brasil. O Centro também desenvolve atividades de análise de tendências, treinamento e conscientização, com o objetivo de aumentar os níveis de segurança e de capacidade de tratamento de incidentes no Brasil. Mais informações em **www.cert.br.**

nic.br

O Núcleo de Informação e Coordenação do Ponto BR — NIC.br (**www.nic.br**) é uma entidade civil, de direito privado e sem fins de lucro, que além de implementar as decisões e projetos do Comitê Gestor da Internet no Brasil, tem entre suas atribuições: coordenar o registro de nomes de domínio — Registro.br (**www.registro.br**), estudar, responder e tratar incidentes de segurança no Brasil — CERT.br (**www.cert.br**), estudar e pesquisar tecnologias de redes e operações — Ceptro.br (**www.ceptro.br**), produzir indicadores sobre as tecnologias da informação e da comunicação — Cetic.br (**www.cetic.br**), implementar e operar os Pontos de Troca de Tráfego — IX.br (**www.ix.br**), viabilizar a participação da comunidade brasileira no desenvolvimento global da Web e subsidiar a formulação de políticas públicas — Ceweb.br (**www.ceweb.br**), e abrigar o escritório do W3C no Brasil (**www.w3c.br**).

cgi.br

O Comitê Gestor da Internet no Brasil, responsável por estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil, coordena e integra todas as iniciativas de serviços Internet no País, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados. Com base nos princípios do multissetorialismo e transparência, o CGI.br representa um modelo de governança da Internet democrático, elogiado internacionalmente, em que todos os setores da sociedade são partícipes de forma equânime de suas decisões. Uma de suas formulações são os 10 Princípios para a Governança e Uso da Internet (**www.cgi.br/principios**). Mais informações em **www.cgi.br**.

outubro / 2020

Cartilha de Segurança para Internet

FASCÍCULO

REDES SOCIAIS

Apoio de Divulgação:

UFPE

STI SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

Produção:

cert.br nic.br cgi.br

O ACESSO ÀS REDES SOCIAIS JÁ ESTÁ INCORPORADO AO COTIDIANO DE GRANDE PARTE DOS USUÁRIOS DA INTERNET E, MUITO PROVAVELMENTE, DO SEU

As redes sociais possuem características que as diferenciam dos outros meios de comunicação, como:

- a facilidade de acesso
- a rápida velocidade com que as informações se propagam
- a grande quantidade de pessoas que elas conseguem atingir, de diferentes faixas etárias
- a grande quantidade de informações pessoais que apresentam
- a dificuldade de exclusão e controle sobre as informações divulgadas
- o tempo em que as informações ficam disponíveis
- o alto grau de confiança que os usuários costumam depositar entre si
- as novas oportunidades de negócios que trazem.

Além disso as redes sociais estão presentes nos mais diversos meios, como pessoal, profissional, econômico, político e jornalístico.

Todas essas características somadas a popularidade dos dispositivos móveis fizeram com que as redes sociais chamassem a atenção, também, de pessoas mal-intencionadas.

Por isso, para usar as redes sociais de forma segura, é muito importante que você esteja ciente dos riscos que elas podem representar e possa, assim, tomar medidas preventivas para evitá-los.

REDES SOCIAIS: CURTA COM MODERAÇÃO

RISCOS PRINCIPAIS

- **Contato com pessoas mal-intencionadas:** qualquer um pode criar um perfil falso e, sem que saiba, você pode ter na sua lista de contatos pessoas com as quais jamais se relacionaria no dia a dia
- **Furto de identidade:** assim como você pode ter um impostor na sua lista de contatos, também pode acontecer de alguém tentar se passar por você e criar um perfil falso
- **Invasão de perfil:** seu perfil pode ser invadido por meio de ataques de força bruta, do acesso a páginas falsas ou do uso de computadores infectados
- **Uso indevido de informações:** aquilo que você divulga pode vir a ser mal-interpretado e usado contra você
- **Invasão de privacidade**: quanto maior a sua rede de contatos, maior é o número de pessoas que possui acesso ao que você divulga, e menores são as garantias de que suas informações não serão repassadas
- **Recebimento de mensagens maliciosas:** alguém pode lhe enviar uma mensagem contendo boatos ou induzi-lo a clicar em um *link* que o fará instalar um código malicioso ou acessar uma página *web* comprometida
- **Acesso a conteúdos impróprios ou ofensivos:** como não há um controle imediato sobre o que as pessoas divulgam, pode ocorrer de você se deparar com mensagens ou imagens que contenham pornografia, violência ou que incitem o ódio e o racismo
- **Danos à imagem e à reputação:** calúnia e difamação podem rapidamente se propagar, jamais serem excluídas e causarem grandes danos às pessoas envolvidas

CUIDADOS A SEREM TOMADOS

PROTEJA O SEU PERFIL

» Acesse o *site* da rede social sempre usando conexão segura (HTTPS)

» Seja cuidadoso ao usar e ao elaborar as suas senhas

- use senhas longas, compostas de diferentes tipos de caracteres
- não use dados pessoais, como nome, sobrenome e datas
- evite usar a mesma senha para acessar diferentes *sites*

» Habilite a notificação de *login* e a verificação em duas etapas, sempre que estes recursos estiverem disponíveis

» Evite cadastrar perguntas de segurança que possam ser facilmente descobertas

» Procure cadastrar um *e-mail* de recuperação que você acesse regularmente

» Solicite o arquivo com suas informações ou verifique o registro de atividades, caso desconfie que seu perfil tenha sido indevidamente usado

» Use opções como silenciar, bloquear e denunciar, caso identifique abusos

MANTENHA SEU COMPUTADOR E DISPOSITIVOS MÓVEIS SEGUROS

» Mantenha todos os programas instalados com as versões mais recentes

» Aplique todas as atualizações disponíveis

» Utilize e mantenha atualizados mecanismos de segurança, como *antispam*, antivírus e *firewall* pessoal

» Desconfie de mensagens recebidas, mesmo que tenham sido enviadas por conhecidos

» Seja cuidadoso ao acessar *links* reduzidos

- use complementos que permitam que você expanda o *link* antes de clicar sobre ele

PROTEJA A SUA PRIVACIDADE

» Considere que você está em um local público, que tudo que você divulga pode ser lido ou acessado por qualquer pessoa

» Pense bem antes de divulgar algo, pois não é possível voltar atrás

» Use as configurações de privacidade oferecidas pelos *sites* e seja o mais restritivo possível

» Mantenha seu perfil e seus dados privados

» Restrinja o acesso ao seu endereço de *e-mail*

» Seja cuidadoso ao aceitar seus contatos e ao se associar a grupos

» Não confie na promessa de anonimato oferecida por algumas redes sociais e aplicativos

  - de acordo com as informações divulgadas é possível inferir a sua identidade e de outras pessoas

» Seja cuidadoso ao fornecer a sua localização

  - cuidado ao divulgar fotos e vídeos, pois ao observar onde eles foram gerados pode ser possível deduzir a sua localização
  - não divulgue planos de viagens e nem por quanto tempo ficará ausente da sua residência
  - ao usar redes sociais baseadas em geolocalização, procure fazer *check-in* apenas em locais movimentados e, de preferência, ao sair do local
  - cuidado ao confirmar sua presença em eventos públicos organizados via redes sociais

RESPEITE A PRIVACIDADE ALHEIA

» Evite falar sobre as ações, hábitos e rotina de outras pessoas

» Não divulgue, sem autorização, imagens em que outras pessoas apareçam

» Não divulgue mensagens ou imagens copiadas do perfil de pessoas que restrinjam o acesso

» Tente imaginar como a outra pessoa se sentiria ao saber que aquilo está se tornando público

PROTEJA SEUS FILHOS

» Informe seus filhos sobre os riscos de uso das redes sociais

» Respeite os limites de idade estipulados pelos *sites*

» Não exponha excessivamente seus filhos

- muitos pais criam perfis em nome dos filhos e postam sobre eles ou como se fossem eles. Isso pode desagradar e confundir as crianças
- evite constranger seus filhos, divulgando fotos ou comentários que possam embaraçá-los
- seja cuidadoso ao divulgar imagens de seus filhos. O que para você pode ser algo inocente, para outras pessoas pode ter uma conotação diferente

» Oriente-os:
  - para não se relacionarem com estranhos e nunca fornecerem informações pessoais
  - para não divulgarem informações sobre hábitos familiares e nem de localização (atual ou futura)
  - para não marcarem encontros com estranhos
  - sobre os riscos de uso da *webcam* e que ela não deve ser usada para se comunicar com estranhos
  - para usar opções como silenciar, bloquear e denunciar, caso alguém os esteja incomodando

PROTEJA A SUA VIDA PROFISSIONAL

» Ao usar redes sociais profissionais procure ser formal e evite tratar de assuntos pessoais

» Antes de postar algo avalie se, de alguma forma, aquilo pode atrapalhar a sua carreira

» Cuidado ao permitir que seus filhos usem o mesmo computador ou dispositivo móvel que você usa para tratar de assuntos profissionais
  - alguns aplicativos, como jogos, divulgam automaticamente nas redes sociais, dependendo das configurações

» Verifique se sua empresa possui um código de conduta e evite divulgar detalhes sobre o seu trabalho

» Oriente seus familiares para não divulgarem informações sobre a sua empresa e vida profissional

PROTEJA A SUA EMPRESA

» Crie um código de conduta

» Invista em treinamento e em campanhas de conscientização

» Informe aos funcionários sobre as regras de acesso durante o expediente e sobre o comportamento esperado, referente à divulgação de informações profissionais e à emissão de opiniões que possam comprometer a empresa

» Cuide da imagem. Observe a opinião de clientes e consumidores ou qualquer ação que envolva o nome da empresa, para que seja capaz de tomar atitudes em tempo de evitar algum dano

SAIBA MAIS

» Para mais detalhes sobre este e outros assuntos relacionados com cuidados na Internet, consulte os demais Fascículos da Cartilha de Segurança e o Livro Segurança na Internet, disponíveis em: **cartilha.cert.br**

» Procurando material para conversar sobre segurança com diferentes públicos? O Portal Internet Segura apresenta uma série de materiais focados em crianças, adolescentes, pais, responsáveis e educadores, confira em: **internetsegura.br**

cert.br

O CERT.br é o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Desde 1997, o grupo é responsável por tratar incidentes de segurança envolvendo redes conectadas à Internet no Brasil. O Centro também desenvolve atividades de análise de tendências, treinamento e conscientização, com o objetivo de aumentar os níveis de segurança e de capacidade de tratamento de incidentes no Brasil. Mais informações em **www.cert.br.**

nic.br

O Núcleo de Informação e Coordenação do Ponto BR — NIC.br (**www.nic.br**) é uma entidade civil, de direito privado e sem fins de lucro, que além de implementar as decisões e projetos do Comitê Gestor da Internet no Brasil, tem entre suas atribuições: coordenar o registro de nomes de domínio — Registro.br (**www.registro.br**), estudar, responder e tratar incidentes de segurança no Brasil — CERT.br (**www.cert.br**), estudar e pesquisar tecnologias de redes e operações — Ceptro.br (**www.ceptro.br**), produzir indicadores sobre as tecnologias da informação e da comunicação — Cetic.br (**www.cetic.br**), implementar e operar os Pontos de Troca de Tráfego — IX.br (**www.ix.br**), viabilizar a participação da comunidade brasileira no desenvolvimento global da Web e subsidiar a formulação de políticas públicas — Ceweb.br (**www.ceweb.br**), e abrigar o escritório do W3C no Brasil (**www.w3c.br**).

cgi.br

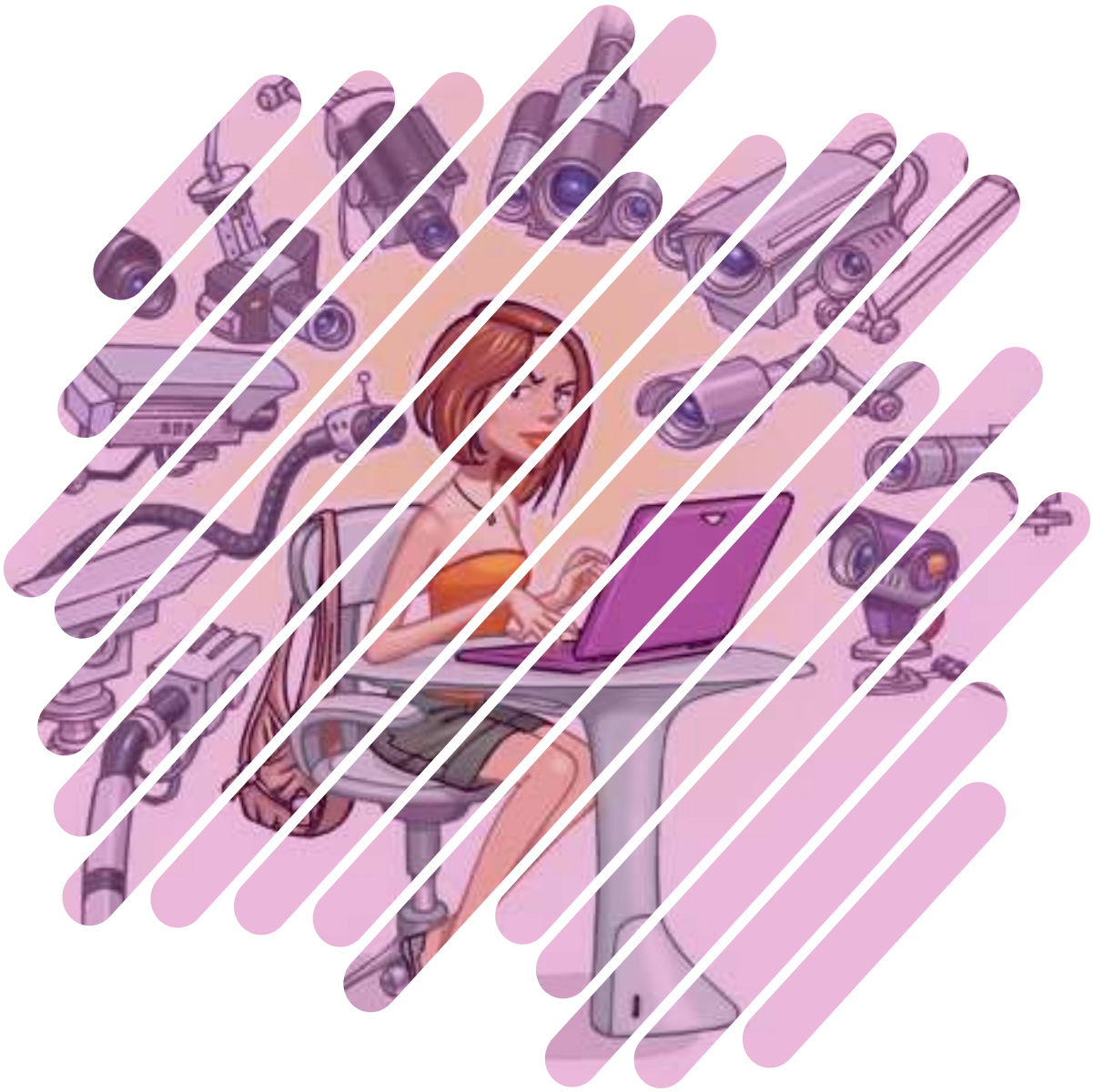
O Comitê Gestor da Internet no Brasil, responsável por estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil, coordena e integra todas as iniciativas de serviços Internet no País, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados. Com base nos princípios do multissetorialismo e transparência, o CGI.br representa um modelo de governança da Internet democrático, elogiado internacionalmente, em que todos os setores da sociedade são partícipes de forma equânime de suas decisões. Uma de suas formulações são os 10 Princípios para a Governança e Uso da Internet (**www.cgi.br/principios**). Mais informações em **www.cgi.br**.

outubro / 2020

Cartilha de Segurança para Internet

FASCÍCULO

PRIVACIDADE



Apoio de Divulgação:

UFPE

SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

Produção:

cert.br nic.br cgi.br

QUANTO MAIS INFORMAÇÕES VOCÊ DISPONIBILIZA NA INTERNET, MAIS DIFÍCIL SE TORNA PRESERVAR A SUA PRIVACIDADE

Nada impede que você abra mão de sua privacidade e, de livre e espontânea vontade, divulgue suas informações. Entretanto, a sua privacidade pode ser exposta independentemente da sua vontade, por exemplo quando:

- alguém divulga informações sobre você ou imagens onde você está presente, sem a sua autorização prévia
- um *site* que você utiliza altera as políticas de privacidade, sem aviso prévio, expondo informações anteriormente restritas
- um impostor se faz passar por você, cria um *e-mail* ou perfil falso em seu nome e o utiliza para coletar informações pessoais sobre você
- um atacante invade a sua conta de *e-mail* ou de sua rede social e acessa informações restritas
- alguém coleta informações que trafegam na rede sem estarem criptografadas, como o conteúdo dos *e-mails* enviados e recebidos por você
- um atacante ou um código malicioso obtém acesso aos dados que você digita ou que estão armazenados em seu computador
- um atacante invade um computador no qual seus dados estão armazenados, como, por exemplo, um servidor de *e-mails*
- seus hábitos e suas preferências de navegação são coletadas pelos *sites* que você acessa e repassadas para terceiros
- um aplicativo instalado em seu computador ou em seu dispositivo móvel coleta seus dados pessoais e os envia ao desenvolvedor/fabricante
- recursos do seu computador, como diretórios, são compartilhados sem as configurações de acesso adequadas.

PRIVACIDADE: PRESERVE A SUA

RISCOS PRINCIPAIS

Preservar a sua privacidade pode ajudá-lo a se proteger dos golpes e ataques aplicados na Internet. A divulgação e a coleta indevida de informações pessoais pode:

- Comprometer a sua privacidade, de seus amigos e familiares
  - mesmo que você restrinja o acesso a uma informação, não há como controlar que ela não será repassada
- Facilitar o furto da sua identidade
  - quanto mais informações você disponibiliza sobre a sua vida e rotina, mais fácil se torna para um golpista criar uma identidade falsa em seu nome, pois mais convincente ele poderá ser
  - a identidade falsa criada pelo golpista pode ser usada para atividades maliciosas, como efetuar transações financeiras, acessar *sites*, enviar mensagens eletrônicas, abrir empresas fantasmas e criar contas bancárias ilegítimas
- Facilitar a invasão de suas contas de usuário (por exemplo, de *e-mail* ou de rede social)
  - caso você use dados pessoais para elaborar suas senhas ou como resposta de dicas/questões de segurança, elas podem ser facilmente adivinhadas
- Fazer com que propagandas direcionadas sejam apresentadas
- Causar perdas financeiras, perda de reputação e falta de crédito
- Colocar em risco a sua segurança física
- Favorecer o recebimento de *spam*

CUIDADOS A SEREM TOMADOS

AO ACESSAR E ARMAZENAR SEUS *E-MAILS*

» Configure seu programa leitor de *e-mails* para não abrir imagens que não estejam na própria mensagem
  - o fato da imagem ser acessada pode ser usado para confirmar que o *e-mail* foi lido

» Use programas leitores de *e-mails* que permitam que as mensagens sejam criptografadas
  - mensagens criptografadas somente poderão ser lidas por quem conseguir decodificá-las

» Armazene *e-mails* confidenciais em formato criptografado
  - isso pode evitar que sejam lidos por atacantes ou pela ação de códigos maliciosos
  - você pode decodificá-los sempre que desejar lê-los

» Use conexão segura quando acessar *e-mails* por meio de navegadores *web*
  - mesmo que você restrinja o acesso a uma informação, não há como controlar que ela não será repassada

» Use criptografia para conexão entre seu leitor de *e-mails* e os servidores de *e-mail* do seu provedor

» Seja cuidadoso ao acessar seu *webmail*
  - digite a URL diretamente no navegador
  - tenha cuidado ao clicar em *links* recebidos por meio de mensagens eletrônicas

AO MANIPULAR SEUS DADOS

» Mantenha seus *backups* em locais seguros e com acesso restrito

» Armazene dados sensíveis em formato criptografado

» Cifre o disco do seu computador e dispositivos removíveis, como disco externo e *pendrive*

» Ao usar serviços de *backup online*, leve em consideração a política de privacidade e de segurança do *site*

AO NAVEGAR NA WEB

» Seja cuidadoso ao usar *cookies*, por meio de uma ou mais das seguintes opções:

- defina um nível de permissão superior ou igual a "médio"
- configure para que os *cookies* sejam apagados assim que o navegador for fechado
- configure para que *cookies* de terceiros não sejam aceitos
  - isso não deverá prejudicar a sua navegação, pois serão bloqueados apenas conteúdos relacionados a publicidade
- você pode também configurar para que, por padrão:
  - os *sites* não possam definir *cookies* e criar listas de exceções, cadastrando *sites* considerados confiáveis e onde o uso é realmente necessário, ou
  - os *sites* possam definir *cookies* e criar listas de exceções, cadastrando os *sites* que deseja bloquear

» Quando disponível, procure utilizar:

- navegação anônima, principalmente ao usar computadores de terceiros
  - dessa forma, informações sobre a sua navegação, como *sites* acessados, dados de formulários e *cookies*, não serão armazenadas

AO COMPARTILHAR RECURSOS DO SEU COMPUTADOR

» Estabeleça senhas para os compartilhamentos e permissões de acesso adequadas

» Compartilhe seus recursos pelo tempo mínimo necessário

AO DIVULGAR INFORMAÇÕES NA WEB (REDES SOCIAIS)

» Esteja atento e avalie com cuidado as informações divulgadas em sua página *web*, rede social ou *blog*
  - elas podem ser usadas em golpes de engenharia social, para obter informações sobre você, para atentar contra a segurança do seu computador ou contra a sua segurança física
  - considere que você está em um local público, que tudo que você divulga pode ser lido ou acessado por qualquer pessoa

» Pense bem antes de divulgar algo, pois não é possível voltar atrás

» Divulgue a menor quantidade possível de informações, tanto sobre você como sobre seus amigos e familiares
  - oriente-os a fazer o mesmo

» Sempre que alguém solicitar dados sobre você ou quando preencher algum cadastro, reflita se é realmente necessário que aquela empresa ou pessoa tenha acesso àquelas informações

» Ao receber ofertas de emprego pela Internet que solicitem o seu currículo, tente limitar a quantidade de informações nele disponibilizada
  - apenas forneça mais dados quando estiver seguro de que tanto a empresa como a oferta são legítimas

