PHISHING E OUTROS GOLPES

Produção:

cert.br nic.br cgi.br

NEM TUDO NA INTERNET É CONFIÁVEL, PODE SER GOLPE!

Golpistas estão sempre criando novos truques para enganar e tirar vantagem das pessoas. Não se deixe enganar.

Veja aqui como se proteger de golpes aplicados na Internet.

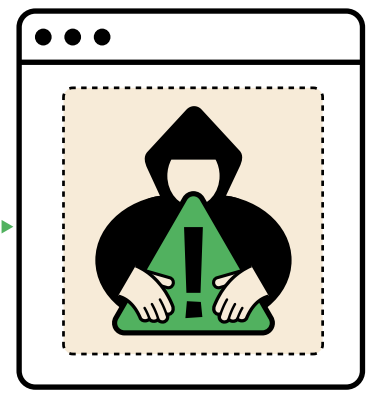
SENSO CRÍTICO É ESSENCIAL

DESCONFIE SEMPRE

Na Internet circulam informações de qualquer tipo e origem, inclusive falsas e maliciosas. Acreditar cegamente em tudo que recebe ou acessa facilita a ação de golpistas.

» Use o senso crítico: pode ser golpe!

- não é porque está na Internet ou alguém conhecido enviou, que é verdadeiro ou confiável



BUSQUE MAIS INFORMAÇÕES

É preciso desconfiar, manter a calma e checar se a mensagem que recebeu ou o conteúdo que viu na Internet são confiáveis, para não cair na lábia de golpistas.

» Informe-se

- busque a informação na fonte
- pesquise por relatos de golpes semelhantes
- converse com amigos e familiares

Veja mais dicas no fascículo "Boatos".

FIQUE ATENTO AO TOM DA MENSAGEM

Golpistas exploram os sentimentos das pessoas, como medo, obediência, caridade, carência afetiva e ganância, para convencê-las a agirem como eles querem e de forma rápida, sem pensar.

» Desconfie de mensagens contendo:

- ameaças
- oportunidades de ganho fácil
- promoções ou descontos muito grandes
- pedido de sigilo
- apelo emocional
- senso de urgência

Engenharia social é o termo usado quando uma pessoa tenta convencer outra a executar ações que a levam a fornecer informações ou seguir passos que facilitem a efetivação de golpes.

QUESTIONE SE O CONTEÚDO FAZ SENTIDO

Golpistas costumam enviar mensagens em massa com conteúdo genérico esperando que alguém "morda a isca". Questionar se o conteúdo faz sentido para você ajuda a não cair em golpes.

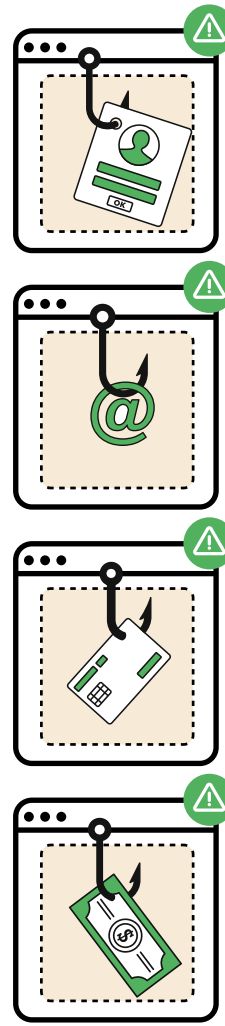
» Pergunte-se, por exemplo:
- tenho conta neste banco?
- esse é o contato que uso com esta instituição?
- o valor da cobrança confere?
- por que antecipar o pagamento e não descontar no final?

» Observe se há erros de escrita

FIQUE ATENTO A GOLPES DO DIA A DIA

Golpe comum, o *phishing* visa capturar dados dos usuários. Chega por meio de mensagens eletrônicas falando de temas que atraem a atenção dos usuários, para fazê-los acessar *links* maliciosos ou instalar *malware*.

