Banco via Internet

Apoio de Divulgação:

GUARDIÃO CIBERNÉTICO

Produção:

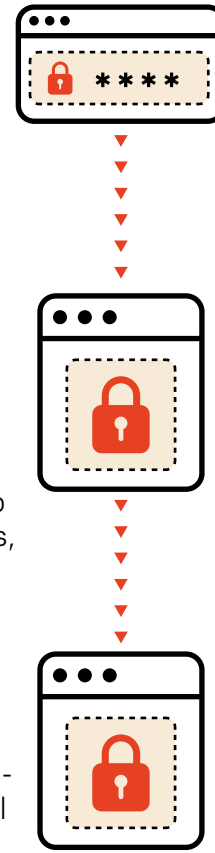
cert.br nic.br cgi.br

PROTEJA SUA VIDA FINANCEIRA

Graças à Internet, realizar transações financeiras se tornou mais fácil e rápido. Mas sem cuidados mínimos, essa praticidade pode ser explorada por golpistas.

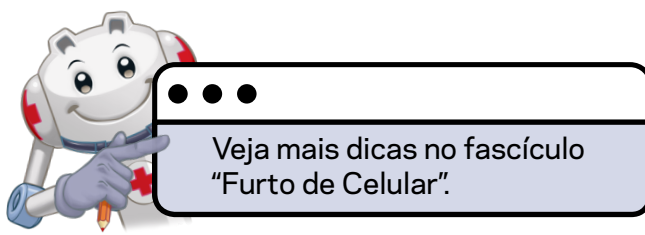
Veja aqui como se proteger e evitar prejuízos.

USE SENHA FORTE NO BLOQUEIO DO CELULAR, MESMO COM BIOMETRIA

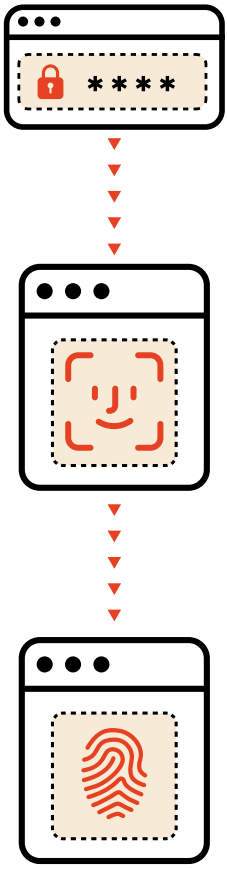


O celular sempre tem uma senha ou padrão que permite desbloqueá-lo, mesmo quando se usa biometria. Se esta senha for fraca, um ladrão pode adivinhá-la, desbloquear e mudar configurações no celular e acessar outros aplicativos, dados e contas.

- Defina uma senha longa, de preferência alfanumérica
- Se usar padrão de desbloqueio, evite desenhos simples
- Ative o bloqueio de tela automático com o menor tempo disponível



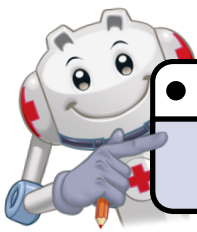
Veja mais dicas no fascículo “Furto de Celular”.



COMBINE SENHA FORTE COM BIOMETRIA NOS APLICATIVOS FINANCEIROS

Aplicativos financeiros geralmente usam senha e biometria para controle de acesso. Mesmo com biometria ativada, se a senha for fácil de adivinhar, um ladrão poderá descobri-la e invadir a sua conta.

- Crie uma senha forte para acesso via aplicativo (Internet)
- Ative biometria para facilitar o acesso e não precisar lembrar tantas senhas
- Não repita senhas

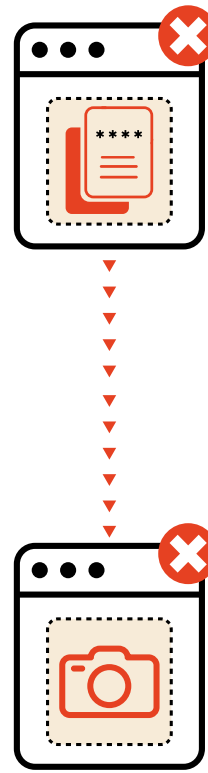


Veja mais dicas no fascículo “Autenticação”.