» Fique atento a ligações telefônicas e *e-mails* pelos quais alguém, geralmente falando em nome de alguma instituição, solicita informações pessoais sobre você, inclusive senhas

» Seja cuidadoso ao divulgar a sua localização geográfica
  - com base nela, é possível descobrir a sua rotina, deduzir informações (como hábitos e classe financeira) e tentar prever seus próximos passos ou de seus familiares

» Verifique a política de privacidade dos *sites* que você utiliza e fique atento às mudanças, principalmente aquelas relacionadas ao tratamento de dados pessoais, para não ser surpreendido com alterações que possam comprometer a sua privacidade

» Use as opções de privacidade oferecidas pelos *sites* e seja o mais restritivo possível

» Mantenha seu perfil e seus dados privados

» Seja seletivo ao aceitar seus contatos e ao se associar a grupos e comunidades

PROTEJA SUAS CONTAS E SENHAS

» Seja cuidadoso ao elaborar as suas senhas
  - use senhas longas, compostas de diferentes tipos de caracteres
  - não utilize dados pessoais, como nome, sobrenome e datas
  - não utilize dados que possam ser facilmente obtidos sobre você

» Evite reutilizar suas senhas, não use a mesma senha para acessar diferentes *sites*

» Não forneça suas senhas para outra pessoa, em hipótese alguma

» Ao usar perguntas de segurança para facilitar a recuperação de senhas, evite escolher questões cujas respostas possam ser facilmente adivinhadas

PROTEJA SEU COMPUTADOR E SEUS DISPOSITIVOS MÓVEIS

» Mantenha o seu computador/dispositivo móvel seguro
  - com a versão mais recente de todos os programas instalados
  - com todas as atualizações aplicadas

» Utilize e mantenha atualizados mecanismos de segurança, como *antispam*, *antimalware* e *firewall* pessoal

» Ao instalar aplicativos desenvolvidos por terceiros:
  - seja cuidadoso ao permitir que os aplicativos acessem seus dados pessoais, como listas de contatos e localização geográfica
  - verifique se as permissões necessárias para a instalação e execução são coerentes, ou seja, um programa de jogos não necessariamente precisa ter acesso à sua lista de chamadas
  - seja seletivo ao selecionar os aplicativos, escolhendo aqueles bem avaliados e com grande quantidade de usuários

SAIBA MAIS

» Para mais detalhes sobre este e outros assuntos relacionados com cuidados na Internet, consulte os demais Fascículos da Cartilha de Segurança e o Livro Segurança na Internet, disponíveis em: **cartilha.cert.br**

» Procurando material para conversar sobre segurança com diferentes públicos? O Portal Internet Segura apresenta uma série de materiais focados em crianças, adolescentes, pais, responsáveis e educadores, confira em: **internetsegura.br**

cert.br

O CERT.br é o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Desde 1997, o grupo é responsável por tratar incidentes de segurança envolvendo redes conectadas à Internet no Brasil. O Centro também desenvolve atividades de análise de tendências, treinamento e conscientização, com o objetivo de aumentar os níveis de segurança e de capacidade de tratamento de incidentes no Brasil. Mais informações em **www.cert.br.**

nic.br

O Núcleo de Informação e Coordenação do Ponto BR — NIC.br (**www.nic.br**) é uma entidade civil, de direito privado e sem fins de lucro, que além de implementar as decisões e projetos do Comitê Gestor da Internet no Brasil, tem entre suas atribuições: coordenar o registro de nomes de domínio — Registro.br (**www.registro.br**), estudar, responder e tratar incidentes de segurança no Brasil — CERT.br (**www.cert.br**), estudar e pesquisar tecnologias de redes e operações — Ceptro.br (**www.ceptro.br**), produzir indicadores sobre as tecnologias da informação e da comunicação — Cetic.br (**www.cetic.br**), implementar e operar os Pontos de Troca de Tráfego — IX.br (**www.ix.br**), viabilizar a participação da comunidade brasileira no desenvolvimento global da Web e subsidiar a formulação de políticas públicas — Ceweb.br (**www.ceweb.br**), e abrigar o escritório do W3C no Brasil (**www.w3c.br**).

cgi.br

O Comitê Gestor da Internet no Brasil, responsável por estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil, coordena e integra todas as iniciativas de serviços Internet no País, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados. Com base nos princípios do multissetorialismo e transparência, o CGI.br representa um modelo de governança da Internet democrático, elogiado internacionalmente, em que todos os setores da sociedade são partícipes de forma equânime de suas decisões. Uma de suas formulações são os 10 Princípios para a Governança e Uso da Internet (**www.cgi.br/principios**). Mais informações em **www.cgi.br**.

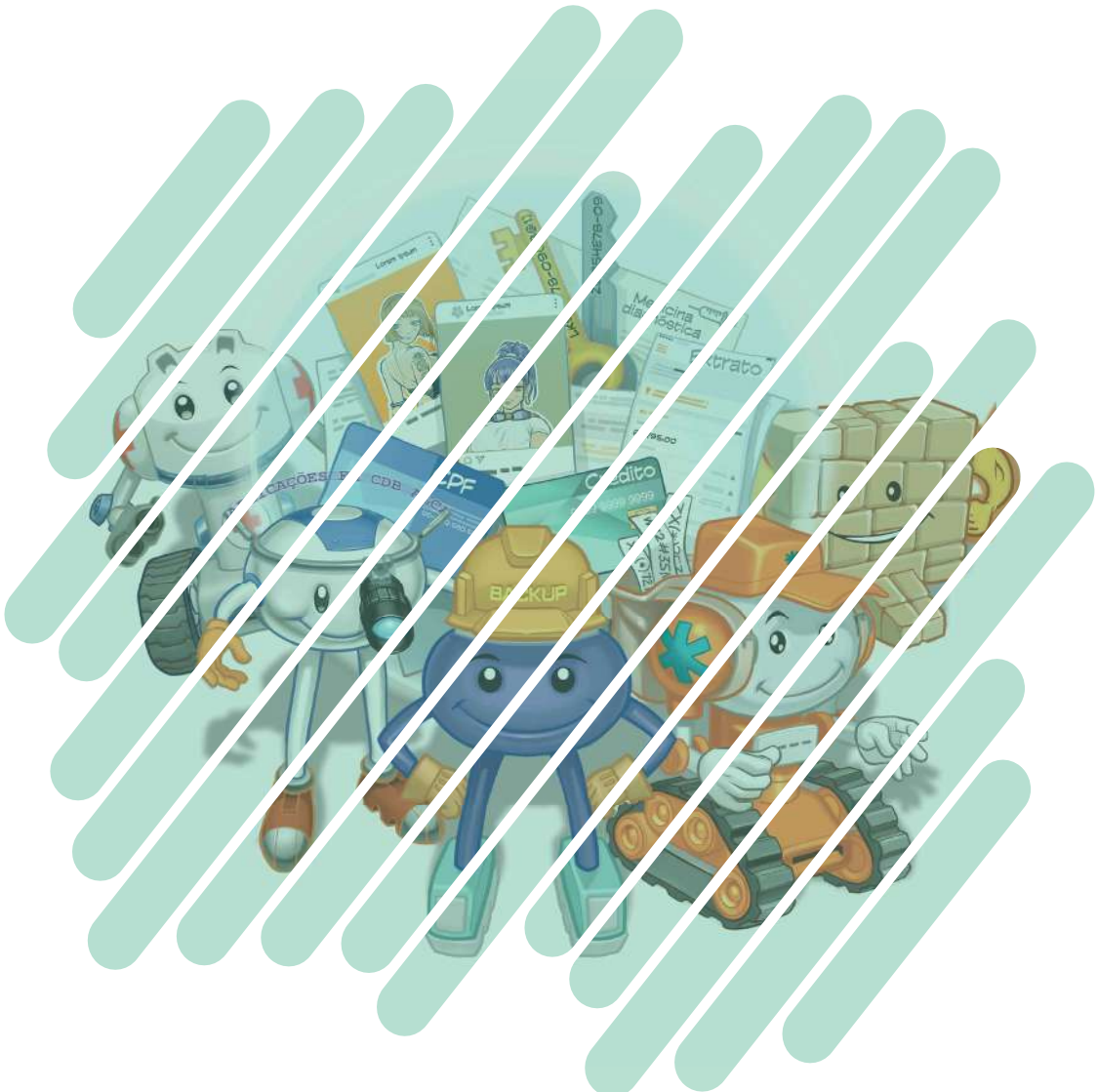
cartilha.cert.br/cc

outubro / 2020

Cartilha de Segurança para Internet

FASCÍCULO

PROTEÇÃO DE DADOS



Apoio de Divulgação:

UFPE

STI SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

Contribuição:

ANPD

Produção:

cert.br nic.br cgi.br

VOCÊ JÁ REPAROU NA QUANTIDADE DE DADOS QUE POSSUI E PRODUZ?

Dados de cadastros, biográficos, profissionais, financeiros e de navegação são apenas alguns exemplos de dados referentes a você que, diariamente, circulam por diversas redes e são armazenados em diferentes sistemas, dispositivos e mídias.

Infelizmente, há situações em que seus dados podem ser perdidos, indevidamente acessados ou até mesmo coletados e vendidos sem que você tenha ciência disso. Alguns exemplos dessas situações incluem:

- você perde o celular, computador ou mídia removível
- seus dados são interceptados ao trafegarem nas redes
- 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.

Para tentar evitar essas situações, proteger seus dados e assegurar que eles sejam tratados de forma adequada há um conjunto de mecanismos de segurança que você pode usar. Por exemplo, o uso de senhas fortes impede o acesso indevido às contas e a criptografia dificulta que seus dados sejam acessados e alterados indevidamente.

Há situações, entretanto, em que os mecanismos de segurança sozinhos não protegem seus dados; por exemplo, quando eles são passados deliberadamente a outros sem sua autorização ou são coletados sem necessidade.

Por isso, adotar uma postura preventiva, tentando reduzir a quantidade de dados fornecida por você, é essencial. Para coibir abusos, garantir seus direitos e agir adequadamente quando necessário é importante também que você conheça um pouco da legislação vigente.

SEUS DADOS SÃO VALIOSOS: PROTEJA-OS

COMO SEUS DADOS PODEM SER ABUSADOS

O abuso de seus dados pode acarretar prejuízos financeiros, restrição a direitos ou benefícios e invasão da sua privacidade. Esse abuso pode ocorrer de diversas formas:

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, aos seus equipamentos ou mídias
- em casos de vazamentos de dados

COLETA EXCESSIVA

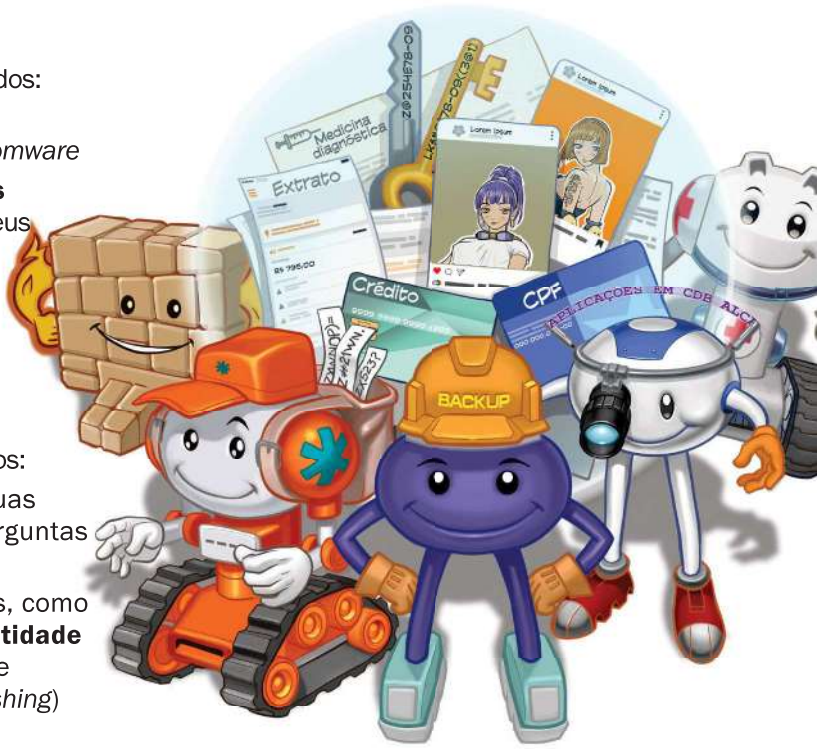
» Muitos aplicativos e *sites* coletam dados extras sem o seu conhecimento e os utilizam para a elaboração de perfis de comportamento (*profiling*)

» Seu perfil pode, então, ser usado, sem o seu consentimento, de forma discriminatória ou para fins como propagandas

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 tentar adivinhar suas senhas e responder perguntas de segurança
- em tentativas de golpes, como **extorsão**, **furto de identidade** e ***phishing*** direcionado e personalizado (*spear phishing*)

COMO SE PREVENIR

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 *backup* regularmente
- Teste periodicamente
- 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 recursos de criptografia para armazená-los
- 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
- **Ative** as configurações de **criptografia** em seus **discos** e **mídias**, como *pen drives* e discos externos
- Use conexões seguras, sempre que possível

CONTAS E SENHAS

- Crie **senhas fortes** e não repita senhas
- Habilite a **verificação em duas etapas** em todas as suas contas
- Habilite, quando disponíveis, **notificações de *login***, para ser mais fácil perceber se outras pessoas estiverem usando suas contas
- Tenha certeza de sair de suas contas (*logout*) ao usar equipamentos compartilhados
- Habilite as configurações de privacidade e segurança nos serviços

APLICATIVOS

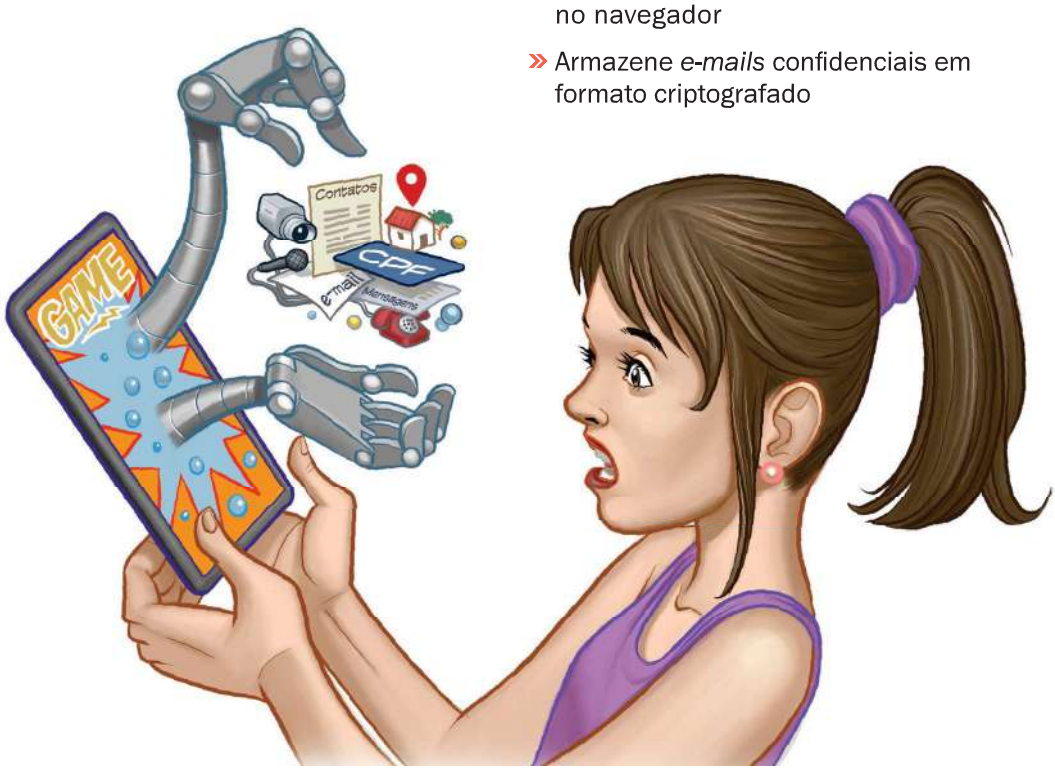
- Instale aplicativos somente de **fontes e lojas oficiais**
- Antes de instalar, verifique as telas e o nome do aplicativo, pois muitos falsos aplicativos se assemelham aos oficiais
- Observe se o **desenvolvedor é confiável**, quantas pessoas instalaram o aplicativo e qual a opinião delas sobre ele
- Durante a instalação, **fique atento às permissões**:
  - forneça apenas aquelas que considerar necessárias
  - por exemplo, um aplicativo de teste de velocidade não precisa ter acesso aos seus contatos para funcionar
- **Limite** quais aplicativos podem acessar o microfone, a câmera, seus contatos e sua localização
- Apague os aplicativos que você não usa mais

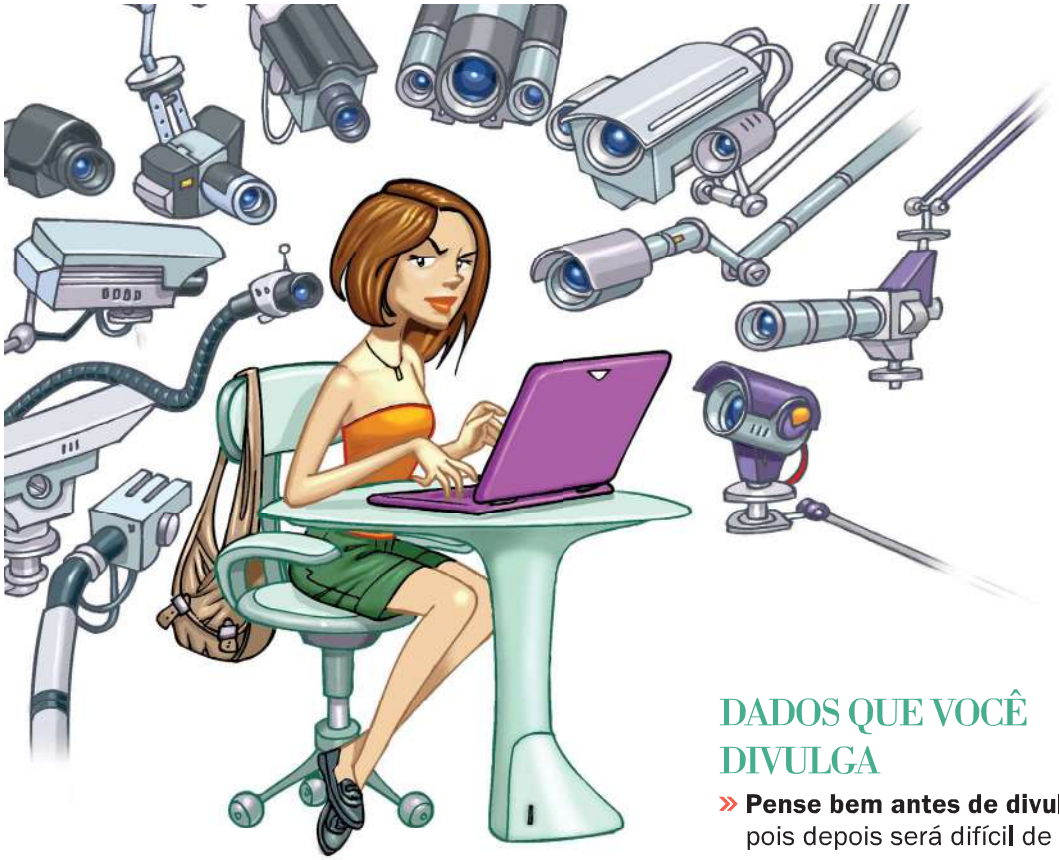
EQUIPAMENTOS E MÍDIAS

- 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**, sobrescrevendo discos ou restaurando opções de fábrica
- Escolha empresas com **boa reputação**, ao enviar seus equipamentos para **manutenção**
- Seja cuidadoso ao usar equipamentos de terceiros

E-MAILS E MENSAGENS ELETRÔNICAS

- **Desconfie** de *links* ou pedidos de pagamentos recebidos via mensagens eletrônicas, **mesmo que vindos de pessoas conhecidas**
- Seja cuidadoso ao acessar seu *webmail*: digite a URL diretamente no navegador
- Armazene *e-mails* confidenciais em formato criptografado





REDUZA A QUANTIDADE DE DADOS SOBRE VOCÊ NA INTERNET

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** e podem ser usadas para criar sua reputação *online* e definir seu perfil comportamental.