- Suspeite de mensagens com temas cotidianos, como:
  - recadastramento de *token*
  - cancelamento de CPF
  - débitos pendentes
  - oferta de emprego
  - pontos ou bônus a vencer
- Não faça o que pede a mensagem
  - na dúvida, contate a instituição usando um canal oficial



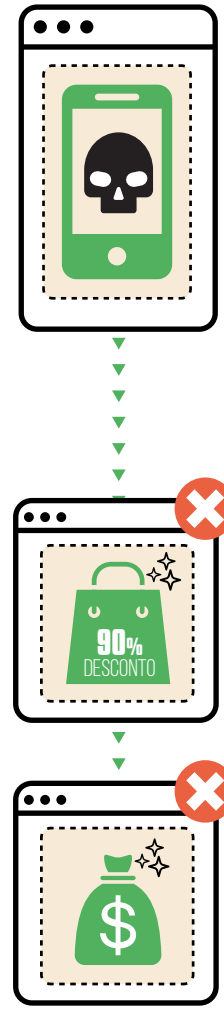
Phishing é um tipo de fraude na qual o golpista tenta obter informações pessoais e financeiras do usuário, combinando meios técnicos e engenharia social.

A palavra *phishing*, do inglês "fishing", é uma analogia criada pelos golpistas, em que "iscas" (mensagens eletrônicas) são usadas para "pescar" informações de usuários.

ATENÇÃO TAMBÉM AOS GOLPES DO MOMENTO

Para atrair vítimas, oportunistas exploram temas de destaque no momento, como Imposto de Renda, eleições, Copa do Mundo, promoções (ex: *Black Friday*) e acontecimentos que geram comoção, como desastres e doenças graves.

- Suspeite de ofertas muito vantajosas
  - lembre-se: "quando a esmola é demais, o santo desconfia"
- Busque informações somente em fontes oficiais
  - certifique-se antes de fazer pagamentos ou doações



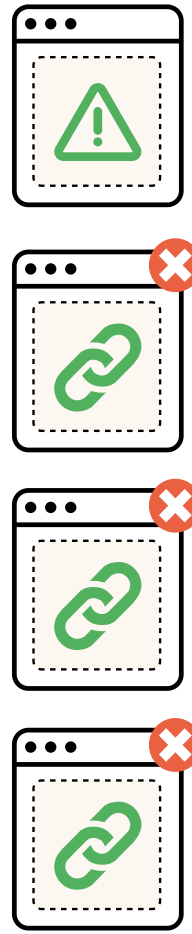
NÃO RESPONDA, DENUNCIE

Ao responder uma mensagem você confirma que sua conta está ativa. Pode ainda revelar informações e preferências que ajudam o golpista a ser mais convincente.

- Denuncie mensagens, anúncios e perfis maliciosos
  - use as opções disponibilizadas pelas plataformas
- Bloqueie números de telefone e contas que enviam mensagens maliciosas

Denunciar ajuda a remover anúncios, mensagens e perfis falsos, evitando que outras pessoas sejam vítimas.

NÃO CLIQUE EM TODOS OS LINKS QUE RECEBE



Links e códigos QR maliciosos são usados para direcionar usuários para páginas falsas ou com *malware*, a fim de capturar dados e cometer fraudes.

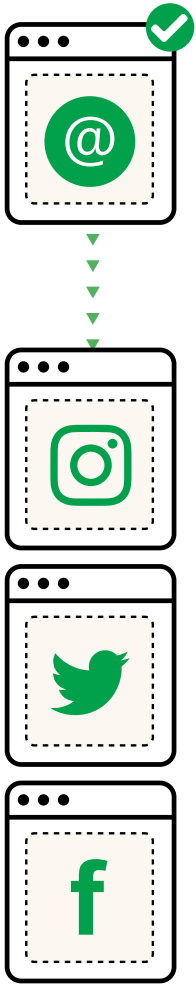
- Antes de clicar, analise o contexto e os detalhes
  - na dúvida, não clique!
- Desconfie até mesmo de mensagens enviadas por "conhecidos"
  - se necessário, contate quem supostamente a enviou usando outro meio de comunicação
- Só leia códigos QR se tiver certeza que a fonte é confiável

ACESSE O SITE OU APLICATIVO OFICIAL

Existem muitas páginas falsas e aplicativos maliciosos que tentam se passar por organizações conhecidas, como bancos, comércio eletrônico e redes sociais. É preciso tomar cuidado para somente acessar *sites* ou instalar aplicativos legítimos.

- Acesse o *site* digitando o endereço (URL) diretamente no navegador
  - se usar *sites* de busca, confirme se a URL apresentada é a correta
  - use sempre conexão segura (https)
- Instale apenas aplicativo oficial da instituição

Veja mais dicas no fascículo "Celulares e *Tablets*".