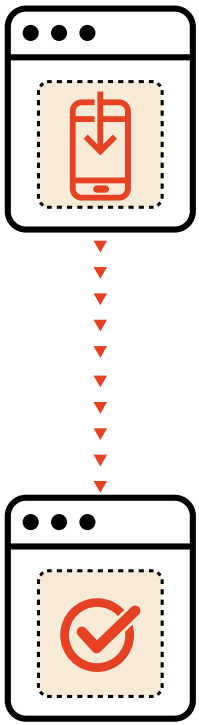
NÃO GRAVE SENHAS DE SERVIÇOS FINANCEIROS NO CELULAR

Senhas gravadas no celular podem ser encontradas por ladrões usando os mecanismos de busca disponíveis no celular e nos aplicativos.

- Não salve senhas em blocos de notas, contatos ou navegador
- Não envie senhas por mensagem ou *e-mail*
- Não tire fotos de senhas



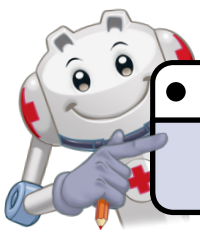
Faça buscas no seu celular pela palavra "senha", você poderá se surpreender com os resultados! É possível achar senhas em vários aplicativos e até em fotos.



INSTALE APENAS APLICATIVOS OFICIAIS

Existem aplicativos falsos que se passam por oficiais. Se instalados, podem dar acesso remoto ao dispositivo, alterar o funcionamento de outros aplicativos e enganar o usuário para que faça transferências para desconhecidos.

- Use apenas a loja oficial do sistema ou do fabricante do dispositivo
- Antes de instalar, confirme se o nome do aplicativo e do desenvolvedor estão corretos

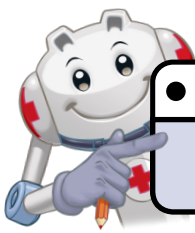


Veja mais dicas no fascículo “Celulares e *Tablets*”.

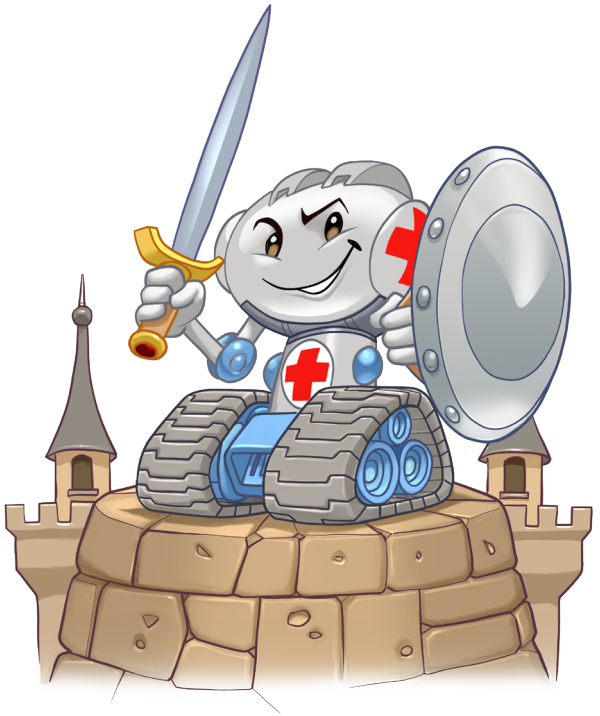
SAIBA OS CANAIS OFICIAIS DA INSTITUIÇÃO FINANCEIRA

Golpistas criam páginas e perfis falsos, e os promovem via anúncios em *sites* de busca, redes sociais e aplicativos de mensagens. Você pode acabar vítima de golpes se seguir os *links* desses anúncios.