DADOS QUE VOCÊ DIVULGA

- **Pense bem antes de divulgar algo**, pois depois será difícil de excluir
- Seja **seletivo** ao aceitar seus **contatos** nas redes sociais
- **Ao preencher cadastros questione-se** sobre a real necessidade de fornecer todos os dados, e de a 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 SEUS DIREITOS

A LEI GERAL DE PROTEÇÃO DE DADOS (LGPD)

» A LGPD foi criada para que o indivíduo tenha **controle** sobre seus **dados pessoais** e saiba **como** esses dados **são tratados** por organizações públicas, privadas e terceiros

» Segundo a LGPD são considerados dados pessoais as 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

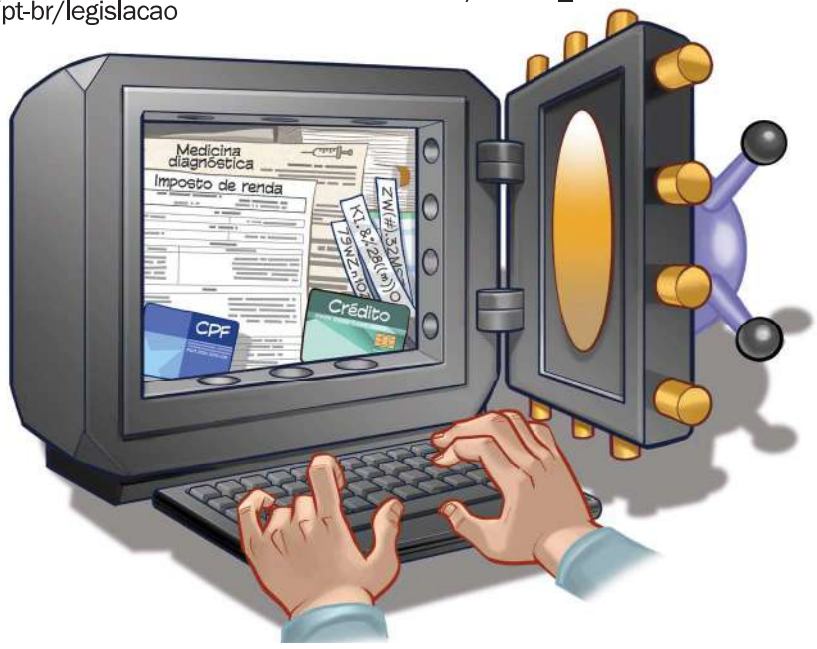
BENEFÍCIOS E DIREITOS TRAZIDOS PELA LGPD

» A LGPD dá a você o direito de **saber** exatamente como seus dados **são tratados**, quais dados são **coletados** e o porquê e com quem eles são **compartilhados**

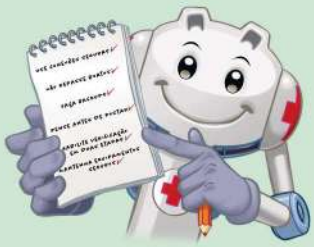
» Organizações públicas e privadas devem disponibilizar informações claras que o ajudem a compreender os termos de consentimento e as bases legais que apoiam o tratamento dos seus dados

» A LGPD traz maior segurança jurídica, ao fornecer mecanismos para que você tenha controle sobre quais dados seus são coletados e como são usados

» **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, através deste *link*: https://www.gov.br/anpd/pt-br/canais_atendimento



SAIBA MAIS



» Para mais detalhes sobre este e outros assuntos relacionados com cuidados na Internet, consulte os demais Fascículos da Cartilha de Segurança e o Livro Segurança na Internet, disponíveis em: **cartilha.cert.br**

» Procurando material para conversar sobre segurança com diferentes públicos? O Portal Internet Segura apresenta uma série de materiais focados em crianças, adolescentes, pais, responsáveis e educadores, confira em: **internetsegura.br**

cert.br

O CERT.br é o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Desde 1997, o grupo é responsável por tratar incidentes de segurança envolvendo redes conectadas à Internet no Brasil. O Centro também desenvolve atividades de análise de tendências, treinamento e conscientização, com o objetivo de aumentar os níveis de segurança e de capacidade de tratamento de incidentes no Brasil. Mais informações em **www.cert.br.**

nic.br

O Núcleo de Informação e Coordenação do Ponto BR — NIC.br (**www.nic.br**) é uma entidade civil, de direito privado e sem fins de lucro, que além de implementar as decisões e projetos do Comitê Gestor da Internet no Brasil, tem entre suas atribuições: coordenar o registro de nomes de domínio — Registro.br (**www.registro.br**), estudar, responder e tratar incidentes de segurança no Brasil — CERT.br (**www.cert.br**), estudar e pesquisar tecnologias de redes e operações — Ceptro.br (**www.ceptro.br**), produzir indicadores sobre as tecnologias da informação e da comunicação — Cetic.br (**www.cetic.br**), implementar e operar os Pontos de Troca de Tráfego — IX.br (**www.ix.br**), viabilizar a participação da comunidade brasileira no desenvolvimento global da Web e subsidiar a formulação de políticas públicas — Ceweb.br (**www.ceweb.br**), e abrigar o escritório do W3C no Brasil (**www.w3c.br**).

cgi.br

O Comitê Gestor da Internet no Brasil, responsável por estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil, coordena e integra todas as iniciativas de serviços Internet no País, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados. Com base nos princípios do multissetorialismo e transparência, o CGI.br representa um modelo de governança da Internet democrático, elogiado internacionalmente, em que todos os setores da sociedade são partícipes de forma equânime de suas decisões. Uma de suas formulações são os 10 Princípios para a Governança e Uso da Internet (**www.cgi.br/principios**). Mais informações em **www.cgi.br.**

ANPD

A Autoridade Nacional de Proteção de Dados – ANPD é um órgão vinculado à Presidência da República, dotada de autonomia técnica e decisória, que tem a competência de zelar pela proteção dos dados pessoais com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, conforme disposto na Lei nº 13.709, de 14 de agosto de 2018, a LGPD. Mais informações em **www.gov.br/anpd.**

cartilha.cert.br/cc

maio / 2021

Cartilha de Segurança para Internet

FASCÍCULO

COMPUTADORES

Apoio de Divulgação:

UFPE

STI SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

Produção:

cert.br nic.br cgi.br

MANTER SEU COMPUTADOR SEGURO É ESSENCIAL PARA SE PROTEGER DOS RISCOS ENVOLVIDOS NO USO DA INTERNET

Um grande risco que você pode correr ao usar a Internet é o de achar que não corre riscos, pois supõe que ninguém tem interesse em usar o seu computador ou que, entre os diversos computadores existentes, o seu dificilmente será localizado.

É justamente este tipo de pensamento que é explorado pelos atacantes, pois, ao se sentir seguro, você também pode achar que não precisa se prevenir. Esta falsa ilusão de segurança costuma terminar quando começam a acontecer os primeiros problemas.

Muitas vezes os atacantes estão interessados em conseguir acesso a grandes quantidades de computadores, independente de quais são e das configurações que possuem, e isso pode incluir o seu.

Por isto, acreditar que seu computador está protegido por não apresentar atrativos para um atacante pode ser um grande erro.

Seu computador pode ser invadido ou infectado, por exemplo, por meio:

- da ação direta de atacantes
- da exploração de contas de usuário sem senha ou com senha fraca
- da exploração de vulnerabilidades existentes nos programas instalados
- da auto-execução de mídias removíveis infectadas, como *pen drives*
- do acesso a páginas *web* maliciosas, utilizando navegadores vulneráveis
- da ação de códigos maliciosos, recebidos pela rede, obtidos em mensagens eletrônicas, via mídias removíveis, em páginas *web* ou de outros computadores.

PRESERVE A INTERNET: PROTEJA SEU COMPUTADOR

RISCOS PRINCIPAIS

Muito provavelmente é em seu computador que a maioria dos seus dados está gravada e, por meio dele, que você acessa *e-mails* e redes sociais e realiza transações bancárias e comerciais. Caso ele seja comprometido, você pode enfrentar problemas como:

- Invasão de privacidade
- Furto de identidade
- Vazamento de informações
- Perda de dados
- Perdas fincanceiras
- Ficar sem acesso ao computador

Além disso, seu computador ainda pode ser usado para atividades maliciosas, como:

- Infectar, invadir e atacar outros computadores
- Aplicar golpes em outros usuários
- Servir de repositório para dados fraudulentos
- Propagar códigos maliciosos
- Disseminar *spam*
- Esconder a real identidade e localização de um atacante

CUIDADOS A SEREM TOMADOS

MANTENHA OS PROGRAMAS ATUALIZADOS

» Tenha sempre as versões mais recentes dos programas instalados

» Remova as versões antigas e os programas que você não utiliza mais

INSTALE AS ATUALIZAÇÕES DISPONÍVEIS

» Configure os programas para serem atualizados automaticamente

» Programe as atualizações automáticas para serem baixadas e aplicadas em um horário em que o computador esteja ligado e conectado à Internet

» Cheque periodicamente por novas atualizações, usando as opções disponíveis nos programas

USE APENAS PROGRAMAS ORIGINAIS

» Ao comprar um computador pré-instalado, certifique-se de que os programas são originais solicitando ao revendedor as licenças de uso

» Caso deseje usar um programa proprietário, mas não possa adquirir a licença, procure por alternativas gratuitas ou mais baratas, e que possuam funcionalidades semelhantes às desejadas

AO INSTALAR APLICATIVOS DESENVOLVIDOS POR TERCEIROS

» Verifique se as permissões de instalação e execução são coerentes

» Seja cuidadoso ao:

- permitir que os aplicativos acessem seus dados pessoais
- selecionar os aplicativos, escolhendo aqueles bem avaliados e com grande quantidade de usuários

USE MECANISMOS DE PROTEÇÃO

» Instale um antivírus (*antimalware*)

- mantenha-o atualizado, incluindo o arquivo de assinaturas
- configure-o para verificar todos os formatos de arquivos
- sempre verifique os arquivos recebidos antes de abri-los ou executá-los

» Assegure-se de ter um *firewall* pessoal instalado e ativo

» Crie um disco de emergência de seu antivírus e use-o se desconfiar que:

- o antivírus instalado está desabilitado/comprometido, ou
- o comportamento do computador está estranho (mais lento, gravando ou lendo o disco rígido com muita frequência, etc.)

» Crie um disco de recuperação do seu sistema e certifique-se de tê-lo por perto no caso de emergências

» Seja cuidadoso ao clicar em *link*s, independente de como foram recebidos e de quem os enviou

- antes de clicar em um *link* curto procure usar complementos que possibilitem que o *link* de destino seja visualizado
- não considere que mensagens vindas de conhecidos são sempre confiáveis
  - o campo de remetente pode ter sido falsificado, ou
  - elas podem ter sido enviadas de contas falsas ou invadidas

» Desabilite a auto-execução de mídias removíveis e de arquivos anexados

PROTEJA SUAS CONTAS DE ACESSO E SENHAS

» Crie uma conta padrão e use-a nas tarefas rotineiras
  - use a conta de administrador somente quando necessário e pelo menor tempo possível
  - use a opção de "executar como administrador" quando necessitar de privilégios administrativos

» Mantenha a conta de convidado desabilitada

» Assegure-se de que:
  - todas as contas de acesso existentes tenham senha
  - não existam contas de uso compartilhado
  - a conta de acesso e a senha sejam solicitadas na tela inicial
  - a opção de *login* automático esteja desabilitada

» Seja cuidadoso ao elaborar suas senhas
  - use senhas longas, compostas de diferentes tipos de caracteres
  - não utilize:
    - sequências de teclado
    - dados pessoais, como nome, sobrenome e datas
    - dados que possam ser facilmente obtidos sobre você

AO USAR O SEU COMPUTADOR EM LOCAIS PÚBLICOS

» Utilize travas que dificultem que ele seja aberto ou furtado

» Mantenha-o bloqueado, para evitar que seja indevidamente usado quando você não estiver por perto

» Utilize criptografia de disco
  - em caso de perda ou furto isso dificultará o acesso aos seus dados

» Configure-o para solicitar senha na tela inicial
  - isso dificulta que alguém reinicie seu computador e o acesse diretamente

SEJA CUIDADOSO AO USAR COMPUTADORES DE TERCEIROS

- Utilize opções de navegar anonimamente
- Não efetue transações bancárias ou comerciais
- Não utilize opções como “Lembre-se de mim” e “Continuar conectado”
- Não permita que suas senhas sejam memorizadas pelo navegador *web*
- Limpe os dados pessoais salvos pelo navegador
- Assegure-se de sair (*logout*) de suas contas de usuário
- Seja cuidadoso ao conectar mídias removíveis, como *pen drives*
- Ao retornar ao seu computador:
  - altere as senhas usadas
  - verifique seu *pen drive* com um antivírus

OUTROS CUIDADOS

- Faça regularmente *backup* dos seus dados
- Mantenha a data e a hora corretas
  - veja como manter seu computador sincronizado em **www.ntp.br**
- Verifique as configurações de segurança oferecidas pelos programas instalados em seu computador e adapte-as as suas necessidades
- Ao compartilhar recursos do seu computador:
  - estabeleça senhas e permissões de acesso adequadas
  - compartilhe seus recursos pelo tempo mínimo necessário
- Ao enviar seu computador para serviços de manutenção:
  - selecione empresas com boas referências
  - não permita a instalação de programas não originais
  - se possível faça *backup* dos seus dados antes de enviá-lo

SAIBA MAIS

» Para mais detalhes sobre este e outros assuntos relacionados com cuidados na Internet, consulte os demais Fascículos da Cartilha de Segurança e o Livro Segurança na Internet, disponíveis em: **cartilha.cert.br**

» Procurando material para conversar sobre segurança com diferentes públicos? O Portal Internet Segura apresenta uma série de materiais focados em crianças, adolescentes, pais, responsáveis e educadores, confira em: **internetsegura.br**

cert.br

O CERT.br é o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Desde 1997, o grupo é responsável por tratar incidentes de segurança envolvendo redes conectadas à Internet no Brasil. O Centro também desenvolve atividades de análise de tendências, treinamento e conscientização, com o objetivo de aumentar os níveis de segurança e de capacidade de tratamento de incidentes no Brasil. Mais informações em **www.cert.br.**

nic.br

O Núcleo de Informação e Coordenação do Ponto BR — NIC.br (**www.nic.br**) é uma entidade civil, de direito privado e sem fins de lucro, que além de implementar as decisões e projetos do Comitê Gestor da Internet no Brasil, tem entre suas atribuições: coordenar o registro de nomes de domínio — Registro.br (**www.registro.br**), estudar, responder e tratar incidentes de segurança no Brasil — CERT.br (**www.cert.br**), estudar e pesquisar tecnologias de redes e operações — Ceptro.br (**www.ceptro.br**), produzir indicadores sobre as tecnologias da informação e da comunicação — Cetic.br (**www.cetic.br**), implementar e operar os Pontos de Troca de Tráfego — IX.br (**www.ix.br**), viabilizar a participação da comunidade brasileira no desenvolvimento global da Web e subsidiar a formulação de políticas públicas — Ceweb.br (**www.ceweb.br**), e abrigar o escritório do W3C no Brasil (**www.w3c.br**).

cgi.br

O Comitê Gestor da Internet no Brasil, responsável por estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil, coordena e integra todas as iniciativas de serviços Internet no País, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados. Com base nos princípios do multissetorialismo e transparência, o CGI.br representa um modelo de governança da Internet democrático, elogiado internacionalmente, em que todos os setores da sociedade são partícipes de forma equânime de suas decisões. Uma de suas formulações são os 10 Princípios para a Governança e Uso da Internet (**www.cgi.br/principios**). Mais informações em **www.cgi.br**.

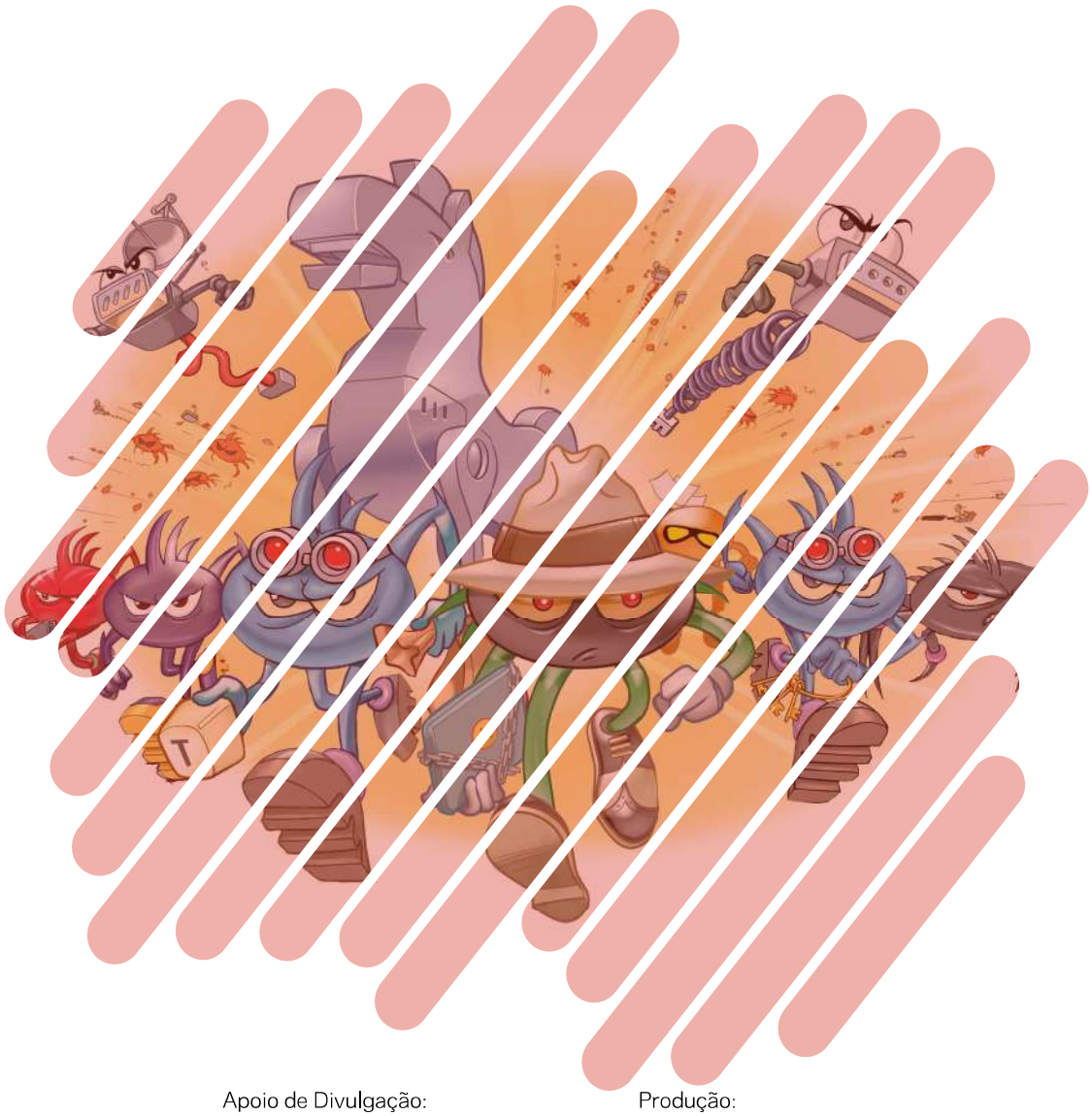
cartilha.cert.br/cc

outubro / 2020

Cartilha de Segurança para Internet

FASCÍCULO

CÓDIGOS MALICIOSOS



Apoio de Divulgação:

UFPE

STI SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

Produção:

cert.br nic.br cgi.br

CÓDIGOS MALICIOSOS SÃO USADOS COMO INTERMEDIÁRIOS E POSSIBILITAM A PRÁTICA DE GOLPES, A REALIZAÇÃO DE ATAQUES E O ENVIO DE *SPAM*

Códigos maliciosos, também conhecidos como pragas e *malware*, são programas desenvolvidos para executar ações danosas e atividades maliciosas em equipamentos, como computadores, *modems*, *switches*, roteadores e dispositivos móveis (*tablets*, celulares, *smartphones*, etc).

Um atacante pode instalar um código malicioso após invadir um equipamento ou explorando alguma vulnerabilidade existente nos programas nele instalados.

Seus equipamentos também podem ser infectados caso você:

- acesse páginas *web* maliciosas, usando navegadores vulneráveis
- acesse mídias removíveis infectadas, como *pen drives*
- execute arquivos infectados, obtidos em anexos de mensagens eletrônicas, via mídias removíveis, em páginas *web*, redes sociais ou diretamente de outros equipamentos.

Após infectar o seu equipamento, o código malicioso pode executar ações como se fosse você, como acessar informações, apagar arquivos, criptografar dados, conectar-se à Internet, enviar mensagens e ainda instalar outros códigos maliciosos.

A melhor prevenção contra os códigos maliciosos é impedir que a infecção ocorra pois nem sempre é possível reverter as ações danosas já feitas ou recuperar totalmente seus dados.

