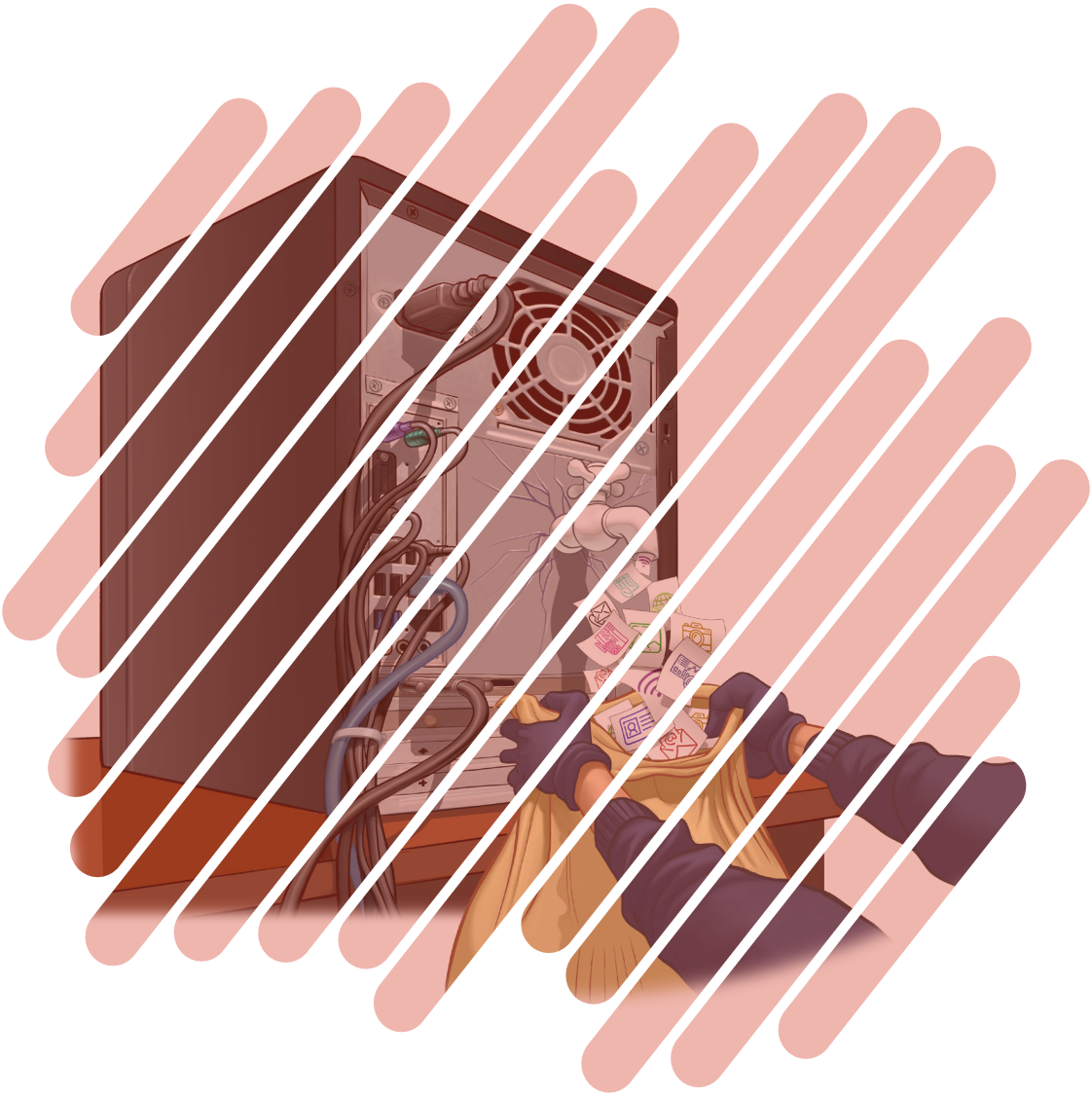
Cartilha de Segurança para Internet

FASCÍCULO

VAZAMENTO DE DADOS



Com a contribuição da:

ANPD

Produzido por:

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

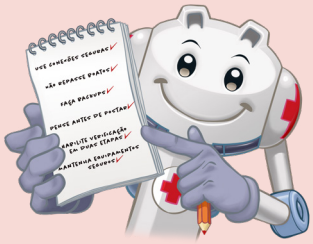
CONTAS E SENHAS

- 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