- Acesse o *site* oficial digitando o endereço (URL) diretamente no navegador
  - use sempre conexão segura (https)
- Salve a página nos "Favoritos" para facilitar futuros acessos
- Cheque no *site* da instituição quais são os outros canais oficiais



Veja mais dicas no fascículo "*Phishing* e Outros Golpes".



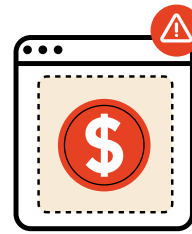
MANTENHA APLICATIVOS E SISTEMAS ATUALIZADOS

Falhas (vulnerabilidades) em aplicativos e sistemas podem ser exploradas, por exemplo, para instalar *malware*, alterar o funcionamento, furtar dados e cometer fraudes financeiras.

» Instale atualizações regularmente

- ative a atualização automática, sempre que possível

AJUSTE LIMITES PARA REDUZIR OS PREJUÍZOS FINANCEIROS



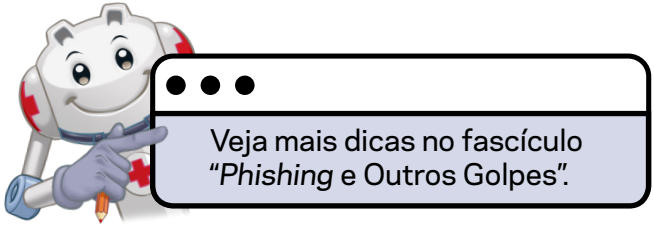
Fraudadores exploram a rapidez das transferências eletrônicas para furtar dinheiro, que nem sempre pode ser recuperado. Adequar os limites das operações ajuda a reduzir os prejuízos.

- Reduza os limites de transferências entre contas, DOC, PIX e TED
- Reavalie limites de créditos pré-aprovados

NÃO PASSE INFORMAÇÕES A PESSOAS QUE ENTRAM EM CONTATO

Instituições financeiras não contatam pessoas pedindo senhas, códigos de verificação, *tokens*, códigos QR, dados de cartão ou outras informações pessoais. Apenas solicitam dados para confirmação de identidade quando o cliente acessa os canais oficiais.

» Encerre a comunicação e, em caso de dúvida, contate a instituição através dos canais oficiais



Veja mais dicas no fascículo "*Phishing* e Outros Golpes".

ACOMPANHE SUAS TRANSAÇÕES FINANCEIRAS E AJA RAPIDAMENTE

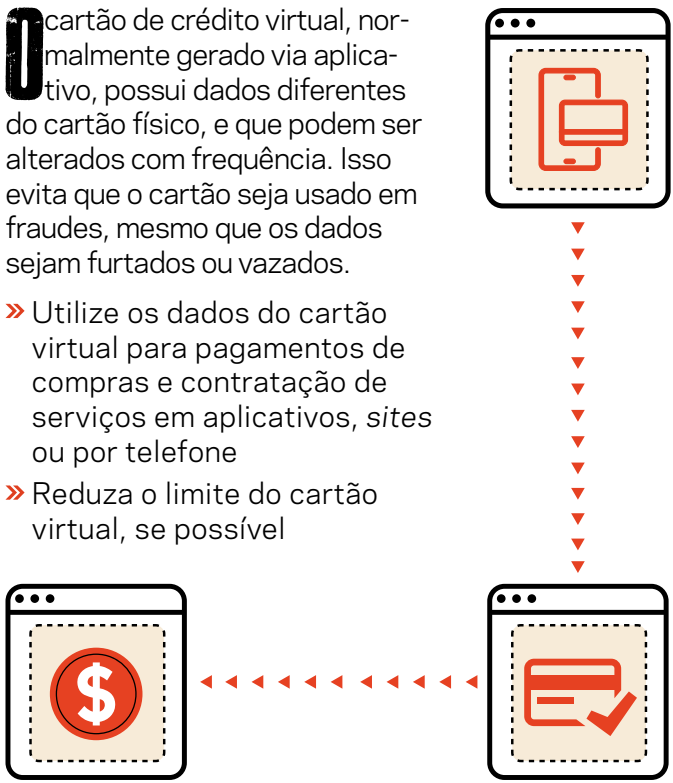
Acompanhar alertas e notificações de transações financeiras permite descobrir movimentações irregulares e agir rapidamente para conter fraudes e prejuízos.