CÓDIGOS MALICIOSOS: PROTEJA-SE DESTA TURMA

TIPOS PRINCIPAIS

VÍRUS

programa ou parte de um programa de computador, normalmente malicioso, que se propaga inserindo cópias de si mesmo e se tornando parte de outros programas e arquivos

CAVALO DE TROIA (*TROJAN*)

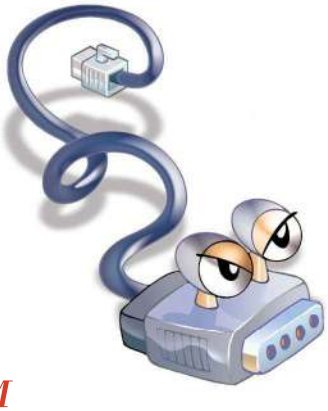
programa que, além de executar as funções para as quais foi aparentemente projetado, também executa outras funções, normalmente maliciosas, e sem o conhecimento do usuário

RANSOMWARE

programa que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate para restabelecer o acesso ao usuário

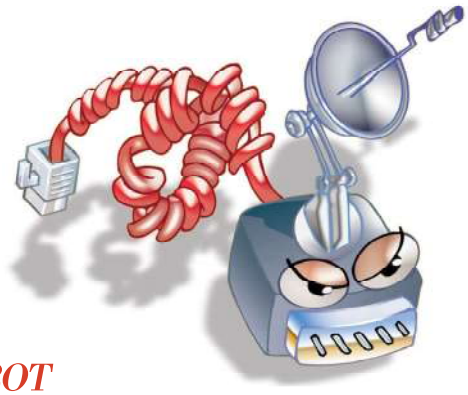
BACKDOOR

programa que permite o retorno de um invasor a um equipamento comprometido, por meio da inclusão de serviços criados ou modificados para este fim



WORM

programa capaz de se propagar automaticamente pelas redes, explorando vulnerabilidades nos programas instalados e enviando cópias de si mesmo de equipamento para equipamento



BOT

programa similar ao *worm* e que possui mecanismos de comunicação com o invasor que permitem que ele seja remotamente controlado

RAT (*REMOTE ACCESS TROJAN*)

ou *trojan* de acesso remoto, é um programa que combina as características de *trojan* e de *backdoor*, já que permite ao atacante acessar o equipamento remotamente e executar ações como se fosse o usuário

ZUMBI

é como também é chamado um equipamento infectado por um *bot*, pois pode ser controlado remotamente, sem o conhecimento do seu dono

BOTNET

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

SPYWARE

programa projetado para monitorar as atividades de um sistema e enviar as informações coletadas para terceiros

KEYLOGGER

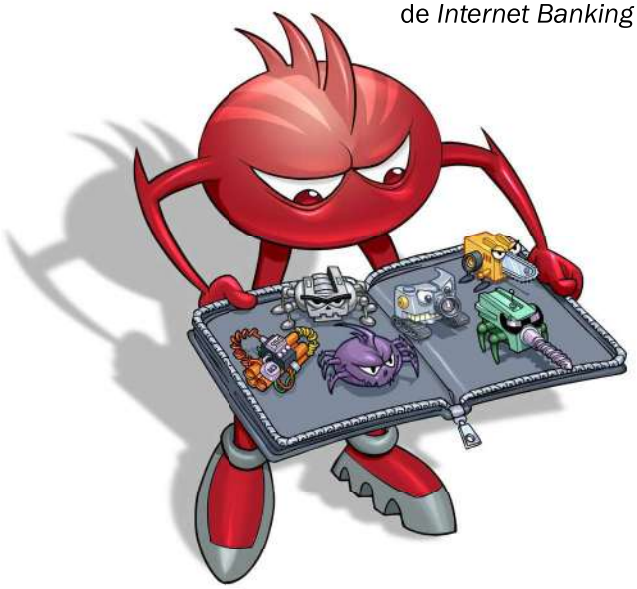
é um tipo de *spyware* capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do equipamento

SCREENLOGGER

é um tipo de *spyware*, similar ao *keylogger*, usado por atacantes para capturar as teclas digitadas pelos usuários em teclados virtuais, disponíveis principalmente em *sites* de *Internet Banking*

ADWARE

é um tipo de *spyware* projetado especificamente para apresentar propagandas



ROOTKIT

conjunto de programas e técnicas que permite esconder e assegurar a presença de um invasor ou de outro código malicioso em um equipamento comprometido

CUIDADOS A SEREM TOMADOS

MANTENHA SEUS EQUIPAMENTOS ATUALIZADOS

» Use apenas programas originais

» Tenha sempre as versões mais recentes dos programas instalados

» Instale todas as atualizações disponíveis, principalmente as de segurança

» Crie um disco de recuperação e tenha-o por perto no caso de emergências

INSTALE UM ANTIVÍRUS (*ANTIMALWARE*)

» Mantenha o antivírus atualizado, incluindo o arquivo de assinaturas

- atualize o arquivo de assinaturas pela rede, de preferência diariamente

» Configure o antivírus para verificar automaticamente toda e qualquer extensão de arquivo, arquivos anexados aos *e-mails*, obtidos pela Internet e os discos rígidos e as unidades removíveis

» Verifique sempre os arquivos recebidos, antes de abri-los ou executá-los

» Evite executar simultaneamente diferentes antivírus

- eles podem entrar em conflito, afetar o desempenho do equipamento e interferir na capacidade de detecção um do outro

» Crie um disco de emergência de seu antivírus

- use-o se desconfiar que o antivírus instalado está desabilitado/comprometido ou que o comportamento do equipamento está estranho

USE UM *FIREWALL* PESSOAL

» Assegure-se de ter um *firewall* pessoal instalado e ativo

» Verifique periodicamente os *logs* do *firewall* à procura de acessos maliciosos

AO INSTALAR APLICATIVOS

» Baixe aplicativos apenas de fontes confiáveis

» Verifique se as permissões de instalação e execução são coerentes

» Escolha aplicativos bem avaliados e com grande quantidade de usuários

FAÇA *BACKUPS*

» Proteja seus dados, fazendo *backups* regularmente

- Nunca recupere um *backup* se desconfiar que ele contenha dados não confiáveis
- Mantenha os *backups* desconectados do sistema

SEJA CUIDADOSO AO CLICAR EM *LINKS*

» Não considere que mensagens vindas de conhecidos são sempre confiáveis
  - o campo de remetente do *e-mail* pode ter sido falsificado, ou
  - elas podem ter sido enviadas de contas falsas ou invadidas

» Antes de acessar um *link* curto procure usar complementos que permitam visualizar o *link* de destino

OUTROS

» Use a conta de administrador apenas quando necessário

» Cuidado com extensões ocultas
  - alguns sistemas possuem como configuração padrão ocultar a extensão de tipos de arquivos conhecidos

» Desabilite a auto-execução de mídias removíveis e de arquivos anexados

SAIBA MAIS

» Para mais detalhes sobre este e outros assuntos relacionados com cuidados na Internet, consulte os demais Fascículos da Cartilha de Segurança e o Livro Segurança na Internet, disponíveis em: **cartilha.cert.br**

» Procurando material para conversar sobre segurança com diferentes públicos? O Portal Internet Segura apresenta uma série de materiais focados em crianças, adolescentes, pais, responsáveis e educadores, confira em: **internetsegura.br**

cert.br

O CERT.br é o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Desde 1997, o grupo é responsável por tratar incidentes de segurança envolvendo redes conectadas à Internet no Brasil. O Centro também desenvolve atividades de análise de tendências, treinamento e conscientização, com o objetivo de aumentar os níveis de segurança e de capacidade de tratamento de incidentes no Brasil. Mais informações em **www.cert.br.**

nic.br

O Núcleo de Informação e Coordenação do Ponto BR — NIC.br (**www.nic.br**) é uma entidade civil, de direito privado e sem fins de lucro, que além de implementar as decisões e projetos do Comitê Gestor da Internet no Brasil, tem entre suas atribuições: coordenar o registro de nomes de domínio — Registro.br (**www.registro.br**), estudar, responder e tratar incidentes de segurança no Brasil — CERT.br (**www.cert.br**), estudar e pesquisar tecnologias de redes e operações — Ceptro.br (**www.ceptro.br**), produzir indicadores sobre as tecnologias da informação e da comunicação — Cetic.br (**www.cetic.br**), implementar e operar os Pontos de Troca de Tráfego — IX.br (**www.ix.br**), viabilizar a participação da comunidade brasileira no desenvolvimento global da Web e subsidiar a formulação de políticas públicas — Ceweb.br (**www.ceweb.br**), e abrigar o escritório do W3C no Brasil (**www.w3c.br**).

cgi.br

O Comitê Gestor da Internet no Brasil, responsável por estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil, coordena e integra todas as iniciativas de serviços Internet no País, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados. Com base nos princípios do multissetorialismo e transparência, o CGI.br representa um modelo de governança da Internet democrático, elogiado internacionalmente, em que todos os setores da sociedade são partícipes de forma equânime de suas decisões. Uma de suas formulações são os 10 Princípios para a Governança e Uso da Internet (**www.cgi.br/principios**). Mais informações em **www.cgi.br**.

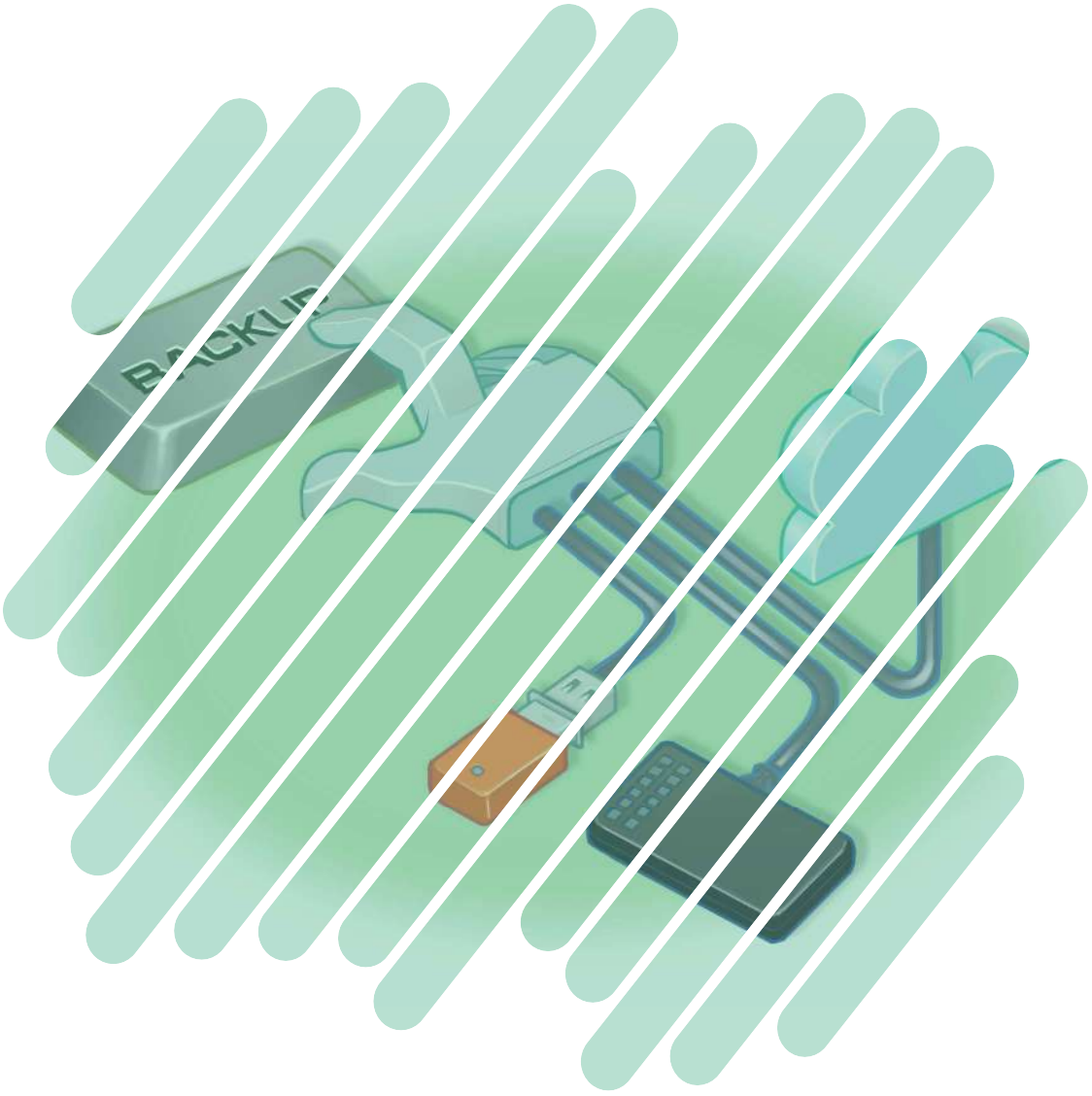
cartilha.cert.br/cc

outubro / 2020

Cartilha de Segurança para Internet

FASCÍCULO

BACKUP



Apoio de Divulgação:

UFPE

STI SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

Produção:

cert.br nic.br cgi.br

VOCÊ JÁ IMAGINOU O QUE ACONTECERIA SE, DE UMA HORA PARA OUTRA, PERDESSE ALGUNS OU ATÉ MESMO TODOS OS ARQUIVOS ARMAZENADOS NOS SEUS EQUIPAMENTOS?

Você já parou para pensar no valor dos seus arquivos? Qual é a importância deles para você? Não é nada fácil responder essas questões pois, com o passar do tempo, acumulamos tantos vídeos, imagens, músicas, documentos, *e-mails* e mensagens que já nem nos lembramos de todos eles. Geralmente, só quando o pior acontece e já é tarde demais para recuperar nossos arquivos, é que percebemos o quanto eles são essenciais para nós.

Para evitar perder seus dados é preciso que você mantenha seus equipamentos seguros e adote uma postura preventiva, o que inclui, entre outras coisas, fazer cópias de segurança dos seus arquivos, ou seja, realizar ***backups***.

O *backup* permite que você:

- recupere seus arquivos em situações inesperadas, como acidentes e infecção por códigos maliciosos
- recupere versões antigas, como a versão original de um arquivo que você alterou ou de uma imagem que você manipulou
- arquive aquilo que você deseja ou que precisa guardar, mas que não é necessário no seu dia a dia e que raramente é alterado.

Para fazer *backups* que garantam a segurança dos seus arquivos e que sejam adequados às suas necessidades, é importante que você conheça as opções existentes e tente responder algumas questões, como:

- quantas cópias devo fazer?
- quais arquivos devo copiar?
- onde os arquivos devem ser copiados?
- qual opção melhor me atende?

Não existem respostas certas, já que elas dependem dos recursos disponíveis, da quantidade de arquivos e da importância dos dados para cada um.

A seguir apresentamos algumas dicas para tentar ajudá-lo a criar uma solução que melhor se adapte às suas necessidades.

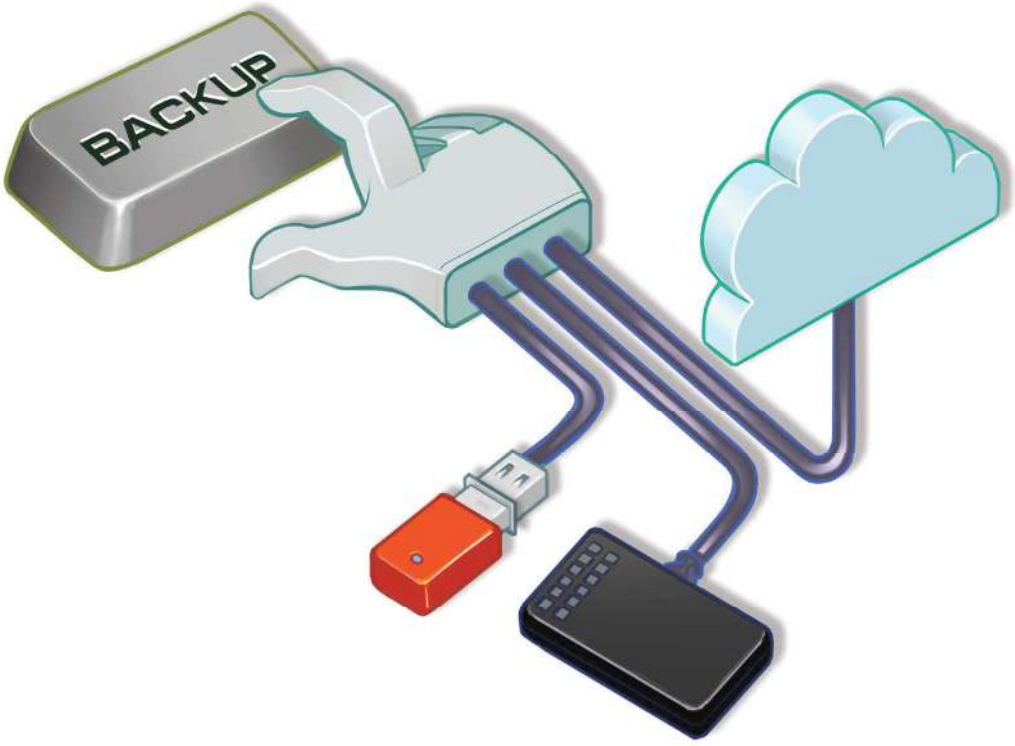
Lembre-se: Não precisa ser nada complicado, o importante é fazer *backups*.

FAÇA *BACKUP*: PROTEJA SEUS ARQUIVOS

COMO OS ARQUIVOS PODEM SER PERDIDOS

Infelizmente há situacões em que seus arquivos podem ser perdidos, tais como:

- Seus arquivos serem acidentalmente apagados
- Seus equipamentos serem perdidos, furtados ou roubados
- Seus equipamentos serem danificados de forma irrecuperável (por exemplo, por umidade ou queda)
- Seus equipamentos apresentarem mau funcionamento (por exemplo, uma falha no disco)
- Seus equipamentos serem invadidos e seus arquivos apagados
- Algum aplicativo apresentar mau funcionamento
- Uma atualização de sistema malsucedida obrigá-lo a reinstalar seus equipamentos
- O servidor em que seus arquivos estão armazenados apresentar problemas
- Algum código malicioso infectar seus equipamentos e apagar ou cifrar todos os seus arquivos
- Alguém descobrir a senha da conta do seu repositório de arquivos, acessá-la e apagar todos seus arquivos
- Alguém descobrir a senha da sua conta de *e-mail*, acessá-la e remover todas as suas mensagens



COMO FAZER *BACKUPS*?

Para fazer *backups* você pode usar programas integrados ao sistema operacional, aplicativos específicos, ferramentas desenvolvidas internamente ou, ainda soluções simples, como andar com um *pen drive* na mochila e enviar uma cópia para seu *e-mail* ou repositório externo de arquivos. Às vezes, basta pesquisar na Internet ou recorrer à "Central Ajuda" ou ao "*Help*" do sistema que você usa para descobrir as soluções disponíveis.

» Programe seus *backups* para serem feitos automaticamente, já que cópias manuais estão mais propensas a erros e esquecimentos

» Certifique-se de que realmente os seus *backups* estão sendo feitos, não confie somente no "automático"

» Você pode fazer *backups*:

- em mídias, como *pen drives,* discos rígidos, CDs, DVDs e discos de *Blu-ray*
- *online,* usando serviços na nuvem (*cloud*), em *datacenter* ou na rede

» A escolha de como fazer depende do tipo do seu equipamento, do aplicativo que será usado e de questões como conectividade, capacidade de armazenamento, custo e confiabilidade. Por exemplo:

- *backups* na nuvem podem ser muito práticos, mas dependem de conectividade e podem consumir muita banda de rede
- *backups* em rede podem ser simples, mas, geralmente, dependem do equipamento estar fisicamente conectado a uma rede específica, o que pode ser difícil em caso de ausências prolongadas
- CDs podem bastar para pequenas quantidades de dados, mas, atualmente, é cada vez mais difícil encontrar gravadores e leitores deste tipo de mídia
- *pen drives* oferecem portabilidade, podem ser indicados para arquivos constantemente modificados e ajudam a liberar espaço nos dispositivos (há modelos especiais para celulares e *tablets* que possuem

aplicativos de gerenciamento de arquivos que permitem fazer *backup*) mas podem ser facilmente perdidos

- discos rígidos podem ser usados para grandes volumes de dados, mas podem apresentar falhas

» Cuidados ao fazer *backups* em mídias:

- tenha cuidado para não perder seus *pen drives*
- proteja as mídias com senhas, sempre que for possível
- criptografe seus *backups* para evitar que alguém consiga acessá-los em caso de perda
  - você pode gravar os arquivos já criptografados ou criptografar a mídia de forma que, para acessá-la, será necessário o fornecimento de senha
- cuidado ao descartar as mídias, pois, se os arquivos não estiverem criptografados, alguém pode tentar acessá-los, expondo a sua privacidade e a confidencialidade das informações
- mantenha as mídias em locais seguros, à prova de fogo, bem acondicionados (longe de poeira, calor ou umidade) e com acesso restrito (apenas de pessoas autorizadas)
- mantenha as mídias etiquetadas e nomeadas, com informações que facilitem a localização e especificando o tipo do arquivo armazenado e a data de gravação
- cuidado com mídias obsoletas, pois com o tempo torna-se cada vez mais difícil encontrar leitores e elas possuem tempo de vida útil limitado

» Cuidados ao fazer *backups online*:

- ao usar recursos compartilhados, como discos em rede, lembre-se de fazer uso consciente, copiando apenas o que for necessário, pois outras pessoas também usarão o mesmo espaço
  - sistemas de cotas ajudam a controlar o uso, mas é necessário que o tamanho da área seja de acordo com a necessidade. Afinal, o que custa mais? Os dados ou a compra de discos maiores ou de mais discos?
- se tiver dispositivos móveis, lembre-se de fazer *backups* sempre que eles ficarem longos períodos desconectados da rede (viagens a trabalho, férias, etc.)

NÃO CONFUNDA

Os serviços de *backup* na nuvem fazem cópia dos arquivos na nuvem. Os sistemas de armazenamento na nuvem gravam os arquivos na nuvem, mas não necessariamente fazem *backup* (apesar de poderem ser usados para tal).

CUIDADOS AO ESCOLHER SERVIÇOS DE *BACKUP* NA NUVEM

Antes de escolher um serviço de *backup* na nuvem você deve observar alguns pontos, como por exemplo:

» Autenticação
- acesso ao sistema (se oferece opção de conexão segura, como https)
- métodos oferecidos (sempre use a verificação em duas etapas)

» Realização
- sistemas operacionais suportados
- possibilidade de automatização
- restrições quanto ao tamanho e tipo de arquivos
- tempo estimado de transmissão de dados (*upload*)
- forma como os dados trafegam pela rede (protegidos por criptografia)

» Armazenagem
- custo
- espaço de armazenagem oferecido (limitado ou ilimitado)
- forma como os dados são armazenados (protegidos por criptografia)
- políticas de privacidade e de segurança

» Restauração
- procedimento (por meio de aplicativos ou interface *web*)
- capacidade de transmissão de dados (*download*)
- tempo para restauração (imediatamente, um dia, uma semana)

» Retenção
- tempo que os dados são mantidos
- procedimento quando não ocorre o pagamento

» Reputação
- disponibilidade do serviço (quantidade de interrupções)
- suporte oferecido
- tempo no mercado
- opinião dos demais usuários
- outras referências

ONDE GUARDAR OS *BACKUPS*?

Você pode guardar seus *backups* localmente (no mesmo local dos arquivos originais) ou remotamente (*off-site*).

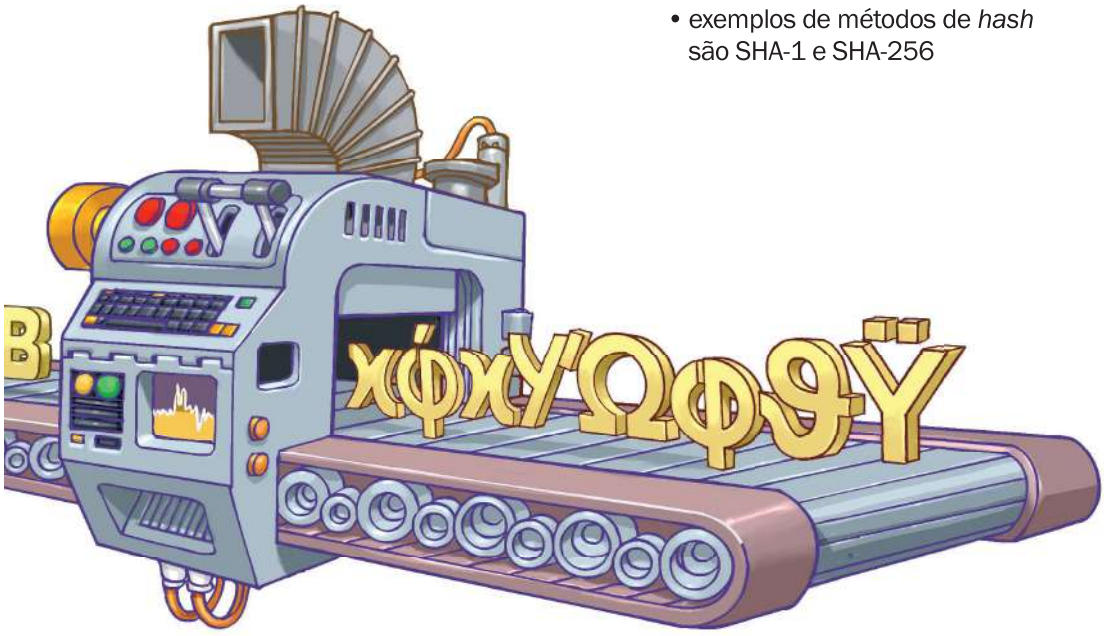
» Armazenamento local
- a recuperação é mais rápida já que os arquivos estão próximos
- não protege em caso de acidentes naturais (como incêndio e inundações), pois tanto a cópia como os originais podem ser perdidos

» Armazenamento remoto
  - garante a disponibilidade em caso de problemas no local onde estão os arquivos originais
  - a recuperação pode ser mais demorada, pois depende da velocidade da rede ou da distância do local onde as mídias estão armazenadas
  - pode comprometer a confidencialidade e integridade dos dados, caso não estejam criptografados, pois o acesso às mídias é mais difícil de ser controlado

» Siga a regra “3 - 2 - 1”, que consiste em:
  - ter pelo menos 3 cópias dos dados (a original e 2 *backups*)
  - armazenar as cópias em 2 tipos diferentes de mídias
  - manter ao menos 1 das cópias remota (ou ao menos *off-line*)

» Cópias *off-line* são aquelas que estão desconectadas do sistema principal quando não estão sendo usadas. Pode ser um *pen drive* que só é colocado no momento da cópia ou até um serviço de nuvem que apenas é conectado quando necessário

» Para tentar detectar alterações indevidas em uma mídia, gere os *hashes*[1] dos arquivos antes de enviá-la para locais remotos e gere-os novamente antes de restaurá-los
  - se os dois *hashes* forem iguais então você pode concluir que o arquivo não foi alterado
  - caso contrário, este pode ser um forte indício de que o arquivo esteja corrompido ou que foi modificado
  - exemplos de métodos de *hash* são SHA-1 e SHA-256



[1] *Hash* é o resultado único e de tamanho fixo gerado quando uma função de resumo (tipo de método criptográfico) é aplicada sobre uma informação.

