



Exército Brasileiro

**Guia de Orientação e Prevenção a
GOLPES**



***PREVENIR NOSSOS RECURSOS HUMANOS
PARA PROTEGER NOSSA FORÇA.***



Edição 2017



MENSAGEM INICIAL

Este Guia tem por finalidade orientar o público interno (militares da ativa e da reserva, pensionistas, familiares e servidores civis) contra ações de atores hostis (golpistas) ou quadrilhas.



ÍNDICE

Assunto	Pag
 Introdução	1
 Golpe da passagem aérea	2
 Golpe do bilhete premiado	3
 Golpe do falso funcionário de banco	4
 Golpe da clonagem do cartão de crédito	5
 Golpe do falso sequestro	6
 Golpe com a cópia de documento pessoal	7
 Golpe do pecúlio ou ação judicial	8
 Golpe do parente em dificuldade	9
 Golpe do familiar internado em hospital	10
 Golpe da falsa promoção em programa de TV ou empresa de telefonia	11
 Golpe do defeito na linha telefônica	12
 Golpe do empréstimo consignado	13
 Golpe da renovação do empréstimo	14
 Golpe da resolução de pendências junto aos órgãos de proteção ao crédito	15
 Golpe da pirâmide ou programa de ajuda mútua	16
 Golpe da facilitação de ingresso em escolas militares	17
 Golpes pela internet - PHISHING	18
 Golpes pela internet - ENGENHARIA SOCIAL	19
 Golpes pela internet - PHARMING	20
 Golpes no comércio eletrônico - SITES FRAUDULENTOS	21
 Golpes no comércio eletrônico - SITES DE LEILÃO E VENDA DE PRODUTOS	22
 Conclusão - Regras básicas de proteção contra golpes	23
 Conclusão - Regras básicas de proteção contra golpes na INTERNET	24
 Mensagem Final	25



INTRODUÇÃO

Diversos tipos de golpes têm sido aplicados por quadrilhas especializadas ou por golpistas isolados contra a Família Militar, com incidência nos militares da reserva e pensionistas, notadamente os idosos.

De modo geral, os criminosos evidenciam conhecimentos relevantes sobre dados pessoais das vítimas e de seus familiares, colhidos em contatos fortuitos ou pelas redes sociais, o que tem facilitado a ação hostil.

As chances de sucesso de um golpe serão maiores se o golpista obtiver êxito em explorar a falta de informação ou a ambição da vítima.

Assim, o presente Guia de Orientação e Prevenção a Golpes foi atualizado com o objetivo de preparar a Família Militar quanto às diversas modalidades de golpes, bem como propor medidas de segurança para salvaguardar os nossos Recursos Humanos, o público interno.

GOLPE DA PASSAGEM AÉREA

ESTELIONATÁRIO

Vende uma **passagem aérea por um preço muito abaixo do praticado pelo mercado**, alegando ser fruto de bônus de cartão de milhagem.



VÍTIMA

Compra a passagem e, no momento do embarque, ocasião em que é solicitada a identidade, é notificada que a **passagem foi adquirida de forma ilícita**, sendo impedida de realizar a viagem e acusada de conluio no golpe.

DICAS DE PREVENÇÃO

- Não acreditar em ofertas muito generosas, principalmente vindo de pessoas estranhas.
- Somente comprar passagens de companhias aéreas ou agências de turismo comprovadamente legais.

GOLPE DO BILHETE PREMIADO

ESTELIONATÁRIO

Por meio de abordagem fortuita no meio da rua, trajando roupas simples e dizendo ser de fora da cidade, afirma para a vítima que está de posse de bilhete de loteria premiado, mas tem que viajar imediatamente, ficando impossibilitado de esperar para resgatar o prêmio.

Dessa forma, o criminoso procura convencer a vítima a comprar o bilhete.



DICAS DE PREVENÇÃO

- Ter em mente que dinheiro fácil não existe.
- Desconfiar de pessoas estranhas com ofertas muito generosas.





GOLPE DO FALSO FUNCIONÁRIO DE BANCO

4

ESTELIONATÁRIO/LADRÃO

Em filas de caixas eletrônicos, particularmente nos destinados a depósitos bancários, o criminoso se passa por funcionário do banco e organiza a fila de espera dos clientes.



Em seguida, recolhe dos clientes as guias de depósito com dinheiro, pedindo que aguardem o recibo por alguns instantes, saindo rapidamente do local, levando o dinheiro das vítimas.



DICAS DE PREVENÇÃO

- Manter sigilo sobre a senha da conta bancária.
- Não aceitar ajuda de estranhos em agências bancárias.
- Se for necessário solicitar ou aceitar auxílio, confirmar quem é o funcionário do banco à disposição.