- » Ative alertas e notificações de movimentações em suas contas e cartões de crédito
- » Analise periodicamente notificações e extratos
  - ▪ conteste rapidamente transações irregulares

USE CARTÕES DE CRÉDITO VIRTUAIS PARA PAGAMENTOS NÃO PRESENCIAIS

O cartão de crédito virtual, normalmente gerado via aplicativo, possui dados diferentes do cartão físico, e que podem ser alterados com frequência. Isso evita que o cartão seja usado em fraudes, mesmo que os dados sejam furtados ou vazados.

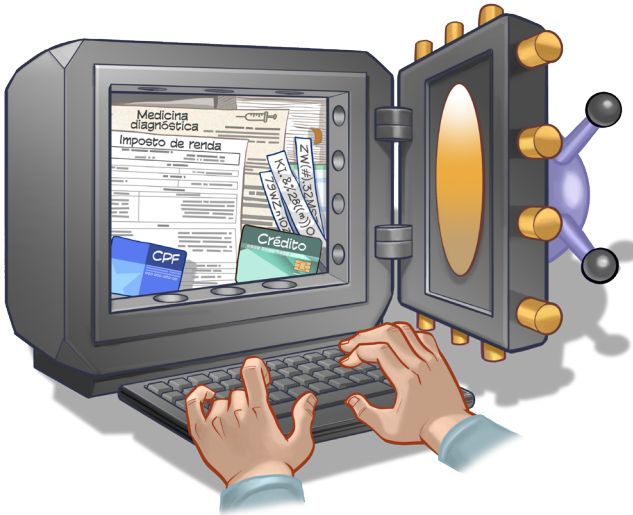
- Utilize os dados do cartão virtual para pagamentos de compras e contratação de serviços em aplicativos, *sites* ou por telefone
- Reduza o limite do cartão virtual, se possível



EXIJA AUTENTICAÇÃO PARA PAGAMENTOS COM CARTEIRAS DIGITAIS

Carteiras digitais, como Apple Wallet e Google Wallet, oferecem opções de pagamentos *online* e por aproximação. Se a carteira não exigir autenticação antes de efetuar a transação, você pode se tornar vítima de golpes ou realizar compras acidentais.

- Escolha um mecanismo de autenticação para realizar pagamentos
- Em pagamentos por aproximação, confira os dados no visor da máquina de cartão antes de aproximar o celular



COMPARTILHE DADOS APENAS COM INSTITUIÇÕES AUTORIZADAS

Compartilhar dados financeiros com instituições que não são autorizadas pelo Banco Central pode comprometer suas finanças e sua privacidade. Prefira usar o Sistema Financeiro Aberto (Open Finance).

» Use aplicativos e *sites* apenas das instituições participantes do Open Finance
https://openfinancebrasil.org.br/

NÃO DIVULGUE INFORMAÇÕES FINANCEIRAS

Divulgar informações financeiras, especialmente em redes sociais, facilita a ação de golpistas.

» Não poste fotos de cartões de crédito ou débito, senhas, pontuação (*score*) de crédito, etc.