O QUE COPIAR?

Apenas arquivos: Geralmente é o mais comum, já que pode ser feito diariamente, ocupa menos espaço e a recuperação é mais fácil.

» Copie apenas os arquivos confiáveis e importantes

» Evite copiar arquivos do sistema ou de aplicativos, pois eles podem ser facilmente reinstalados posteriormente

Tudo (imagem do sistema): Incluindo sistema operacional, programas instalados, configurações e arquivos. Facilita a substituição de equipamentos, mas não é indicada para proteger arquivos constantemente alterados, já que ocupa muito espaço e a restauração é mais complexa.

» Faça uma imagem do sistema quando for substituir seus equipamentos ou fazer alterações que possam comprometê-los

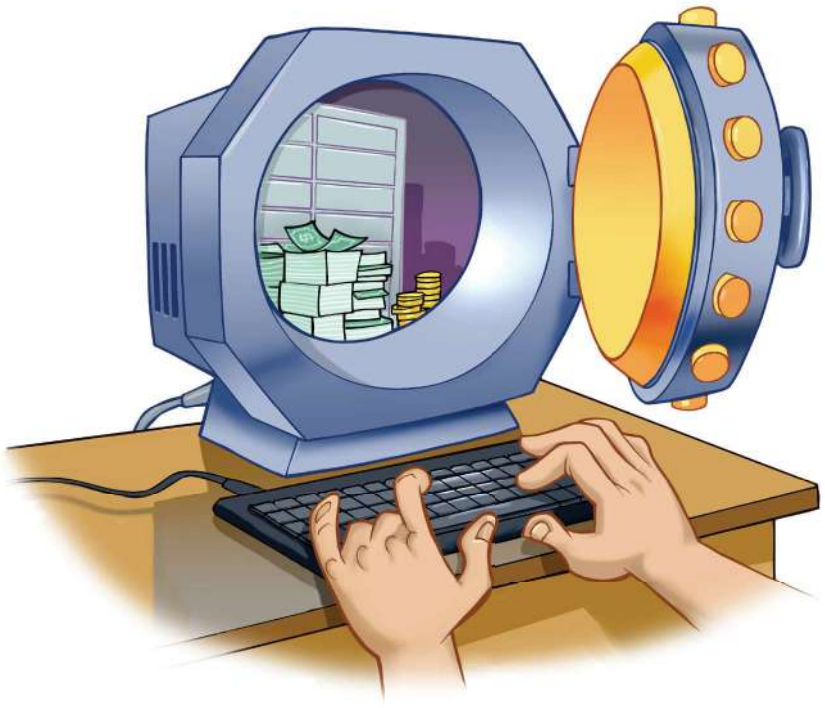
QUANDO COPIAR?

» Mantenha seus *backups* atualizados, fazendo cópias periódicas, de acordo com a frequência com que você cria ou modifica seus arquivos

- arquivos frequentemente modificados devem ser copiados diariamente
- arquivos pouco alterados podem ser copiados semanalmente ou mensalmente

» Para determinar a frequência adequada tente se perguntar "quantos dados estou disposto a perder?"

- fazer *backups* pode ser trabalhoso e custoso, por isso é importante encontrar um



equilíbrio entre copiar demais e perder dados

- Faça cópias sempre que houver indícios de risco iminente, como mau funcionamento, alerta de falhas, atualização de sistemas, envio a serviços de manutenção, grandes alterações no sistema e adição de *hardware*, etc.

Para tentar otimizar as cópias você pode escolher entre os diferentes tipos de *backups*:

- ***Backup* completo, total ou *full*:** Copia todos os arquivos
- ***Backup* incremental:** Copia apenas os arquivos alterados ou criados após o último *backup* completo, incremental ou diferencial
- ***Backup* diferencial:** Copia os arquivos alterados ou criados após o último *backup* completo (diferente do incremental que se baseia no último *backup*, independente do tipo)

Uma politica de proteção bastante comum é fazer um *backup* completo pelo menos uma vez por semana e nos demais dias fazer *backups* incrementais.

COMO RECUPERAR OS ARQUIVOS?

A recuperação de um *backup* pode ser parcial (quando um ou mais arquivos são recuperados) ou total (quando todos arquivos são recuperados).

- Nunca recupere um *backup* se desconfiar que ele contém dados não confiáveis
- Para recuperar totalmente (do zero) um equipameno você pode usar uma imagem do sistema previamente feita
- Se precisar recuperar um sistema invadido, isole-o da rede, revise a configuração e certifique-se de que não tenha ficado alguma porta de entrada incluída pelo invasor

COMO SABER SE O *BACKUP* ESTÁ FUNCIONANDO?

Testes evitam surpresas, como dados corrompidos, mídia ou formato obsoleto, programas mal configurados ou falta do programa de recuperação. Não deixe para perceber falhas quando já for tarde demais.

- Teste seus *backups* periodicamente e logo após eles terem sido gerados

POR QUANTO TEMPO DEVE-SE MANTER OS *BACKUPS*?

O tempo de retenção dos *backups* depende do tipo de cada arquivo que foi copiado. Suas fotos e seus vídeos, provavelmente, você vai querer guardar para sempre, pois possuem valor emocional. Seus trabalhos de escola, talvez, você queira se desfazer após um tempo, pois o conteúdo vai ficando ultrapassado.

- Mantenha seus *backups* pelo tempo que os arquivos tiverem valor ou utilidade para você ou enquanto não tiver problemas de espaço
- Lembre-se de identificar seus *backups* com informações que ajudem a localizar o tipo do arquivo armazenado e a data de gravação, pois isso ajuda a selecionar o que será apagado em caso de necessidade

CUIDADOS COM *RANSOMWARE*

O *ransomware* é um tipo de código malicioso que torna inacessíveis os dados armazenados em um equipamento, geralmente usando criptografia, e que exige pagamento de resgate (*ransom*) para restabelecer o acesso ao usuário.

» As formas mais comuns de propagação de *ransomware* são:

- 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

» Além de cifrar os arquivos, o *ransomware* também costuma:

- cifrar *backups* na nuvem
- procurar por arquivos com extensões típicas de *backup*, como .bak, .zip, .gz e .rar
- buscar por outros equipamentos conectados, locais ou em rede, e criptografá-los também

Se seu equipamento for infectado por *ransomware* a única garantia de que você conseguirá acessar novamente seus arquivos é possuir *backups* atualizados. O pagamento do resgate não garante que o acesso será restabelecido e ainda pode incentivar o crime e levar a novos pedidos de extorsão. Por isso é importante que você proteja seus *backups*:

» Mantenha os *backups* desconectados dos seus equipamentos

» Desabilite o compartilhamento de arquivos, se ele não for necessário

» Escolha serviços de nuvem que ofereçam proteção *anti-ransomware* e habilite a verificação em duas etapas, sempre que possível

PROTEJA SEUS EQUIPAMENTOS

Lembre-se: O *backup* é a última linha de defesa para proteção dos seus arquivos, aquela que só deverá ser usada quando todas as demais falharem. Por isso é importante que você tome alguns cuidados para proteger seus arquivos e equipamentos.

» Mantenha seus equipamentos seguros

- instale a versão mais nova do sistema operacional e dos aplicativos usados
- aplique todas as atualizações e não se esqueça de reiniciar o equipamento sempre que solicitado
- desabilite os serviços desnecessários
- instale mecanismos de segurança, como antivírus, *anti-ransomware* e *firewall* pessoal, e mantenha-os atualizados

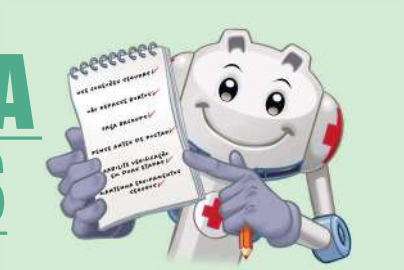
» Proteja suas contas de acesso

- crie senhas bem elaboradas
- não reutilize suas senhas
- ative a verificação em duas etapas

» Adote uma postura preventiva

- seja cuidadoso ao abrir arquivos anexos e ao clicar em *links*
- não repasse correntes e nem mensagens contendo ofertas e promoções, pois elas podem conter *links* para *sites* falsos (*phishing*) ou instalar códigos maliciosos
- seja cuidadoso ao clicar em *links*, independente de quem os enviou
- não considere que mensagens vindas de conhecidos são sempre confiáveis, pois quem enviou pode não ter verificado o conteúdo, o campo de remetente pode ter sido falsificado e elas podem ter sido enviadas de contas falsas ou invadidas

SAIBA MAIS



» Para mais detalhes sobre este e outros assuntos relacionados com cuidados na Internet, consulte os demais Fascículos da Cartilha de Segurança e o Livro Segurança na Internet, disponíveis em: **cartilha.cert.br**

» Procurando material para conversar sobre segurança com diferentes públicos? O Portal Internet Segura apresenta uma série de materiais focados em crianças, adolescentes, pais, responsáveis e educadores, confira em: **internetsegura.br**

cert.br

O CERT.br é o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Desde 1997, o grupo é responsável por tratar incidentes de segurança envolvendo redes conectadas à Internet no Brasil. O Centro também desenvolve atividades de análise de tendências, treinamento e conscientização, com o objetivo de aumentar os níveis de segurança e de capacidade de tratamento de incidentes no Brasil. Mais informações em **www.cert.br.**

nic.br

O Núcleo de Informação e Coordenação do Ponto BR — NIC.br (**www.nic.br**) é uma entidade civil, de direito privado e sem fins de lucro, que além de implementar as decisões e projetos do Comitê Gestor da Internet no Brasil, tem entre suas atribuições: coordenar o registro de nomes de domínio — Registro.br (**www.registro.br**), estudar, responder e tratar incidentes de segurança no Brasil — CERT.br (**www.cert.br**), estudar e pesquisar tecnologias de redes e operações — Ceptro.br (**www.ceptro.br**), produzir indicadores sobre as tecnologias da informação e da comunicação — Cetic.br (**www.cetic.br**), implementar e operar os Pontos de Troca de Tráfego — IX.br (**www.ix.br**), viabilizar a participação da comunidade brasileira no desenvolvimento global da Web e subsidiar a formulação de políticas públicas — Ceweb.br (**www.ceweb.br**), e abrigar o escritório do W3C no Brasil (**www.w3c.br**).

cgi.br

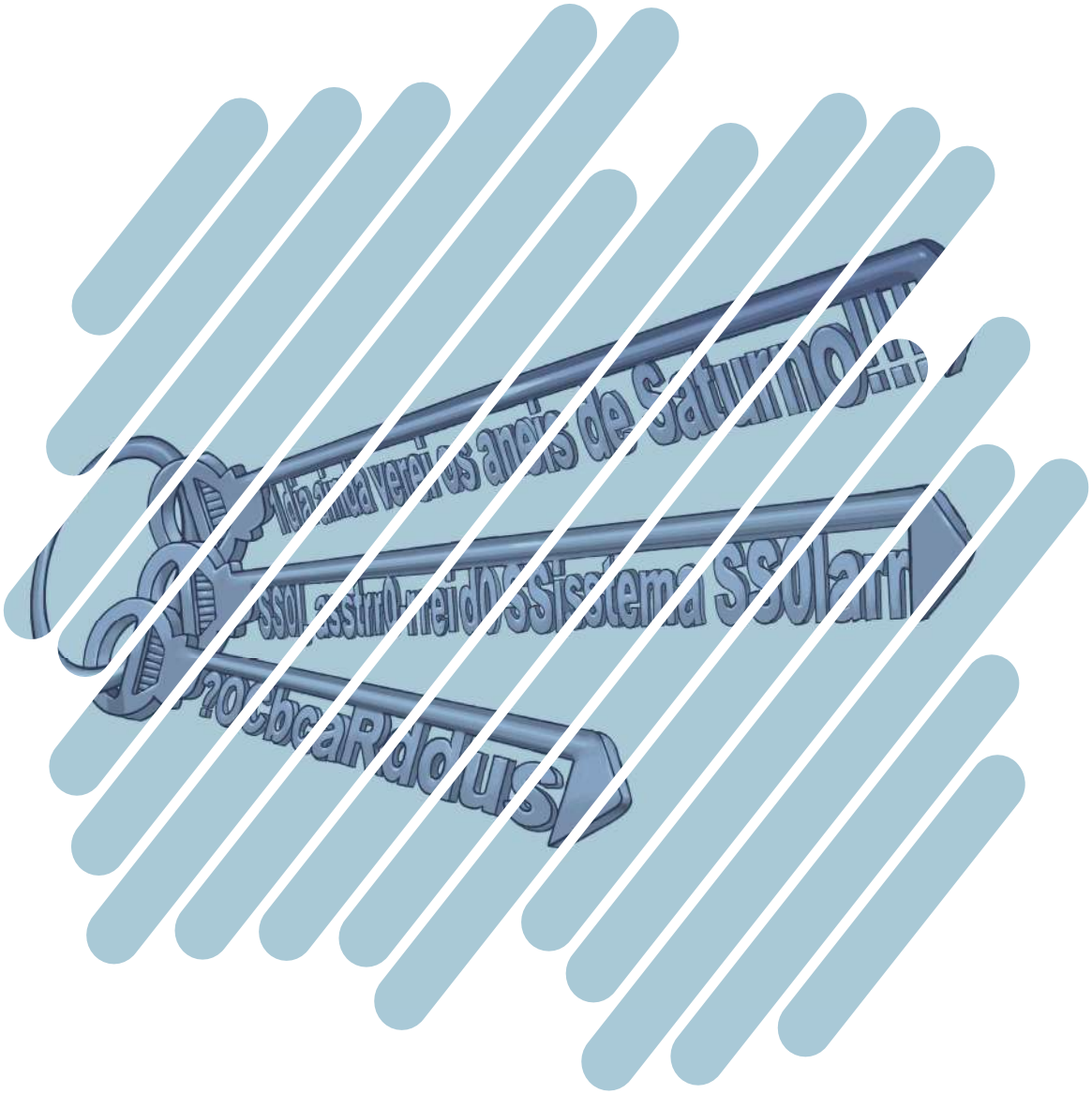
O Comitê Gestor da Internet no Brasil, responsável por estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil, coordena e integra todas as iniciativas de serviços Internet no País, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados. Com base nos princípios do multissetorialismo e transparência, o CGI.br representa um modelo de governança da Internet democrático, elogiado internacionalmente, em que todos os setores da sociedade são partícipes de forma equânime de suas decisões. Uma de suas formulações são os 10 Princípios para a Governança e Uso da Internet (**www.cgi.br/principios**). Mais informações em **www.cgi.br**.

outubro / 2020

Cartilha de Segurança para Internet

FASCÍCULO

SENHAS



Apoio de Divulgação:

UFPE

STI SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

Produção:

cert.br nic.br cgi.br

CONTAS E SENHAS SÃO OS MECANISMOS DE AUTENTICAÇÃO MAIS UTILIZADOS NA INTERNET ATUALMENTE

Por meio de contas e senhas os sistemas conseguem saber quem você é, confirmar sua identidade e definir as ações que você pode realizar.

A sua conta de usuário em um determinado sistema normalmente é de conhecimento público, já que é por meio dela que as pessoas e serviços conseguem identificar quem você é. Desta forma, **proteger sua senha é essencial** para se prevenir dos riscos envolvidos no uso da Internet, pois **é o segredo dela que garante a sua identidade**, ou seja, que você é o dono da sua conta de usuário.

Se uma outra pessoa souber a sua conta de usuário e tiver acesso à sua senha, ela poderá usá-las para se passar por você na Internet e realizar ações em seu nome. Algumas das formas como sua senha pode ser indevidamente descoberta são:

- quando usada em computadores infectados
- quando usada em computadores invadidos
- quando usada em *sites* falsos (*phishing*)
- por meio de tentativas de adivinhação
- ao ser capturada enquanto trafega na rede
- por meio do acesso ao arquivo onde foi armazenada
- com o uso de técnicas de engenharia social
- pela observação da movimentação dos seus dedos no teclado ou dos cliques do *mouse* em teclados virtuais.

PRESERVE SUAS SENHAS: PROTEJA SUA IDENTIDADE

RISCOS PRINCIPAIS

Proteger suas senhas é fundamental para se prevenir dos riscos que o uso da Internet pode representar. Algumas das ações que um invasor pode realizar, caso tenha acesso às suas senhas, e os riscos que estas ações podem representar são:

» Acessar a sua conta de correio eletrônico e:
- ler e/ou apagar seus *e-mails*
- furtar sua lista de contatos e enviar *e-mails* em seu nome
- enviar mensagens de *spam* e/ou contendo *phishing* e códigos maliciosos
- pedir o reenvio de senhas de outras contas (e assim conseguir acesso a elas)
- trocar sua senha, dificultando que você acesse novamente sua conta

» Acessar o seu computador e:
- apagar seus arquivos e obter informações sensíveis, inclusive outras senhas
- instalar códigos e serviços maliciosos
- usá-lo para desferir ataques contra outros computadores

» Acessar redes sociais e:
- denegrir a sua imagem e explorar a confiança de seus amigos/seguidores
- enviar mensagens de *spam* ou contendo boatos e códigos maliciosos
- alterar as configurações feitas por você, tornando públicas informações privadas
- trocar sua senha, dificultando que você acesse novamente sua conta

» Acessar sua conta bancária e:
- verificar seu extrato e seu saldo bancário

» Acessar seu *site* de comércio eletrônico e:
- alterar informações de cadastro
- fazer compras em seu nome e verificar informações sobre suas compras anteriores

CUIDADOS A SEREM TOMADOS

SEJA CUIDADOSO AO ELABORAR SUAS SENHAS

» Evite usar:

- dados pessoais, como nomes, sobrenomes, contas de usuário, datas, números de documentos, placas de carros e números de telefones
- dados que possam ser obtidos em redes sociais e páginas *web*
- sequências de teclado, como “1qaz2wsx” e “QwerTAsdfG”
- palavras que fazem parte de listas publicamente conhecidas, como nomes de músicas, times de futebol, personagens de filmes e dicionários de diferentes idiomas

» Use:

- números aleatórios
- grande quantidade de caracteres
- diferentes tipos de caracteres

DICAS PRÁTICAS PARA ELABORAR BOAS SENHAS

» Escolha uma frase e selecione a primeira, a segunda ou a última letra de cada palavra: com a frase “O Cravo brigou com a Rosa debaixo de uma sacada” você pode gerar a senha “?OCbcaRddus”

» Escolha uma frase longa, que seja fácil de ser memorizada e que, se possível, tenha diferentes tipos de caracteres: se quando criança você sonhava em ser astronauta, pode usar como senha “1 dia ainda verei os aneis de Saturno!!!”