BUSQUE O PERFIL OFICIAL DAS INSTITUIÇÕES NAS REDES SOCIAIS

Ao fazer contato com instituições em redes sociais, como serviços de atendimento ao cliente, é preciso verificar se o perfil é o legítimo, para não entregar seus dados a golpistas, que criam perfis falsos.

- Confira se é o perfil oficial
- Procure pelo indicativo de "conta verificada", sempre que disponível

PROTEJA SUAS CONTAS E SENHAS

Se conseguirem suas senhas e códigos de verificação, golpistas podem invadir suas contas, furtar sua identidade e praticar fraudes em seu nome, causando prejuízos a você e a seus contatos.

- Nunca forneça senhas ou códigos de verificação
  - inclusive imagens de códigos QR
- Ative a verificação em duas etapas

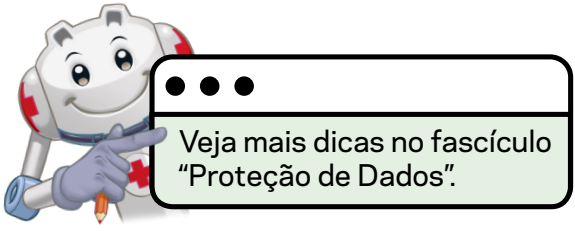
Veja mais dicas no fascículo “Autenticação”.

REDUZA A QUANTIDADE DE DADOS SOBRE VOCÊ

Quanto mais informações você divulga, mais fácil será furtar sua identidade, e mais convincente o golpista será nas abordagens. As informações também podem ser usadas para tentar adivinhar suas senhas.

» Pense bem antes de publicar algo
  - avalie o que publica e quem terá acesso

» Seja seletivo ao aceitar novos contatos



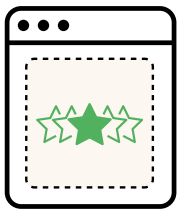
Veja mais dicas no fascículo “Proteção de Dados”.

CUIDADOS COM OPERAÇÕES BANCÁRIAS E COMPRAS ONLINE

CONFIRME A IDENTIDADE ANTES DE FAZER TRANSAÇÕES FINANCEIRAS

Golpistas exploram a confiança entre familiares e amigos pedindo empréstimos ou ajuda para pagar contas, geralmente com urgência. Usam contas invadidas ou alegam alteração de contato, como número de telefone.

- Desconfie de mensagens pedindo ajuda financeira
  - contate a pessoa por outro meio de comunicação
  - informe o ocorrido ao real dono da conta, amigos e familiares
- Confira sempre os dados do recebedor antes de efetivar transações



VERIFIQUE SE O SITE OU LOJA É CONFIÁVEL

Golpistas criam *site* falsos de comércio eletrônico com preços abaixo do mercado e enganam os clientes, que não recebem as mercadorias. Os dados fornecidos podem ainda ser usados em outras fraudes.

- Pesquise a reputação da empresa e as opiniões dos clientes
  - em redes sociais e *sites* de reclamações
  - prefira *sites* e lojas que você conheça ou tenha boas referências
- Faça uma pesquisa de mercado e desconfie se o preço estiver muito baixo

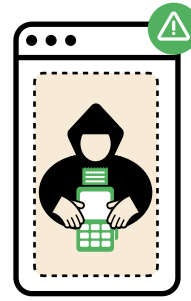
NÃO ACEITE INTERMEDIÁRIOS EM TRANSAÇÕES DE COMPRA E VENDA

Fraudadores criam anúncios falsos com valores mais baixos para atrair compradores. Se dizendo intermediários na transação, recebem o dinheiro do comprador. O real vendedor não recebe o pagamento e não faz entrega.

» Conduza toda a transação somente pela plataforma do anúncio

- suspeite de intermediário pedindo sigilo sobre valores da negociação

FAÇA PAGAMENTOS APENAS NA PLATAFORMA ORIGINAL DA COMPRA



Fraudadores alegam falha de sistema e pedem às vítimas para fazer pagamentos fora da plataforma da compra. No pagamento separado, o valor é alterado e ocultado para cobrar a mais. O cartão também pode ser clonado.