TENHA UM E-MAIL SEPARADO PARA INSTITUIÇÕES FINANCEIRAS

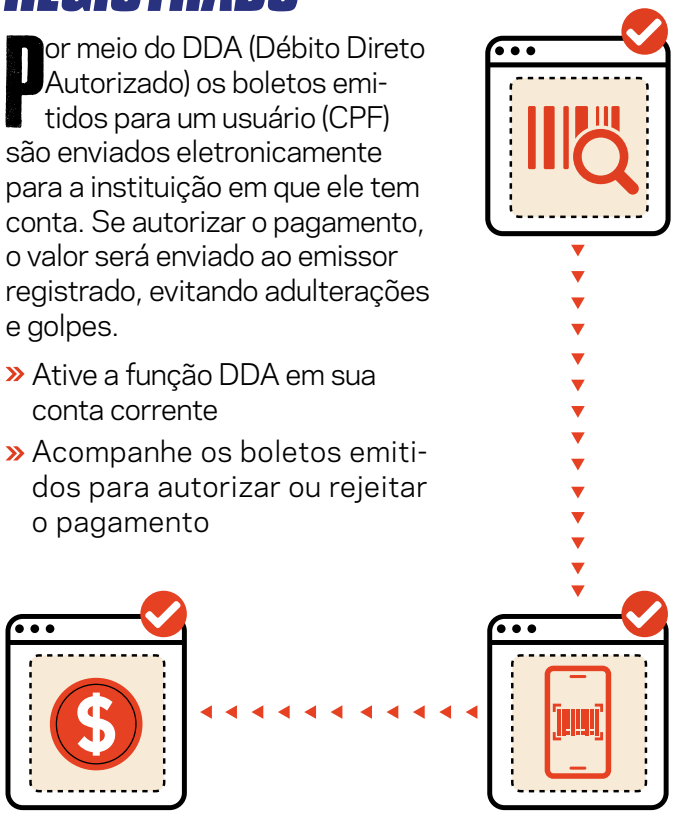
Para invadir contas financeiras, golpistas exploram mecanismos de recuperação de senha em que um *link* ou código é enviado ao *e-mail* cadastrado. Se a conta de *e-mail* estiver logada em um celular furtado, o golpista conseguirá o acesso.

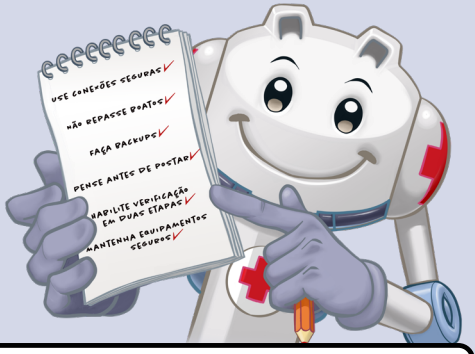
- Crie um *e-mail* exclusivo para cadastro em instituições financeiras
- Não deixe este *e-mail* logado em aplicativos ou navegador do celular
- Acesse-o regularmente para verificar notificações de *login* e comunicações enviadas pelas instituições financeiras

USE BOLETO ELETRÔNICO REGISTRADO

Por meio do DDA (Débito Direto Autorizado) os boletos emitidos para um usuário (CPF) são enviados eletronicamente para a instituição em que ele tem conta. Se autorizar o pagamento, o valor será enviado ao emissor registrado, evitando adulterações e golpes.

- Ative a função DDA em sua conta corrente
- Acompanhe os boletos emitidos para autorizar ou rejeitar o pagamento





SAIBA MAIS

- Para mais detalhes sobre este e outros assuntos relacionados com cuidados na Internet, consulte os demais Fascículos da Cartilha de Segurança para Internet, disponíveis em: **https://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: **https://internetsegura.br/**

cert.br

O CERT.br **(https://cert.br/)** é um Grupo de Resposta a Incidentes de Segurança (CSIRT) de responsabilidade nacional de último recurso, mantido pelo NIC.br. Além da gestão de incidentes, também atua na conscientização sobre os problemas de segurança, na consciência situacional e transferência de conhecimento, sempre respaldado por forte integração com as comunidades nacional e internacional de CSIRTs.

nic.br

O Núcleo de Informação e Coordenação do Ponto BR - NIC.br **(https://nic.br/)** é uma entidade civil de direito privado e sem fins de lucro, encarregada da operação do domínio .br, bem como da distribuição de números IP e do registro de Sistemas Autônomos no País. Conduz ações e projetos que trazem benefícios à infraestrutura da Internet no Brasil.

cgi.br

O Comitê Gestor da Internet no Brasil **(https://cgi.br/)**, 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.

https://cartilha.cert.br/cc/

abril / 2023