» Invente um padrão de substituição baseado, por exemplo, na semelhança visual ou de fonética entre os caracteres: duplicando as letras “s” e “r”, substituindo “o” por “0” (número zero) e usando a frase “Sol, astro-rei do Sistema Solar” você pode gerar a senha “SS0l, asstrr0-rrei d0 SSisstema SS0larr”

SEJA CUIDADOSO AO USAR SUAS SENHAS

» Não exponha suas senhas
  - certifique-se de não estar sendo observado ao digitá-las
  - não as deixe anotadas em locais onde outras pessoas possam vê-las (por exemplo, em um papel colado no monitor do seu computador)
  - evite digitá-las em computadores e dispositivos móveis de terceiros

» Não forneça as suas senhas para outra pessoa, em hipótese alguma
  - fique atento a ligações telefônicas e *e-mails* pelos quais alguém, geralmente falando em nome de alguma instituição, solicita informações pessoais sobre você, inclusive senhas

» Certifique-se de usar conexões seguras sempre que o acesso envolver senhas

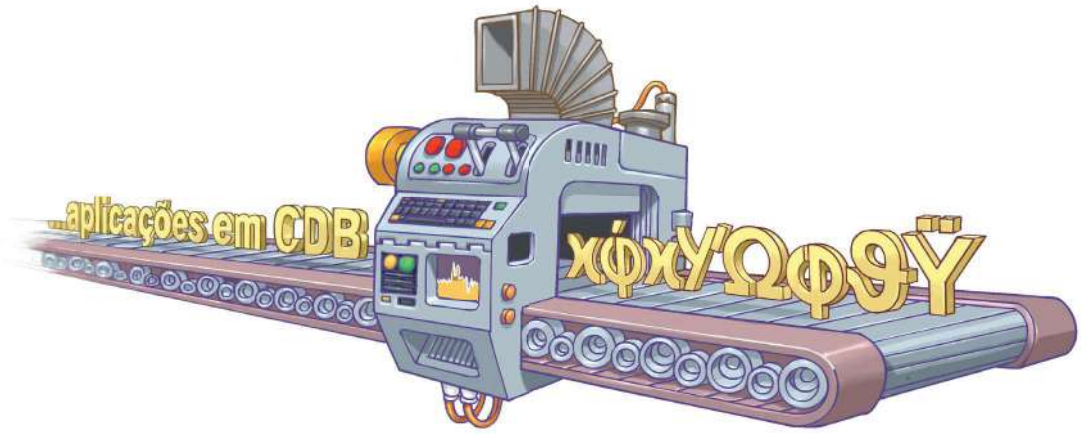
» Evite salvar as suas senhas no navegador *web*

» Evite usar opções como "Lembre-se de mim" e "Continuar conectado"

» Evite usar a mesma senha para todos os serviços que você acessa
  - basta ao atacante conseguir uma senha para ser capaz de acessar as demais contas onde ela seja usada

» Crie grupos de senhas, de acordo com o risco envolvido
  - crie senhas únicas, bastante fortes, e use-as onde haja recursos valiosos envolvidos
  - crie senhas únicas, um pouco mais simples, e use-as onde o valor dos recursos protegidos é inferior
  - crie senhas simples e reutilize-as para acessos sem risco
  - não use senhas de acesso a assuntos pessoais para acessar assuntos profissionais, e vice-versa (respeite os contextos)

» Armazene suas senhas de forma segura. Por exemplo:
  - anote suas senhas em um papel e guarde-o em local seguro
  - grave suas senhas em um arquivo criptografado
  - use programas gerenciadores de contas/senhas



ALTERE SUAS SENHAS

» Imediatamente:

- se desconfiar que elas tenham sido descobertas ou que o computador no qual você as usou tenha sido invadido ou infectado

» Rapidamente:

- se alguém furtar ou você perder um computador onde elas estejam gravadas
- se usar um padrão para a formação de senhas e desconfiar que uma delas tenha sido descoberta (altere também o padrão e as demais senhas elaboradas com ele)
- se usar uma mesma senha em mais de um lugar e desconfiar que ela tenha sido descoberta em algum deles (altere-a em todos os lugares nos quais é usada)
- ao adquirir equipamentos acessíveis via rede, como roteadores Wi-Fi e *modems* ADSL (eles podem estar configurados com senha padrão, facilmente obtida na Internet)

» Regularmente:

- nos demais casos

SEJA CUIDADOSO AO USAR MECANISMOS DE RECUPERAÇÃO

» Certifique-se de configurar opções de recuperação de senha, como um endereço de *e-mail* alternativo, uma pergunta de segurança e um número de telefone celular

» Ao usar perguntas de segurança evite escolher questões cujas respostas possam ser facilmente adivinhadas (crie suas próprias questões com respostas falsas)

» 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 possa entendê-las

» Ao solicitar o envio de suas senhas por *e-mail* altere-as o mais rápido possível e certifique-se de cadastrar um *e-mail* de recuperação que você acesse regularmente (para não esquecer a senha desta conta também)

PROTEJA-SE DE *PHISHING* E CÓDIGOS MALICIOSOS

» Desconfie de mensagens recebidas, mesmo que enviadas por conhecidos

» Evite seguir *links* recebidos em mensagens eletrônicas

» Não utilize um *site* 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 que você expanda o *link* antes de clicar sobre ele

PRESERVE A SUA PRIVACIDADE

- Procure reduzir a quantidade de informações que possam ser coletadas sobre você, pois elas podem ser usadas para adivinhar as suas senhas
- Seja cuidadoso com as informações que você disponibiliza em *blogs* e redes sociais (elas podem ser usadas por invasores para tentar confirmar os seus dados cadastrais, descobrir dicas e responder perguntas de segurança)

PROTEJA SEU COMPUTADOR

- Mantenha o seu computador seguro
  - com a versão mais recente de todos os programas instalados
  - com todas as atualizações aplicadas
- Utilize e mantenha atualizados mecanismos de segurança, como *antispam*, *antimalware* e *firewall* pessoal
- Configure seu computador para solicitar senha na tela inicial
- Ative o compartilhamento de recursos de seu computador apenas quando necessário e usando senhas bem elaboradas
- Nunca compartilhe a senha de administrador e use-a o mínimo necessário
- Crie contas individuais para todos aqueles que usam seu computador e assegure que todas elas tenham senha

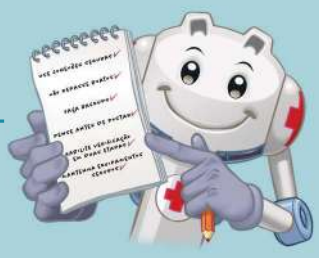
PROTEJA SEUS DISPOSITIVOS MÓVEIS

- Cadastre uma senha de acesso que seja bem elaborada e, se possível, configure-o para aceitar senhas complexas (alfanuméricas)
- Em caso de perda ou furto altere as senhas que possam estar nele armazenadas

SEJA CUIDADOSO AO USAR COMPUTADORES DE TERCEIROS

- Certifique-se de fechar a sua sessão (*logout*) ao acessar *sites* que usem senhas
- Procure, sempre que possível, utilizar opções de navegação anônima
- Evite efetuar transações bancárias e comerciais
- Ao retornar ao seu computador, procure alterar as senhas que você tenha usado

SAIBA MAIS



» Para mais detalhes sobre este e outros assuntos relacionados com cuidados na Internet, consulte os demais Fascículos da Cartilha de Segurança e o Livro Segurança na Internet, disponíveis em: **cartilha.cert.br**

» Procurando material para conversar sobre segurança com diferentes públicos? O Portal Internet Segura apresenta uma série de materiais focados em crianças, adolescentes, pais, responsáveis e educadores, confira em: **internetsegura.br**

cert.br

O CERT.br é o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Desde 1997, o grupo é responsável por tratar incidentes de segurança envolvendo redes conectadas à Internet no Brasil. O Centro também desenvolve atividades de análise de tendências, treinamento e conscientização, com o objetivo de aumentar os níveis de segurança e de capacidade de tratamento de incidentes no Brasil. Mais informações em **www.cert.br.**

nic.br

O Núcleo de Informação e Coordenação do Ponto BR — NIC.br (**www.nic.br**) é uma entidade civil, de direito privado e sem fins de lucro, que além de implementar as decisões e projetos do Comitê Gestor da Internet no Brasil, tem entre suas atribuições: coordenar o registro de nomes de domínio — Registro.br (**www.registro.br**), estudar, responder e tratar incidentes de segurança no Brasil — CERT.br (**www.cert.br**), estudar e pesquisar tecnologias de redes e operações — Ceptro.br (**www.ceptro.br**), produzir indicadores sobre as tecnologias da informação e da comunicação — Cetic.br (**www.cetic.br**), implementar e operar os Pontos de Troca de Tráfego — IX.br (**www.ix.br**), viabilizar a participação da comunidade brasileira no desenvolvimento global da Web e subsidiar a formulação de políticas públicas — Ceweb.br (**www.ceweb.br**), e abrigar o escritório do W3C no Brasil (**www.w3c.br**).

cgi.br

O Comitê Gestor da Internet no Brasil, responsável por estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil, coordena e integra todas as iniciativas de serviços Internet no País, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados. Com base nos princípios do multissetorialismo e transparência, o CGI.br representa um modelo de governança da Internet democrático, elogiado internacionalmente, em que todos os setores da sociedade são partícipes de forma equânime de suas decisões. Uma de suas formulações são os 10 Princípios para a Governança e Uso da Internet (**www.cgi.br/principios**). Mais informações em **www.cgi.br.**

outubro / 2020

Cartilha de Segurança para Internet

FASCÍCULO

DISPOSITIVOS MÓVEIS

Apoio de Divulgação:

UFPE

STI SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

Produção:

cert.br nic.br cgi.br

O USO DE *TABLETS*, *SMARTPHONES* E CELULARES ESTÁ CADA VEZ MAIS COMUM E INSERIDO EM NOSSO COTIDIANO

Caso tenha um dispositivo móvel (*tablet*, *smartphone*, celular, etc.) muito provavelmente você:

- costuma levá-lo aos locais que frequenta, como sua residência, trabalho, escola, restaurante, cinema, ônibus, metrô, etc.
- mantém informações pessoais nele armazenadas, como compromissos, lista de contatos, chamadas realizadas e mensagens recebidas
- mantém informações de trabalho nele armazenadas e/ou por meio dele acessa seu *e-mail* profissional
- procura por novidades tecnológicas, como novos recursos, aplicativos, modelos ou opções de uso
- procura estar conectado, seja para manter-se informado sobre o que está ocorrendo ou para publicar informações
- frequenta locais onde sempre tem alguém usando um dispositivo móvel, seja para tirar fotos, acessar *e-mails*, ler notícias ou comentar sobre o que está fazendo.

Se você apresenta um ou mais destes comportamentos, é importante estar ciente dos riscos que o uso de dispositivos móveis podem representar para que, assim, possa tomar os devidos cuidados.

DISPOSITIVOS MÓVEIS: MOBILIDADE COM SEGURANÇA

RISCOS PRINCIPAIS

Os dispositivos móveis, além de funcionalidades similares aos dos computadores pessoais, também apresentam os mesmos riscos. Além disso, possuem características que podem torná-los ainda mais atraentes para pessoas mal-intencionadas. Alguns destes riscos são:

» Vazamento de informações
- informações armazenadas nos aparelhos, como mensagens SMS, lista de contatos, calendários, histórico de chamadas, fotos, vídeos, senhas e números de cartão de crédito, podem ser indevidamente coletadas
- os aparelhos costumam ser rapidamente substituídos por novos modelos, sem que sejam tomados cuidados para excluir as informações gravadas

» Maior possibilidade de perda e furto
- em virtude do tamanho reduzido, do alto valor financeiro e do *status* que representam, além de estarem em uso constante, podem ser facilmente esquecidos, perdidos ou atrair a atenção de assaltantes

» Invasão de privacidade
- como estão sempre à mão alguém pode tirar uma foto sua e publicá-la, sem seu conhecimento ou permissão. Isso pode expor mais informações do que realmente você gostaria

» Instalação de aplicativos maliciosos
- dentre a grande infinidade de aplicativos disponíveis, podem existir alguns com erros de implementação, não confiáveis ou especificamente desenvolvidos para execução de atividades maliciosas

» Propagação de códigos maliciosos
- você pode receber mensagens contendo códigos maliciosos e, caso não seja cuidadoso, ter seus equipamentos infectados, seus dados coletados, participar de ataques na Internet e contribuir para a disseminação de *spam*

CUIDADOS A SEREM TOMADOS

ANTES DE ADQUIRIR UM DISPOSITIVO MÓVEL

» Observe os mecanismos de segurança disponibilizados pelos diferentes modelos e fabricantes
  - escolha aquele que considerar mais seguro

» Não adquira um dispositivo ilegalmente desbloqueado (*jailbreak*) ou cujas permissões de acesso tenham sido alteradas
  - além de ilegal, isso pode violar os termos de garantia e comprometer a segurança e o funcionamento do aparelho

» Restaure as configurações originais, ou "de fábrica", caso opte por um modelo usado

AO USAR SEU DISPOSITIVO MÓVEL

» Instale um programa antivírus, **antes de instalar qualquer tipo de aplicativo**

» Instale também outros mecanismos de segurança, como *antispam*, *antispyware* e *antimalware*

- não se esqueça de mantê-los atualizados

» Mantenha-o seguro

- com a versão mais recente de todos os programas instalados
- com todas as atualizações aplicadas

» Não siga *link*s recebidos por meio de mensagens eletrônicas (SMS, *e-mail*s, redes sociais, etc.)

- desconfie de mensagens recebidas, mesmo que enviadas por conhecidos

» Mantenha controle físico sobre o seu dispositivo

- principalmente quando estiver em locais considerados de risco
- procure não deixá-lo sobre a mesa e cuidado com bolsos/bolsas quando estiver em ambientes públicos

» Proteja suas senhas

- cadastre senhas de acesso bem elaboradas
- se possível, configure-o para aceitar senhas complexas (alfanuméricas)
- use senhas longas, compostas de diferentes tipos de caracteres
- não utilize:
  - sequências de teclado
  - dados pessoais, como nome, sobrenome e datas
  - dados que possam ser facilmente obtidos sobre você

» Proteja sua privacidade

- seja cuidadoso ao:
  - publicar sua geolocalização
  - permitir que aplicativos acessem seus dados pessoais

» Proteja seus dados

- configure:
  - uma senha de bloqueio na tela inicial
  - para que seja solicitado o código PIN
- faça *backup*s periódicos
- mantenha as informações sensíveis em formato criptografado
- use conexão segura sempre que a comunicação envolver dados confidenciais

AO INSTALAR APLICATIVOS

- Procure obter aplicativos de fontes confiáveis, como lojas oficiais ou o *site* do fabricante
- Escolha aqueles que tenham sido bem avaliados e com grande quantidade de usuários
- Verifique com seu programa antivírus antes de instalar um aplicativo
- Observe se as permissões para a execução são 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, como *bluetooth*, infravermelho e Wi-Fi, desativadas
  - somente as habilite quando necessário
- Configure a conexão *bluetooth* para que seu dispositivo não seja identificado (ou "descoberto") por outros aparelhos

AO SE DESFAZER DO SEU DISPOSITIVO MÓVEL

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

EM CASO DE PERDA OU FURTO

» 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 dele 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 com essa configuração: principalmente se você tiver filhos e eles gostarem de brincar com o seu dispositivo

» Informe sua operadora e solicite o bloqueio do seu número (*chip*)

» Informe 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 cujos números estejam nele armazenados

» Ative a localização remota, caso você a tenha configurado
- se achar necessário, apague remotamente todos os dados nele armazenados

SAIBA MAIS

» Para mais detalhes sobre este e outros assuntos relacionados com cuidados na Internet, consulte os demais Fascículos da Cartilha de Segurança e o Livro Segurança na Internet, disponíveis em: **cartilha.cert.br**

» Procurando material para conversar sobre segurança com diferentes públicos? O Portal Internet Segura apresenta uma série de materiais focados em crianças, adolescentes, pais, responsáveis e educadores, confira em: **internetsegura.br**

cert.br

O CERT.br é o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Desde 1997, o grupo é responsável por tratar incidentes de segurança envolvendo redes conectadas à Internet no Brasil. O Centro também desenvolve atividades de análise de tendências, treinamento e conscientização, com o objetivo de aumentar os níveis de segurança e de capacidade de tratamento de incidentes no Brasil. Mais informações em **www.cert.br.**

nic.br

O Núcleo de Informação e Coordenação do Ponto BR — NIC.br (**www.nic.br**) é uma entidade civil, de direito privado e sem fins de lucro, que além de implementar as decisões e projetos do Comitê Gestor da Internet no Brasil, tem entre suas atribuições: coordenar o registro de nomes de domínio — Registro.br (**www.registro.br**), estudar, responder e tratar incidentes de segurança no Brasil — CERT.br (**www.cert.br**), estudar e pesquisar tecnologias de redes e operações — Ceptro.br (**www.ceptro.br**), produzir indicadores sobre as tecnologias da informação e da comunicação — Cetic.br (**www.cetic.br**), implementar e operar os Pontos de Troca de Tráfego — IX.br (**www.ix.br**), viabilizar a participação da comunidade brasileira no desenvolvimento global da Web e subsidiar a formulação de políticas públicas — Ceweb.br (**www.ceweb.br**), e abrigar o escritório do W3C no Brasil (**www.w3c.br**).

cgi.br

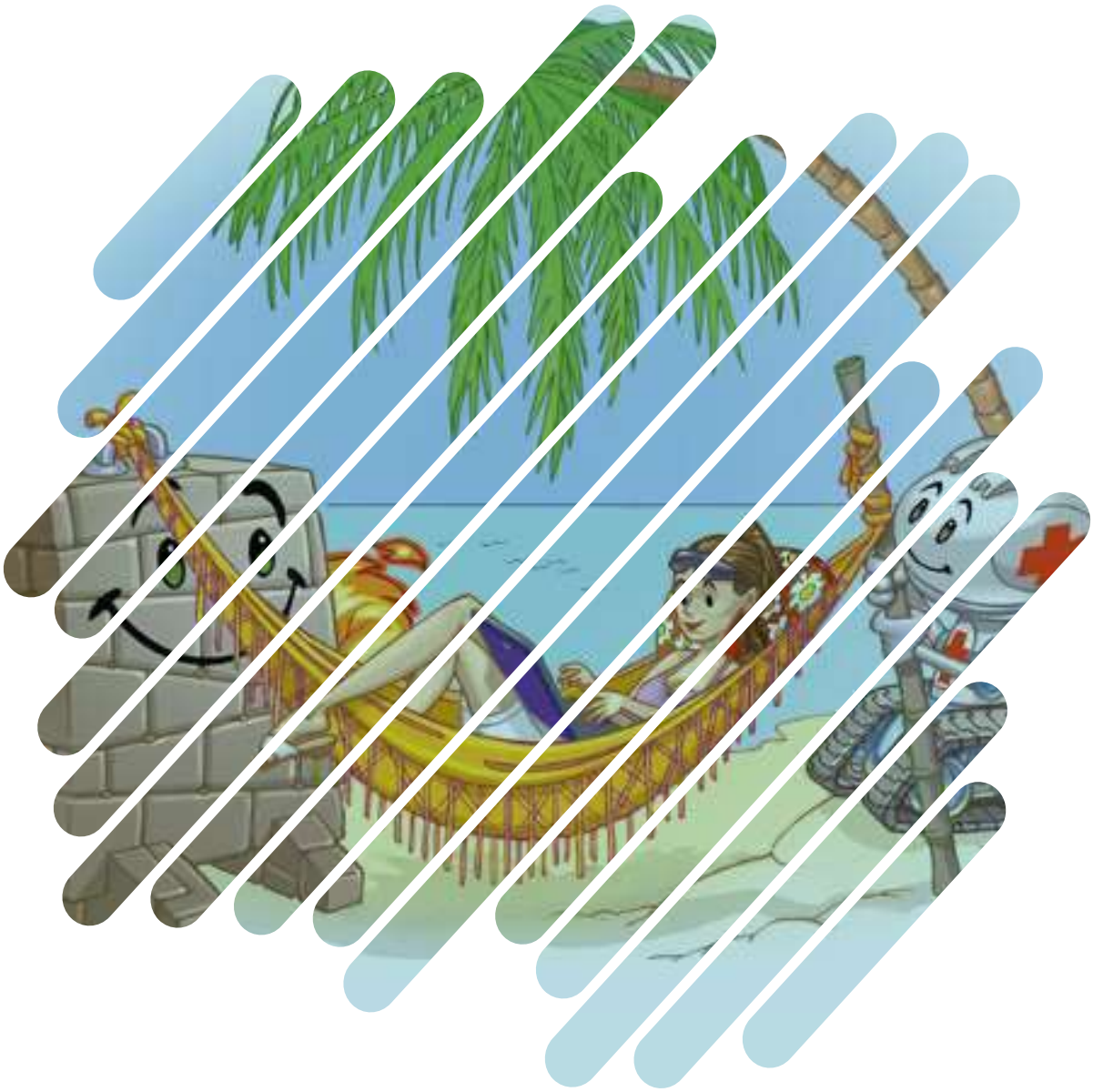
O Comitê Gestor da Internet no Brasil, responsável por estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil, coordena e integra todas as iniciativas de serviços Internet no País, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados. Com base nos princípios do multissetorialismo e transparência, o CGI.br representa um modelo de governança da Internet democrático, elogiado internacionalmente, em que todos os setores da sociedade são partícipes de forma equânime de suas decisões. Uma de suas formulações são os 10 Princípios para a Governança e Uso da Internet (**www.cgi.br/principios**). Mais informações em **www.cgi.br**.

outubro / 2020

Cartilha de Segurança para Internet

FASCÍCULO

REDES



Apoio de Divulgação:

UFPE

STI SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

Produção:

cert.br nic.br cgi.br

EQUIPAMENTOS DE REDE TAMBÉM PRECISAM DE CUIDADOS DE SEGURANÇA

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 nele existentes
- de ataques de força bruta, pelo uso de senhas fracas, padrão e/ou de conhecimento dos atacantes.

Após invadido ou infectado ele pode, de acordo com suas características, ser usado em atividades maliciosas, como propagação de códigos maliciosos, e estar sujeito a ameaças, como furto de dados e uso indevido de recursos.

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
- 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).

CONECTE-SE COM SEGURANÇA: PROTEJA SEUS EQUIPAMENTOS

CUIDADOS GERAIS A SEREM TOMADOS

» 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

» 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

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

CONFIGURANDO O ACESSO INTERNET DA SUA CASA

O acesso residencial costuma ser feito por meio de roteadores ou *modems* de banda larga que podem prover também a funcionalidade de rede sem fio. Esses equipamentos possuem senha de administração que pode ser usada para acesso remoto, tanto por você como pelo provedor de serviços Internet. Infelizmente muitos destes equipamentos são instalados com senhas fracas, padrão ou de conhecimento dos atacantes e por isso precisam ser alteradas.

- Siga os cuidados gerais para proteger seus equipamentos de rede, lembrando-se principalmente de atualizar o *firmware* e de alterar a senha de administração
- Desabilite:
  - o gerenciamento do equipamento de rede via Internet (WAN), assim as 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 utilizando

CONFIGURANDO UMA REDE WI-FI DOMÉSTICA

A 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.

- Siga as recomendações gerais para proteger seus equipamentos de rede, lembrando-se de atualizar o *firmware* e de alterar a senha de administração
- Altere também 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
- "Esconda" a sua rede
  - desabilite a difusão (*broadcast*) do SSID, evitando que o nome da rede seja anunciado para outros dispositivos, dificultando o acesso por quem não sabe a identificação
- Desabilite:
  - o WPS (*Wi-Fi Protected Setup*) para evitar acessos indevidos
  - o gerenciamento remoto (via rede sem fio), assim as funções de administração só estarão disponíveis por quem tiver acesso físico ao equipamento

CUIDADOS AO SE CONECTAR A REDES WI-FI

» 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 já utilizada por você e, sem saber, você estará acessando essa rede falsa)

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

» 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

» Certifique-se de usar conexão segura e observe se os dados do certificado digital correspondem ao da instituição a que pertence a página que você está acessando

CUIDADOS AO USAR REDES MÓVEIS (3G/4G)

Ao usar redes móveis é importante estar atento à segurança dos seus equipamentos. Um dispositivo infectado conectado via rede móvel pode ser usado para desferir ataques, enviar as informações coletadas e se propagar para outros dispositivos.