GOLPE DA CLONAGEM DO CARTÃO DE CRÉDITO

5

Trabalhando em estabelecimento comercial, o golpista utiliza uma máquina leitora de cartão com mecanismo de cópia de dados, chamado vulgarmente de “Chupa-Cabra”.

Quando a vítima entrega seu cartão para efetuar o pagamento, o golpista o insere nessa máquina e, após o cliente digitar sua senha, diz que a máquina está com dificuldade de acesso e passa o cartão em outra máquina, efetuando o pagamento.

Os dados do cartão são gravados pela primeira máquina, inclusive a senha da vítima, possibilitando a clonagem do cartão para utilização em diversas transações ilícitas (compras, pagamentos etc).

Esse golpe poderá ocorrer, também, em caixas eletrônicos, utilizando dispositivos para leitura dos dados do seu cartão.



DICAS DE PREVENÇÃO

- Se a máquina leitora de cartão não funcionar e for necessária a sua troca, solicitar a presença do responsável pelo estabelecimento e anotar a ocorrência para, se for o caso, registrar em uma delegacia.
- Cadastrar o seu celular junto ao banco, para receber mensagens SMS, avisando sobre todos os movimentos financeiros na conta bancária ou cartão de crédito.



GOLPE DO FALSO SEQUESTRO

6

FALSO SEQUESTRADOR



Telefona para a vítima e diz que sequestrou algum parente dela.

Exige, para o resgate, que uma quantia em dinheiro seja depositada em uma conta corrente por ele indicada.

PROÍBE A VÍTIMA DE INTERROMPER A LIGAÇÃO

Ação não comum de sequestrador verdadeiro



DICAS DE PREVENÇÃO

- Orientar todas as pessoas da casa a não fornecerem dados pessoais, sobretudo por telefone ou pelas redes sociais. São essas informações que os meliantes usam para dar mais credibilidade aos golpes.
- Antes de qualquer atitude, procurar ajuda de alguém que não esteja envolvido emocionalmente com o caso.



GOLPE COM A CÓPIA DE DOCUMENTO PESSOAL

7

O golpe é aplicado utilizando-se cópia de algum documento pessoal.

Na maioria das instituições ou estabelecimentos comerciais que concedem crédito, é necessária a apresentação da cópia de vários documentos como, por exemplo, a identidade militar.



Nestas ocasiões, a cópia de algum documento pessoal da vítima pode ser furtada ou extraviada, vindo a ser utilizada por golpistas para uso indevido, como por exemplo, para realizar empréstimos em instituições bancárias.

DICAS DE PREVENÇÃO

➤ Quando entregar cópia de documentos em alguma instituição ou estabelecimento comercial, inserir duas linhas sobre o documento e escrever a finalidade daquela cópia.



GOLPE DO PECÚLIO OU AÇÃO JUDICIAL

8

ESTELIONATÁRIO

Passando-se por funcionário de associação, empresa de previdência privada, advogado, representante jurídico de grupo de inativos e pensionistas ou por Oficial do Exército, telefona para a vítima, normalmente militar da reserva, informando sobre suposto saldo de pecúlio, ou valores financeiros decorrentes de ação judicial coletiva a receber, oferecendo o saque imediato.



VÍTIMA

Para receber o suposto pecúlio, deposita em conta indicada pelo estelionatário, quantia correspondente aos custos administrativos ou processuais.

Por estar de posse de dados pessoais e bancários da vítima, o estelionatário deposita na conta corrente um cheque furtado/roubado, que fica bloqueado por mais de 24 horas e depois é sustado.

DICAS DE PREVENÇÃO

- Não fornecer ou confirmar seus dados a estranhos. Trate de assuntos financeiros em instituições credenciadas e, de preferência, pessoalmente.
- Por mais animadora que seja a notícia de receber uma razoável quantia em dinheiro, não se deixe enganar. A prática judicial não prevê ligações para comunicar êxito em ações na justiça.

ESTELIONATÁRIO

Passando-se por um parente ou militar (da ativa ou reserva) relata estar vivenciando algum tipo de dificuldade.



Em seguida, pede por telefone que a vítima deposite uma quantidade de dinheiro para socorrê-lo.



DICAS DE PREVENÇÃO

- Não tratar de assuntos financeiros ao telefone.
- Desligar o telefone e ligar para a pessoa conhecida.
- Não depositar dinheiro na conta de desconhecidos.



