Publicação cert.br

Cartilha de Segurança para Internet

Fascículo Internet Banking

https://cartilha.cert.br/

nic.br

cgi.br

Via *Internet Banking* você pode realizar as mesmas ações disponíveis nas agências bancárias, sem enfrentar filas ou ficar restrito aos horários de atendimento

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

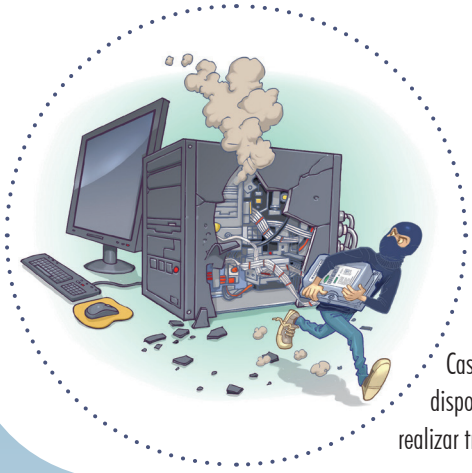
Como não é uma tarefa simples fraudar dados em um servidor de uma instituição bancária ou comercial, os golpistas procuram enganar e persuadir as potenciais vítimas a fornecerem informações sensíveis ou a realizarem ações, como executar códigos maliciosos e acessar páginas falsas (*phishing*). Para isso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

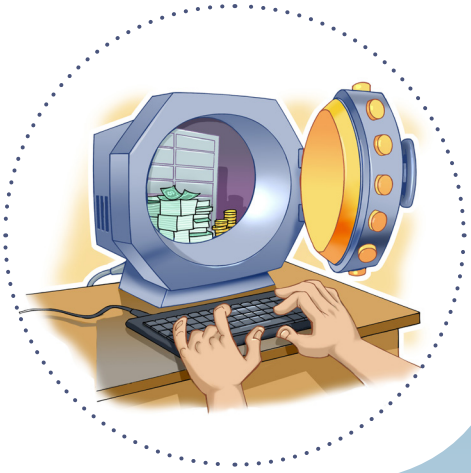


Riscos *principais*

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
- ✓ **invasão de privacidade**
  - alguém que tenha acesso indevido a sua conta pode obter informações pessoais sobre suas transações bancárias e assim expor sua privacidade
- ✓ **violação de sigilo bancário**
  - o sigilo bancário é um direito seu, que pode ser violado caso alguém acesse indevidamente sua conta
- ✓ **participação em esquemas de fraude**
  - sua conta bancária pode ser usada como intermediária para aplicar golpes e cometer fraudes

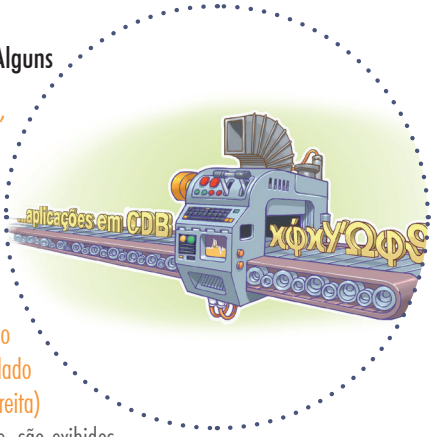
Cuidados
a serem tomados



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:

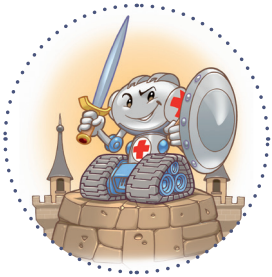
- ✓ entre imediatamente em contato com a central de relacionamento do seu banco, diretamente com o seu gerente ou com a operadora do seu cartão de crédito

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



Consulte a **Cartilha de Segurança** para a Internet para mais detalhes sobre os cuidados a serem tomados ao utilizar seu *Internet Banking*:

https://cartilha.cert.br/uso-seguro/

INTERNET SEGURA.BR

Precisa conversar sobre o uso seguro da Internet com **crianças e adolescentes**? O **Portal Internet Segura** apresenta uma série de iniciativas e de recomendações sobre esse assunto, confira!
http://internetsegura.br/

cert.br
Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil

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 https://www.cert.br/.

nic.br
Núcleo de Informação e Coordenação do Ponto BR

O Núcleo de Informação e Coordenação do Ponto BR - NIC.br (http://www.nic.br/) é uma entidade civil, sem fins lucrativos, que implementa as decisões e projetos do Comitê Gestor da Internet no Brasil. São atividades permanentes do NIC.br coordenar o registro de nomes de domínio - Registro.br (http://www.registro.br/), estudar e tratar incidentes de segurança no Brasil - CERT.br (https://www.cert.br/), estudar e pesquisar tecnologias de redes e operações - CEPTRO.br (http://www.ceptro.br/), produzir indicadores sobre as tecnologias da informação e da comunicação - CETIC.br (http://www.cetic.br/) e abrigar o escritório do W3C no Brasil (http://www.w3c.br/).

cgi.br
Comitê Gestor da Internet no Brasil

O Comitê Gestor 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 de multilateralidade, transparência e democracia, o CGI.br representa um modelo de governança multissetorial da Internet com efetiva participação de todos os setores da sociedade nas suas decisões. Uma de suas formulações são os 10 Princípios para a Governança e Uso da Internet (http://www.cgi.br/principios). Mais informações em http://www.cgi.br/.

março / 2017