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

CUIDADOS AO USAR CONEXÕES *BLUETOOTH*

» 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 e seja cuidadoso ao elaborar a nova

» 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

» Para mais detalhes sobre este e outros assuntos relacionados com cuidados na Internet, consulte os demais Fascículos da Cartilha de Segurança e o Livro Segurança na Internet, disponíveis em: **cartilha.cert.br**

» Procurando material para conversar sobre segurança com diferentes públicos? O Portal Internet Segura apresenta uma série de materiais focados em crianças, adolescentes, pais, responsáveis e educadores, confira em: **internetsegura.br**

cert.br

O CERT.br é o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Desde 1997, o grupo é responsável por tratar incidentes de segurança envolvendo redes conectadas à Internet no Brasil. O Centro também desenvolve atividades de análise de tendências, treinamento e conscientização, com o objetivo de aumentar os níveis de segurança e de capacidade de tratamento de incidentes no Brasil. Mais informações em **www.cert.br.**

nic.br

O Núcleo de Informação e Coordenação do Ponto BR — NIC.br (**www.nic.br**) é uma entidade civil, de direito privado e sem fins de lucro, que além de implementar as decisões e projetos do Comitê Gestor da Internet no Brasil, tem entre suas atribuições: coordenar o registro de nomes de domínio — Registro.br (**www.registro.br**), estudar, responder e tratar incidentes de segurança no Brasil — CERT.br (**www.cert.br**), estudar e pesquisar tecnologias de redes e operações — Ceptro.br (**www.ceptro.br**), produzir indicadores sobre as tecnologias da informação e da comunicação — Cetic.br (**www.cetic.br**), implementar e operar os Pontos de Troca de Tráfego — IX.br (**www.ix.br**), viabilizar a participação da comunidade brasileira no desenvolvimento global da Web e subsidiar a formulação de políticas públicas — Ceweb.br (**www.ceweb.br**), e abrigar o escritório do W3C no Brasil (**www.w3c.br**).

cgi.br

O Comitê Gestor da Internet no Brasil, responsável por estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil, coordena e integra todas as iniciativas de serviços Internet no País, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados. Com base nos princípios do multissetorialismo e transparência, o CGI.br representa um modelo de governança da Internet democrático, elogiado internacionalmente, em que todos os setores da sociedade são partícipes de forma equânime de suas decisões. Uma de suas formulações são os 10 Princípios para a Governança e Uso da Internet (**www.cgi.br/principios**). Mais informações em **www.cgi.br**.

cartilha.cert.br/cc

outubro / 2020

Cartilha de Segurança para Internet

FASCÍCULO

BOATOS

Apoio de Divulgação:

UFPE

STI SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

Produção:

cert.br nic.br cgi.br

DENTRE TANTAS NOTÍCIAS QUE CIRCULAM POR AÍ, FICA DIFÍCIL SABER NO QUE ACREDITAR

Boato é “uma notícia de fonte desconhecida, muitas vezes infundada, que se divulga entre o público”[1]. Se após verificada, a notícia for considerada verdadeira diz-se que o boato foi confirmado e, caso contrário, que ele foi desmentido.

Como não se conhece a fonte da notícia não é possível saber exatamente o motivo pelo qual ela foi criada, podendo variar de simples diversão até interesses políticos e econômicos.

Popularmente conhecidos como “disse me disse”, “zunzunzum” e falatório, os boatos circulam há muito tempo no boca a boca. A Internet, porém, lhes deu maior alcance e dimensão.

Nunca foi tão fácil criar conteúdos e emitir opiniões. Entretanto, o excesso de informações, a velocidade com que elas se espalham, a impossibilidade de checar todas elas, o medo de estar “por fora” e o impulso em confiar no que conhecidos compartilham tornaram a Internet um ambiente propício para a multiplicação de boatos.

Para circularem, os boatos contam com a ajuda de contas falsas automatizadas e da boa vontade das pessoas que os repassam, atraídas principalmente pela curiosidade e pelo desejo de solidariedade. Para chamar a atenção, os boatos costumam usar como tema assuntos que estão em destaque no momento.

Na Internet os boatos circulam em redes sociais, grupos de mensagens e *e-mails*. Você pode recebê-los, por exemplo, via *spam*, em seu *feed* de notícias ou repassados por seus amigos e familiares.

No início os boatos eram conhecidos como ***hoaxes*** e circulavam por *e-mail*. Outro nome às vezes utilizado é **corrente**, que é aquele boato que pede para ser compartilhado com muitas pessoas. Atualmente, um termo muito utilizado é ***fake news***, geralmente associado a notícias que tentam se passar por reportagens jornalísticas verdadeiras e que possuem conteúdo falso, impreciso ou distorcido.

Independente do nome recebido, os boatos geram desinformação, causam problemas e precisam ser combatidos.

BOATOS: NA DÚVIDA, NÃO COMPARTILHE

[1]Segundo o dicionário Houaiss da Língua Portuguesa.

PROBLEMAS TRAZIDOS PELOS BOATOS

Há quem, mesmo suspeitando da notícia, prefira repassá-la pois "vai que é verdade" e "não custa nada compartilhar". Na verdade "**custa sim**" - quando você repassa um boato está lhe dando valor e importância, influenciando outros a acreditarem, contribuindo para que ele circule e potencializando as consequências.

Alguns exemplos de problemas trazidos pelos boatos são:

- Boatos espalham desinformação, reforçam crenças erradas, distraem de assuntos importantes e podem influenciar negativamente as opiniões
- O excesso de boatos leva ao descrédito, tornando frases como "li" e "vi na Internet" sinônimos de suspeitos, e pode servir para desmerecer notícias sérias
- Quem repassa boatos:
  - pode ser responsabilizado pelos danos causados, como difamação e calúnia
  - passa vergonha, pois assume publicamente que foi enganado
  - perde a credibilidade pois, se virar rotina, ninguém confiará no que ele compartilha
- Quem recebe boatos:
  - desperdiça tempo analisando as notícias
  - desperdiça o plano de dados de seus dispositivos móveis
  - pode ser vítima de golpes, ao acessar *links* para *sites* fraudulentos ou invadidos
- As empresas e pessoas citadas podem ter a reputação manchada, pois seus nomes ficam vinculados a conteúdos caluniosos e difamatórios, que dificilmente serão excluídos
- Coletivamente, os boatos geram pânico e espalham medo, ao circularem alertas sobre tragédias e catástrofes, como um suposto toque de recolher ou terremoto

COMO IDENTIFICAR UM BOATO

USE O BOM SENSO

» Às vezes a notícia é tão sem sentido (“sem pé nem cabeça”) que basta refletir um pouco para identificá-la como boato

» A sua intuição também é uma boa aliada - se a notícia parece estranha, levando-o a desconfiar, há uma grande chance dela realmente ser falsa

OBSERVE

» Os boatos apresentam características[2] em comum entre eles que podem servir como indícios e ajudar a identificá-los. Geralmente um boato:

- afirma não ser um boato
- possui título bombástico, resumido e com destaques em maiúsculo[3]
- possui tom alarmista e usa palavras como “Cuidado” e “Atenção”
- omite a data e/ou o local
- não possui fonte ou cita fontes desconhecidas
- não apresenta evidências e nem embasamento dos fatos noticiados
- apresenta um fato exclusivo, ainda não encontrado em outros locais
- mostra dados superlativos (“o maior”, “o melhor”)
- explora assuntos que estão repercutindo no momento
- usa URL e identidade visual similares às de *sites* conhecidos
- apresenta erros gramaticais e de ortografia
- usa imagens adulteradas ou fora de contexto
- sugere consequências trágicas, se determinada tarefa não for realizada
- promete ganhos financeiros mediante a realização de alguma ação
- pede para ser repassado para um grande número de pessoas
- possui grande quantidade de curtidas e compartilhamentos
- vem de um perfil ou *site* já conhecido por divulgar boatos

[2]Estas características devem ser usadas como guia, já que podem existir boatos que não apresentem nenhuma delas e notícias legítimas que apresentem algumas.

[3]Notícias que apelam para títulos sensacionalistas para despertar a curiosidade, atrair cliques, ganhar audiência e lucrar com os acessos, são chamadas pejorativamente de caça-cliques (ou *clickbaits*).

FIQUE ATENTO AOS DETALHES

» Verifique todo o conteúdo antes de repassar uma notícia

» Observe a data, a notícia pode ser verdadeira mas se referir a fatos antigos

» Verifique a URL, às vezes, na tentativa de dar maior credibilidade à notícia, são criados *sites* com nomes similares aos de outros veículos de comunicação

VÁ DIRETO À FONTE

» Verifique a origem da notícia. Mesmo que a notícia cite fontes confiáveis, as informações podem estar fora do contexto ou com partes excluídas

» Observe se a fonte da notícia já não é um boato (um boato baseado em outro boato)

» Se a fonte da notícia tiver sido escrita em outro idioma, tente ler a notícia original (erros de tradução podem levar a interpretações erradas)

CONFIRME EM OUTRAS FONTES

» Pesquise pelas palavras citadas. Mesmo furos de reportagem possuem poucas chances de ainda não terem sido divulgados em outros locais

» Pesquise a imagem usada (caso haja), tente identificar a sua origem e observe em quais outras páginas e contextos ela aparece

» Consulte o *site* oficial das empresas citadas à procura de comunicados que confirmem ou desmintam a notícia

» Consulte *sites* especializados em desmentir boatos *online*, como:

- Boatos.org
  www.boatos.org
- E-farsas
  www.e-farsas.com
- Quatro cantos
  www.quatrocantos.com/lendas

QUESTIONE-SE

» Ao ler uma notícia tente se fazer algumas perguntas - as respostas poderão lhe ajudar a identificar notícias falsas e, com a prática, isso se tornará um hábito

- qual é a fonte? quem a escreveu? essa pessoa tem conhecimento para isso? existem fatos que comprovem? o mesmo fato está sendo noticiado em outros lugares? você conhece o *site* onde está a notícia? quais são os outros conteúdos desse *site*? quando e onde ela aconteceu? pode ser uma piada? ela é útil para alguém? vale a pena ser repassada?

AJUDE A COMBATER OS BOATOS

INFORME-SE

» Consulte meios diversos de comunicação e converse com outras pessoas, não se limite somente ao que recebe nas redes sociais

» Não confunda opinião com notícia. Opinião cada um tem a sua e ela deve ser respeitada, mesmo que você não concorde

» Lembre-se: nada melhor que a informação para combater a desinformação

DESCONFIE, DUVIDE E SEJA CRÍTICO

» Não acredite em qualquer notícia, mesmo que vinda de conhecidos, pois ela pode ter sido enviada de uma conta invadida ou falsa

» Verifique as configurações das suas redes sociais e, se possível, priorize seus contatos e denuncie os boatos recebidos

CUIDADO COM CONTAS FALSAS

» Contas falsas[4] são usadas para replicar automaticamente boatos e costumam ser proibidas, já que ferem os termos de uso das redes sociais

» Seja cuidadoso ao aceitar seguidores. Ao aceitar uma conta falsa você ajudará a torná-la "real", já que a conexão entre vocês pode induzir outros a também aceitá-la

» Tente reconhecer contas falsas e as denuncie. Uma conta falsa geralmente possui muitos seguidores, publica pouco, curte e compartilha muito, apresenta poucas informações pessoais e não possui foto de perfil

PROTEJA SUAS CONTAS DE ACESSO

» Contas de *e-mail* e de redes sociais são bastante visadas para a divulgação de boatos, já que as pessoas

[4]Contas falsas costumam usar *bots* para multiplicar os boatos. *Bot*, originado de *robot* (robô), refere-se a um tipo de programa que permite automatizar tarefas e que pode ser usado tanto para fins legítimos como maliciosos.

tendem a confiar no que conhecidos compartilham

- use senhas longas, com diferentes caracteres e evite usar dados pessoais
- não reutilize suas senhas
- ative a verificação em duas etapas
- acesse os *sites* digitando a URL no navegador ou usando aplicativos oficiais

MANTENHA SEUS EQUIPAMENTOS SEGUROS

» Equipamentos infectados ou invadidos podem ser usados para o envio de boatos

- use apenas programas originais

- instale a versão mais nova do sistema operacional e dos aplicativos usados
- aplique todas as atualizações e não esqueça de reiniciá-los quando solicitado
- instale mecanismos de segurança, como antivírus, *antispam* e *firewall* pessoal
- tenha cuidado ao abrir arquivos anexos e ao clicar em *links*

OUTRAS FONTES DE INFORMAÇÕES FALSAS

» **Piadas, paródias e sátiras** são histórias inventadas com o objetivo de divertir. *Sites* e canais com conteúdo humorístico costumam deixar isso claro justamente para não serem levados a sério. *E aí? Você conhece aquela do papagaio?*

» **Lendas urbanas** são histórias fabulosas incorporadas ao folclore moderno, que apresentam lição de moral e são contadas como fatos verídicos ocorridos com alguém próximo. *Já ouviu falar na loira do banheiro? Uma vez o amigo do meu tio...*

» **Fofocas** são comentários, geralmente maldosos, feitos às escondidas sobre a vida de outras pessoas. *Você já ficou sabendo da última? Mas não diga que fui eu que contei.*

SAIBA MAIS

» Para mais detalhes sobre este e outros assuntos relacionados com cuidados na Internet, consulte os demais Fascículos da Cartilha de Segurança e o Livro Segurança na Internet, disponíveis em: **cartilha.cert.br**

» Procurando material para conversar sobre segurança com diferentes públicos? O Portal Internet Segura apresenta uma série de materiais focados em crianças, adolescentes, pais, responsáveis e educadores, confira em: **internetsegura.br**

cert.br

O CERT.br é o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Desde 1997, o grupo é responsável por tratar incidentes de segurança envolvendo redes conectadas à Internet no Brasil. O Centro também desenvolve atividades de análise de tendências, treinamento e conscientização, com o objetivo de aumentar os níveis de segurança e de capacidade de tratamento de incidentes no Brasil. Mais informações em **www.cert.br.**

nic.br

O Núcleo de Informação e Coordenação do Ponto BR — NIC.br (**www.nic.br**) é uma entidade civil, de direito privado e sem fins de lucro, que além de implementar as decisões e projetos do Comitê Gestor da Internet no Brasil, tem entre suas atribuições: coordenar o registro de nomes de domínio — Registro.br (**www.registro.br**), estudar, responder e tratar incidentes de segurança no Brasil — CERT.br (**www.cert.br**), estudar e pesquisar tecnologias de redes e operações — Ceptro.br (**www.ceptro.br**), produzir indicadores sobre as tecnologias da informação e da comunicação — Cetic.br (**www.cetic.br**), implementar e operar os Pontos de Troca de Tráfego — IX.br (**www.ix.br**), viabilizar a participação da comunidade brasileira no desenvolvimento global da Web e subsidiar a formulação de políticas públicas — Ceweb.br (**www.ceweb.br**), e abrigar o escritório do W3C no Brasil (**www.w3c.br**).

cgi.br

O Comitê Gestor da Internet no Brasil, responsável por estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil, coordena e integra todas as iniciativas de serviços Internet no País, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados. Com base nos princípios do multissetorialismo e transparência, o CGI.br representa um modelo de governança da Internet democrático, elogiado internacionalmente, em que todos os setores da sociedade são partícipes de forma equânime de suas decisões. Uma de suas formulações são os 10 Princípios para a Governança e Uso da Internet (**www.cgi.br/principios**). Mais informações em **www.cgi.br**.

outubro / 2020

Cartilha de Segurança para Internet

FASCÍCULO

VAZAMENTO DE DADOS

Apoio de Divulgação:

UFPE

STI SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

Contribuição:

ANPD

Produção:

cert.br nic.br cgi.br

INFELIZMENTE, HÁ SITUAÇÕES EM QUE SEUS DADOS PODEM VAZAR NA INTERNET

Vazamentos de dados (*data leak*) ocorrem quando dados são indevidamente acessados, coletados e divulgados na Internet, ou repassados a terceiros. Com a disseminação dos serviços *online*, seus dados estão cada vez mais expostos e sendo coletados pelos diferentes serviços disponíveis.

O vazamento pode ser originado:

- do furto de dados por atacantes e códigos maliciosos que exploram vulnerabilidades em sistemas
- do acesso a contas de usuários, por meio de senhas fracas ou vazadas
- da ação de funcionários ou ex-funcionários que coletam dados dos sistemas da empresa e os repassam a terceiros
- do furto de equipamentos que contenham dados sigilosos
- de erros ou negligência de funcionários, como descartar mídias (discos e *pen drives*) sem os devidos cuidados.

Exemplos de dados que podem vazar:

- credenciais de acesso, como nomes de usuário e senhas
- informações financeiras, como números de contas bancárias e de cartões de crédito
- documentos, como CPF, RG e carteira de habilitação
- informações de contato, como endereços e números de telefone
- registros de saúde, como resultados de exames e prontuários médicos
- outros dados, como data de nascimento e nomes de familiares.

Para evitar vazamentos é importante que todos contribuam e **você pode ajudar tentando reduzir a quantidade de dados expostos sobre você.** Também é importante ficar atento e, no caso de um vazamento envolvendo seus dados, agir rapidamente para reduzir os danos.

ATENÇÃO: Após um vazamento é esperado um aumento nas tentativas de golpes por diferentes meios, como *e-mails*, mensagens de texto e ligações telefônicas.

PROTEJA SEUS DADOS: CUIDADO COM VAZAMENTOS

RISCOS PRINCIPAIS

Dados vazados podem expor você e sua família e ser usados para abrir contas, contrair dívidas ou aplicar golpes.

FURTO DE IDENTIDADE E INVASÃO DE CONTAS *ONLINE*

- Abertura de contas em seu nome
- Tentativas de adivinhação de senhas ou para responder perguntas de segurança
- Uso de senhas vazadas para invadir outros serviços onde a mesma senha é usada, se eles não tiverem ativado algum mecanismo de segurança adicional como:
  - verificação em duas etapas, ou
  - autorização prévia de dispositivos

FURTO DE IDENTIDADE LEVANDO A PREJUÍZOS FINANCEIROS

- Criação de cartões de crédito, contas bancárias e empréstimos, levando a dívidas ou transações ilícitas em seu nome
- Movimentações financeiras indevidas em suas contas bancárias ou cartões de crédito
- Transferência de bens móveis ou imóveis

VIOLAÇÃO DE PRIVACIDADE

- Informações privadas, como dados médicos ou conversas particulares, podem ficar expostas na Internet

TENTATIVAS DE GOLPES

- Extorsão, onde o atacante faz chantagem para não expor os seus dados
- Quanto mais informações um atacante tiver, mais convincente ele será, e mais facilmente enganará outras pessoas
- Os dados vazados podem ser usados, por exemplo:
  - em tentativas de *phishing* direcionado e personalizado *(spear phishing)*
  - para convencê-lo a revelar mais informações
  - para induzi-lo a efetivar transações
  - para se passar por você

O QUE FAZER EM CASO DE VAZAMENTO

INFORME-SE

» Se receber notificações ou souber pela mídia de algum vazamento envolvendo seus dados pessoais, informe-se sobre o ocorrido e tente identificar:

- quais dados vazaram (isso ajuda a saber quais medidas tomar)
- quais medidas de mitigação foram ou serão tomadas pela organização
- quais medidas devem ser tomadas por você
- as datas do potencial vazamento
- comunicados e notícias a respeito

» Evite acessar *sites* e abrir arquivos que supostamente confirmem ou exibam os dados do vazamento. Em caso de dúvida, contate diretamente as organizações envolvidas e busque mais informações

O QUE FAZER EM CADA CASO

» **Credenciais de acesso vazadas**

- troque imediatamente as senhas expostas
- ative a verificação em duas etapas nas contas que ofereçam esse recurso, caso ainda não tenha feito
- use os mecanismos disponíveis para analisar os registros de acesso e denunciar tentativas/acessos indevidos

» **Cartões de crédito ou débito vazados**

- informe as instituições emissoras dos cartões
- revise o extrato dos seus cartões e da sua conta bancária
- conteste os eventuais lançamentos irregulares que identificar, via os canais oficiais das respectivas instituições

FIQUE ATENTO

» Monitore sua vida financeira e sua identidade

- ative alertas e monitore o extrato dos seus cartões e da sua conta bancária. Preste atenção a movimentações “estranhas”
- acompanhe outros registros financeiros, por meio de serviços específicos, como o oferecido pelo Banco Central (Serviço “Registrato”)
- verifique no “Cadastro Pré”, mantido por empresas do Setor de Telecomunicações, se alguma linha pré-paga de celular foi ativada usando seu CPF
- busque saber mais se:
  - receber notificações de instituições de proteção ao crédito
  - ao tentar se cadastrar em algum serviço ou benefício, for informado que seu cadastro já existe

» Cuide de suas contas e senhas

- nunca forneça códigos de verificação a terceiros
- ative notificações e monitore tentativas de *login*, de recuperação ou troca de senhas

- se constatar que alguma conta foi invadida ou criaram um perfil em seu nome:
  - efetue os procedimentos disponíveis nas plataformas para recuperação do acesso ou denúncia do perfil falso
  - informe seus contatos para que não caiam em golpes

» Previna-se contra golpes

- não clique em *links* recebidos por *e-mail* ou mensagens de texto, mesmo que pareçam enviados por alguém que você conhece (pode ser um *spear phishing*)
- não efetive transações financeiras sem antes confirmar a identidade das partes envolvidas

A QUEM RECORRER

Seguem recomendações sobre quem contatar caso verifique que seus dados foram usados de maneira fraudulenta ou você foi prejudicado de alguma forma.