» Ao fazer compras em *sites* ou aplicativos:
  - se usar cartão de crédito, prefira o cartão virtual
  - não faça pagamentos fora da plataforma

» Ao fazer qualquer pagamento:
  - confira o valor antes de autorizar a cobrança
  - verifique o valor cobrado em sua conta e/ou cartão

O QUE FAZER SE FOR VÍTIMA DE GOLPE

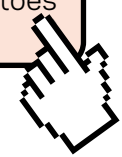
MONITORE SUA VIDA FINANCEIRA E SUA IDENTIDADE

O furto da sua identidade pode causar muitos prejuízos. Você pode ficar com dívidas em seu nome, perder reputação e crédito e ainda se envolver em processos judiciais.

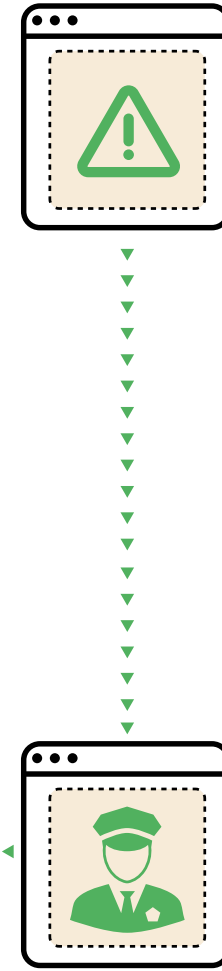
- Ative alertas e monitore extratos de cartões e contas bancárias
- Contate as instituições envolvidas
  - para esclarecer dúvidas ou contestar irregularidades
- Acompanhe seus registros financeiros junto ao Banco Central
  - busque pelo serviço "Registrato"

Sinais de furto de identidade:

- notificações de instituições de proteção ao crédito
- contas bancárias, empréstimos, cartões ou benefícios que não solicitou



FAÇA BOLETIM DE OCORRÊNCIA



O boletim de ocorrência (BO) é o registro policial que ajuda você a se defender caso seja vítima de golpe, em especial nos casos de perda financeira e de furto de identidade. É geralmente exigido para contestar fraudes e acionar seguros.

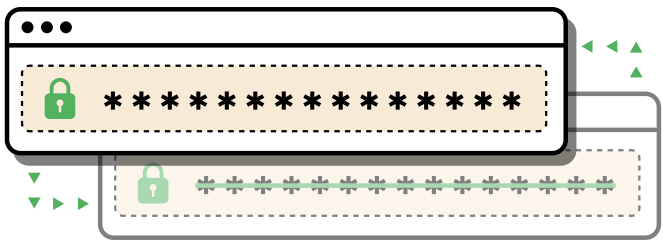
» Registre ocorrência junto à autoridade policial caso:

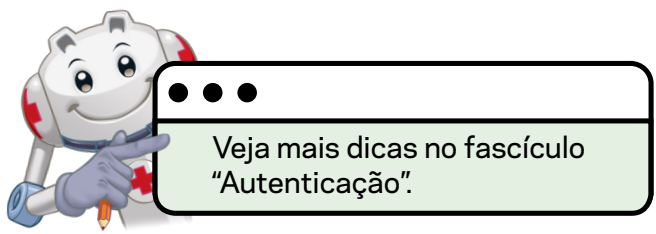
- alguém esteja se passando por você (furto de identidade)
- tenha prejuízos financeiros

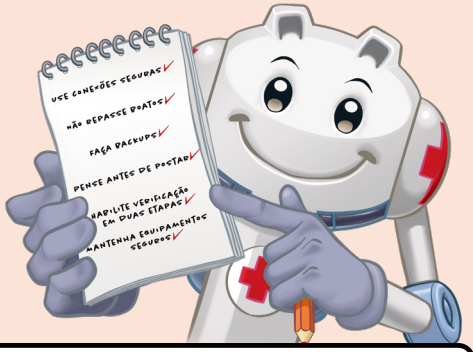
RECUPERE SUAS CONTAS E TROQUE SUAS SENHAS

Contas invadidas podem ser a porta de entrada para fraudes. Podem ser usadas para trocar senhas de outras contas, inclusive de instituições financeiras, e para aplicar golpes em seus contatos.

- Se alguma conta sua foi invadida:
  - tente trocar sua senha
  - siga os procedimentos para recuperação do acesso, se necessário
- Denuncie na plataforma se identificar perfil falso em seu nome
- Informe seus contatos







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/

dezembro / 2022