» Fraude financeira
- contate as instituições envolvidas e siga as orientações recebidas

» Furto de identidade
- registre Boletim de Ocorrência junto à autoridade policial, para viabilizar a apuração e resguardar-se
- contate as instituições envolvidas

» Se comprovadamente ocorrer um vazamento envolvendo seus dados pessoais, busque informações junto à instituição responsável (também chamada controladora de dados) e, caso a sua solicitação não seja atendida, ou não saiba qual instituição está envolvida, você pode fazer uma denúncia no *site* da Autoridade Nacional de Proteção de Dados (ANPD - https://www.gov.br/anpd/), informando:
- quais os dados vazados
- quando teve ciência do vazamento
- se acredita que seus dados pessoais foram indevidamente usados em alguma ação criminosa (como estelionato, fraude ou comércio ilegal de dados pessoais)
- quais evidências possui para corroborar essa hipótese

NÃO INCENTIVE VAZAMENTOS E ABUSOS

» Não compre listas de dados, essa prática incentiva que mais vazamentos ocorram e coloca todos em risco, inclusive você

» Evite acessar *sites* e abrir arquivos que supostamente confirmem ou exibam os dados vazados. Eles podem ter sido criados com fins maliciosos para expor ainda mais seus dados

COMO SE PREVENIR

Os seus dados pessoais são valiosos e muitas instituições têm interesse em obtê-los para fins comerciais, bem como atacantes para ações maliciosas. Reduza a quantidade de dados que possam ser divulgados sobre você, caso haja um vazamento. Veja dicas para reduzir os riscos em diferentes ambientes.

CADASTROS E *SITES*

- Ao preencher cadastros questione-se sobre a real necessidade de fornecer todos os dados e da instituição retê-los
- Leia as políticas de privacidade dos serviços que usa
- Ao acessar *sites*, procure limitar a coleta de dados por *cookies*. Preferencialmente, autorize somente aqueles essenciais ao funcionamento da sessão e limpe frequentemente o histórico de navegação
- Use conexões seguras para evitar que seus dados sejam interceptados e coletados

LINKS E APLICATIVOS

- Desconfie de *links* recebidos via mensagens eletrônicas, mesmo que vindos de pessoas conhecidas (podem ter sido enviadas de perfis falsos ou invadidos)
- Observe as configurações de privacidade de seus equipamentos e dos *softwares* instalados. Limite quais aplicativos podem acessar o microfone, a câmera, seus contatos e sua localização
- Apague os aplicativos que você não usa mais

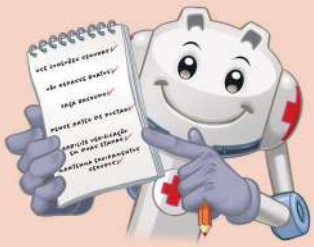
CONTAS E SENHAS

- Crie senhas fortes, não repita senhas e, se possível, habilite a verificação em duas etapas
- Habilite, quando disponíveis, notificações de *login*, para ser mais fácil perceber se outras pessoas estiverem usando suas contas

ARQUIVOS E EQUIPAMENTOS

- Mantenha seus equipamentos seguros, com o sistema e os aplicativos atualizados e utilize mecanismos de segurança
- Verifique no monitor de atividades de seu equipamento a lista de programas em execução e desconfie de processos “estranhos”
- Evite colocar na nuvem arquivos contendo dados pessoais que considere confidenciais, como fotos e cópias de documentos
- Use criptografia, sempre que possível, para proteger os dados armazenados em seus equipamentos

SAIBA MAIS



» Para mais detalhes sobre este e outros assuntos relacionados com cuidados na Internet, consulte os demais Fascículos da Cartilha de Segurança e o Livro Segurança na Internet, disponíveis em: **cartilha.cert.br**

» Procurando material para conversar sobre segurança com diferentes públicos? O Portal Internet Segura apresenta uma série de materiais focados em crianças, adolescentes, pais, responsáveis e educadores, confira em: **internetsegura.br**

cert.br

O CERT.br é o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Desde 1997, o grupo é responsável por tratar incidentes de segurança envolvendo redes conectadas à Internet no Brasil. O Centro também desenvolve atividades de análise de tendências, treinamento e conscientização, com o objetivo de aumentar os níveis de segurança e de capacidade de tratamento de incidentes no Brasil. Mais informações em **www.cert.br.**

nic.br

O Núcleo de Informação e Coordenação do Ponto BR — NIC.br (**www.nic.br**) é uma entidade civil, de direito privado e sem fins de lucro, que além de implementar as decisões e projetos do Comitê Gestor da Internet no Brasil, tem entre suas atribuições: coordenar o registro de nomes de domínio — Registro.br (**www.registro.br**), estudar, responder e tratar incidentes de segurança no Brasil — CERT.br (**www.cert.br**), estudar e pesquisar tecnologias de redes e operações — Ceptro.br (**www.ceptro.br**), produzir indicadores sobre as tecnologias da informação e da comunicação — Cetic.br (**www.cetic.br**), implementar e operar os Pontos de Troca de Tráfego — IX.br (**www.ix.br**), viabilizar a participação da comunidade brasileira no desenvolvimento global da Web e subsidiar a formulação de políticas públicas — Ceweb.br (**www.ceweb.br**), e abrigar o escritório do W3C no Brasil (**www.w3c.br**).

cgi.br

O Comitê Gestor da Internet no Brasil, responsável por estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil, coordena e integra todas as iniciativas de serviços Internet no País, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados. Com base nos princípios do multissetorialismo e transparência, o CGI.br representa um modelo de governança da Internet democrático, elogiado internacionalmente, em que todos os setores da sociedade são partícipes de forma equânime de suas decisões. Uma de suas formulações são os 10 Princípios para a Governança e Uso da Internet (**www.cgi.br/principios**). Mais informações em **www.cgi.br**.

ANPD

A Autoridade Nacional de Proteção de Dados – ANPD é um órgão vinculado à Presidência da República, dotada de autonomia técnica e decisória, que tem a competência de zelar pela proteção dos dados pessoais com o objetivo de proteger os direitos fundamentais de liberdade e de privacidade e o livre desenvolvimento da personalidade da pessoa natural, conforme disposto na Lei nº 13.709, de 14 de agosto de 2018, a LGPD. Mais informações em **www.gov.br/anpd.**

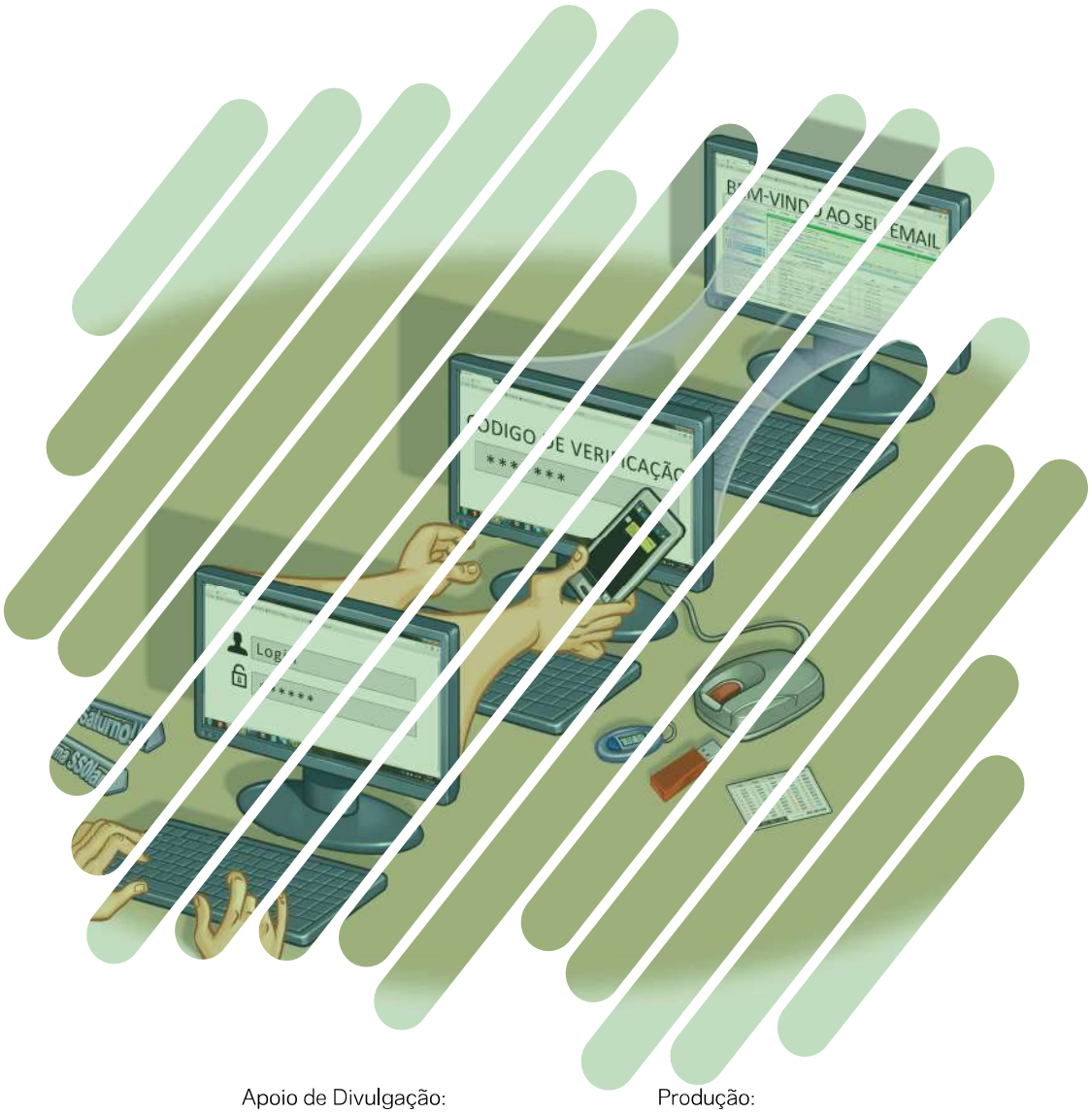
cartilha.cert.br/cc

maio / 2021

Cartilha de Segurança para Internet

FASCÍCULO

VERIFICAÇÃO EM DUAS ETAPAS



Apoio de Divulgação:

UFPE

STI SUPERINTENDÊNCIA DE TECNOLOGIA DA INFORMAÇÃO

Produção:

cert.br nic.br cgi.br

USAR APENAS SENHAS PODE NÃO SER SUFICIENTE PARA PROTEGER SUAS CONTAS NA INTERNET

Senhas são simples e bastante usadas para autenticação em *sites* na Internet. Infelizmente elas podem não ser suficientes para garantir a sua identidade.

Senhas podem ser facilmente descobertas por meio de técnicas de engenharia social, por observação, se não forem bem elaboradas, se usadas em páginas falsas *(phishing)* ou em computadores infectados/invadidos ou, ainda, se trafegarem na rede sem criptografia.

Por isso, é importante que a verificação da identidade do usuário baseie-se em informações adicionais, além do uso único da senha.

[1]Verificação em duas etapas também é chamada de:
- *two-factor authentication*
- aprovação de *login*
- verificação ou autenticação em dois fatores
- verificação ou autenticação em dois passos

Com a verificação em duas etapas[1] fica mais difícil da sua conta de acesso ser invadida pois, para que isso ocorra, é necessário que o atacante saiba a sua senha (primeira etapa) e também realize com sucesso uma segunda etapa, a qual pode envolver algo que:

» apenas você sabe
- outra senha, pergunta de segurança, número PIN, alguma informação pessoal

» apenas você possui
- código de verificação, cartão de senhas bancárias, *token* gerador de senhas, acesso a um determinado computador ou dispositivo móvel

» você é
- informações biométricas, como impressão digital, palma da mão, rosto, voz e olho.

VERIFICAÇÃO EM DUAS ETAPAS: CONTAS DE ACESSO MAIS SEGURAS

PRINCIPAIS TIPOS E CUIDADOS A SEREM TOMADOS

A verificação em duas etapas é um recurso opcional oferecido por diversos serviços de Internet, como *webmail*, redes sociais, *Internet Banking* e de armazenamento em nuvem. Ao habilitá-la você estará aumentando a segurança de sua conta e, caso não deseje mais utilizá-la, basta que você a desabilite.

O tipo de verificação usado pode variar de acordo com o serviço acessado mas, por facilidade, a maioria costuma utilizar-se de algo que apenas você sabe ou possui.

Alguns dos tipos mais comuns e os cuidados que você deve tomar ao usá-los são:

CÓDIGO DE VERIFICAÇÃO

é um código individual criado pelo serviço e enviado de forma que apenas você possa recebê-lo, por exemplo, por *e-mail*, chamada de voz ou mensagem de texto (SMS) para o telefone celular que você cadastrou. Também pode ser gerado por um aplicativo autenticador, instalado em seu dispositivo móvel.

- Mantenha seus dados para recebimento sempre atualizados
  - números de telefones celulares alternativos também podem ser cadastrados, caso o seu principal não esteja disponível
- Tenha certeza de estar de posse de seu telefone celular, caso tenha configurado o envio via SMS ou gerado pelo aplicativo autenticador
- Recomenda-se o uso do aplicativo autenticador em casos onde não é possível receber mensagens SMS
  - por exemplo, se você estiver viajando ou em uma área sem cobertura de celular
- Tarifas de recebimento de SMS podem ser aplicadas por sua operadora

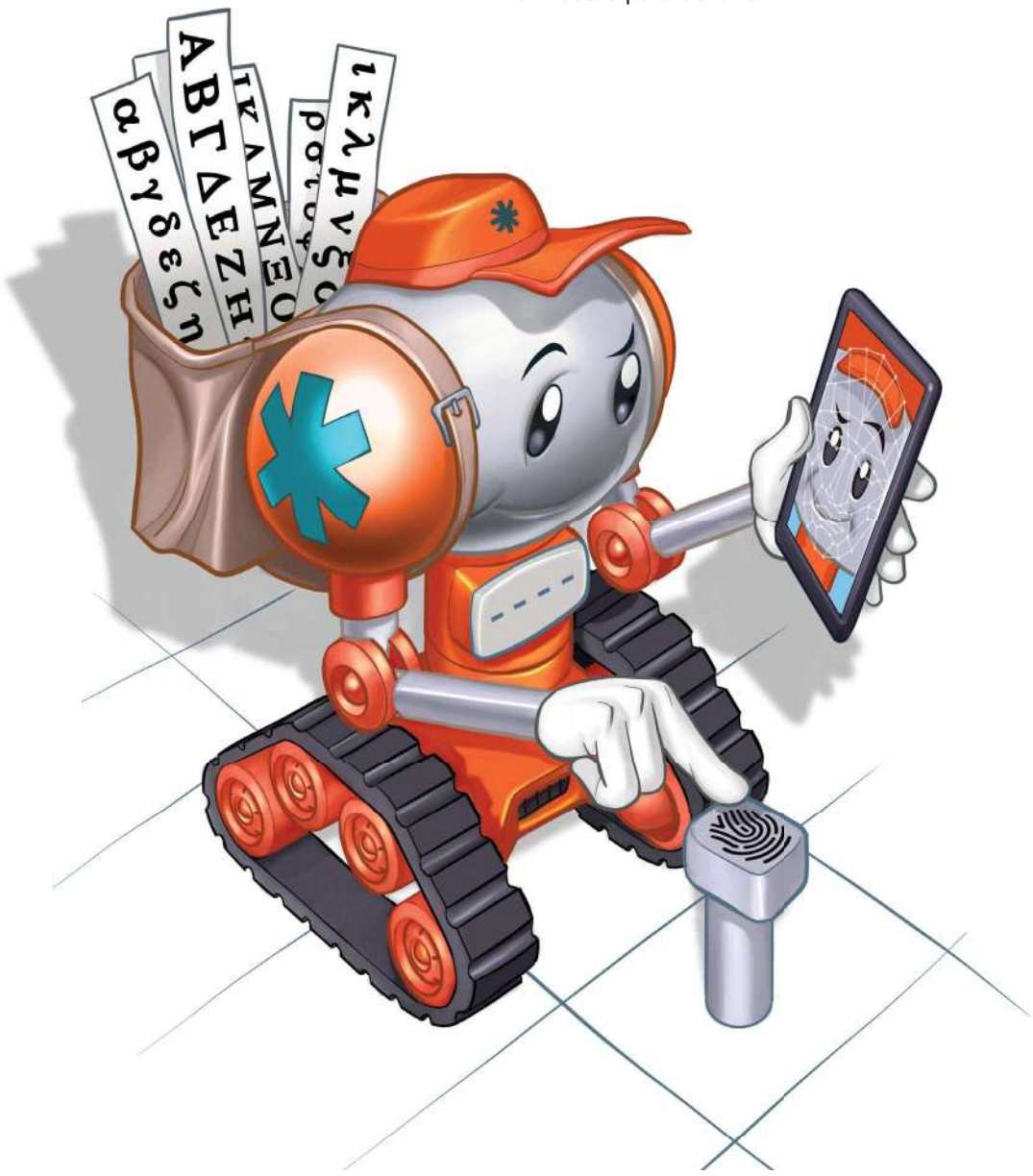
CÓDIGO DE VERIFICAÇÃO ESPECÍFICO

é um código gerado para aplicativos que não suportam a verificação em duas etapas.

» Caso perca o acesso ao seu dispositivo móvel, revogue os códigos específicos gerados para os acessos realizados por meio dele

TOKEN GERADOR DE SENHAS (OU CHAVE ELETRÔNICA)

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



- Guarde seu *token* em um local seguro
- Nunca 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

CARTÃO DE SEGURANÇA

é um cartão com diversos códigos numerados e que são solicitados quando você acessa a sua conta.

- 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 que é 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

DISPOSITIVO CONFIÁVEL (OU DE CONFIANÇA)

é um computador ou dispositivo móvel que você frequentemente usa para acessar suas contas. Pode ser necessário inserir um código de segurança no primeiro acesso. Ele não será necessário nos demais, pois seu dispositivo será "lembrado", caso você assim o configure.

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

LISTA DE CÓDIGOS RESERVA/*BACKUP*

é uma lista de códigos que devem ser usados de forma sequencial e uma única vez.

- 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)

CHAVE DE RECUPERAÇÃO

é um 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.

- 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)

OUTROS CUIDADOS

MANTENHA SEU CADASTRO ATUALIZADO

» Dados pessoais, como data de aniversário, podem ser solicitados aleatoriamente para checar a sua identidade

» É importante manter seu endereço de correspondência atualizado, para o recebimento de *tokens* e cartões de segurança

» Dados pessoais e perguntas de segurança podem ser solicitados, caso você desabilite a verificação em duas etapas

SEJA CUIDADOSO AO ELABORAR SUAS SENHAS

» Evite usar:

- dados que possam ser obtidos em redes sociais e páginas *web*
- dados pessoais, como nomes, sobrenomes e contas de usuário
- sequências de teclado, como "1qaz2wsx" e "QwerTAsdfG"
- palavras que fazem parte de listas publicamente conhecidas

» Use:

- números aleatórios
- grande quantidade e diferentes tipos de caracteres

SEJA CUIDADOSO AO USAR SUAS SENHAS

» Certifique-se de utilizar conexão segura

» Evite utilizar computadores de terceiros

» Somente acesse os serviços digitando o endereço diretamente no navegador *web*, nunca clicando em um *link* existente em uma página ou em uma mensagem

PROTEJA SEUS DISPOSITIVOS MÓVEIS

» Cadastre uma senha de acesso que seja bem elaborada e, se possível, configure-os para aceitarem senhas complexas (alfanuméricas)

» Se disponível, instale um programa antivírus

» Mantenha o sistema operacional e as aplicações instaladas sempre com a versão mais recente e com todas as atualizações aplicadas

» Mantenha controle físico sobre eles, principalmente em locais de risco

- procure não deixá-los sobre a mesa
- cuidado com bolsos e bolsas quando estiver em ambientes públicos

» Em caso de perda ou furto:

- revogue todas as autorizações concedidas para os aplicativos neles instalados
- remova-os da lista de dispositivos confiáveis
- cadastre um novo número de celular para continuar a receber códigos de verificação
- se tiver configurado a localização remota, você pode ativá-la e, se achar necessário, apagar remotamente todos os dados neles armazenados

PROTEJA SEU COMPUTADOR

» Mantenha o seu computador seguro

- com a versão mais recente de todos os programas instalados
- com todas as atualizações aplicadas

» Utilize e mantenha atualizados mecanismos de segurança, como *antispam*, antivírus e *firewall* pessoal

» Configure-o para solicitar senha na tela inicial

SAIBA MAIS

» Para mais detalhes sobre este e outros assuntos relacionados com cuidados na Internet, consulte os demais Fascículos da Cartilha de Segurança e o Livro Segurança na Internet, disponíveis em: **cartilha.cert.br**

» Procurando material para conversar sobre segurança com diferentes públicos? O Portal Internet Segura apresenta uma série de materiais focados em crianças, adolescentes, pais, responsáveis e educadores, confira em: **internetsegura.br**

cert.br

O CERT.br é o Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil. Desde 1997, o grupo é responsável por tratar incidentes de segurança envolvendo redes conectadas à Internet no Brasil. O Centro também desenvolve atividades de análise de tendências, treinamento e conscientização, com o objetivo de aumentar os níveis de segurança e de capacidade de tratamento de incidentes no Brasil. Mais informações em **www.cert.br.**

nic.br

O Núcleo de Informação e Coordenação do Ponto BR — NIC.br (**www.nic.br**) é uma entidade civil, de direito privado e sem fins de lucro, que além de implementar as decisões e projetos do Comitê Gestor da Internet no Brasil, tem entre suas atribuições: coordenar o registro de nomes de domínio — Registro.br (**www.registro.br**), estudar, responder e tratar incidentes de segurança no Brasil — CERT.br (**www.cert.br**), estudar e pesquisar tecnologias de redes e operações — Ceptro.br (**www.ceptro.br**), produzir indicadores sobre as tecnologias da informação e da comunicação — Cetic.br (**www.cetic.br**), implementar e operar os Pontos de Troca de Tráfego — IX.br (**www.ix.br**), viabilizar a participação da comunidade brasileira no desenvolvimento global da Web e subsidiar a formulação de políticas públicas — Ceweb.br (**www.ceweb.br**), e abrigar o escritório do W3C no Brasil (**www.w3c.br**).

cgi.br

O Comitê Gestor da Internet no Brasil, responsável por estabelecer diretrizes estratégicas relacionadas ao uso e desenvolvimento da Internet no Brasil, coordena e integra todas as iniciativas de serviços Internet no País, promovendo a qualidade técnica, a inovação e a disseminação dos serviços ofertados. Com base nos princípios do multissetorialismo e transparência, o CGI.br representa um modelo de governança da Internet democrático, elogiado internacionalmente, em que todos os setores da sociedade são partícipes de forma equânime de suas decisões. Uma de suas formulações são os 10 Princípios para a Governança e Uso da Internet (**www.cgi.br/principios**). Mais informações em **www.cgi.br.**

cartilha.cert.br/cc

outubro / 2020