GOLPE DO FAMILIAR INTERNADO EM HOSPITAL

10

GOLPISTA

Telefona para familiares de paciente internado em hospital e, se passando por médico, diz que é necessário realizar um depósito bancário, numa conta fornecida por ele, para a liberação de exames ou realização de cirurgias urgentes.



Após a realização do depósito, o golpista transfere ou saca o dinheiro, deixando a vítima no prejuízo.

DICAS DE PREVENÇÃO

- Desconfiar de qualquer ligação solicitando depósito para essas finalidades.
- Ir até a administração ou ouvidoria do hospital para ter certeza de que não está sendo vítima deste golpe.



GOLPE DA FALSA PROMOÇÃO EM PROGRAMA DE TV OU EMPRESA DE TELEFONIA

11

ESTELIONATÁRIO

Dizendo ser representante de um determinado programa de TV ou funcionário de empresa de Telefonia, faz contato com a vítima informando que ela foi sorteada e tem prêmios a receber ou foi selecionada para participar de uma promoção.



No entanto, para validar a ação, a vítima deve comprar cartões de recarga de celular e repassar o código para o estelionatário.

DICAS DE PREVENÇÃO

- Ter em mente que ninguém dá dinheiro de graça. Além disso, as empresas de TV só distribuem prêmios para quem se cadastra.
- Cabe ressaltar, também, que as empresas telefônicas não ligam para a residência dos clientes, condicionando a participação em promoções à aquisição de cartões de recarga.

GOLPE DO DEFEITO NA LINHA TELEFÔNICA

ESTELIONATÁRIO

Passando-se por funcionário da empresa concessionária de telefonia, liga para o celular da vítima dizendo que foi detectado um defeito naquele aparelho e solicita que a pessoa digite um número por ele fornecido.



Com esta simples ação, o criminoso clona o número da linha e a utiliza de forma indiscriminada, realizando ligações interurbanas e internacionais.

DICAS DE PREVENÇÃO

- Ter em mente que as empresas telefônicas não ligam para os celulares dos clientes solicitando que sejam digitados números no aparelho, a fim de solucionarem possíveis falhas ou defeitos.



GOLPE DO EMPRÉSTIMO CONSIGNADO

13

A vítima vai a uma empresa que oferece empréstimos consignados, motivada por propaganda realizada por meios diversos, e o atendente faz um cadastro dela na página do Centro de Pagamento do Exército (CPEX), para obter o acesso ao contracheque e em consequência à sua margem consignável.

Por ocasião do cadastro, que requer o fornecimento de um e-mail para situações diversas, o atendente disponibiliza o e-mail da empresa. Após a visita da vítima, a empresa utiliza a ferramenta **“esqueci minha senha”** e o programa envia a nova senha para o e-mail cadastrado, que é o da empresa.

De posse da nova senha da vítima, junto ao CPEX, o que permite o acesso à sua margem consignável, os criminosos terão facilidade em obter empréstimos pessoais, em nome da vítima, junto às instituições financeiras.

DICAS DE PREVENÇÃO

- Nunca deixar que pessoas estranhas preencham cadastros em seu nome, criem senhas para você ou disponibilizem e-mail que não são seus, possibilitando assim, o acesso aos seus dados pessoais.





GOLPE DA RENOVAÇÃO DO EMPRÉSTIMO

14

ESTELIONATÁRIO

Liga para a vítima, passando-se por um representante de instituição financeira, oferecendo renovação de empréstimo com juros menores. Para isso, solicita o identificador da margem consignável do contracheque da vítima.

Em seguida, é realizado o depósito de um valor considerável na conta corrente da vítima. Ato contínuo, liga novamente para a vítima dizendo que o valor depositado tratava-se de equívoco e solicita a devolução de parte do valor em uma conta corrente por ele indicada.

No mês seguinte a vítima é surpreendida com o desconto em contracheque da 1ª parcela de empréstimo (feito em seu nome pelo estelionatário de posse de seu identificador da margem consignável).



DICAS DE PREVENÇÃO

- Jamais informar o identificador da margem consignável por telefone e desconfiar de qualquer depósito bancário não programado.
- Procure seu gerente de conta.



GOLPE DA RESOLUÇÃO DE PENDÊNCIAS JUNTO AOS ÓRGÃOS DE PROTEÇÃO AO CRÉDITO

15

A vítima recebe uma correspondência supostamente de Cartório de Títulos e Documentos e Pessoas Jurídicas.



A correspondência sugere que a vítima está negativada junto aos órgãos de proteção ao crédito, possui pendência em alguma instituição bancária e que essa pendência foi protestada e registrada em Cartório.

Juntamente com a correspondência, é enviado, anexo, um boleto bancário para quitação da suposta dívida.

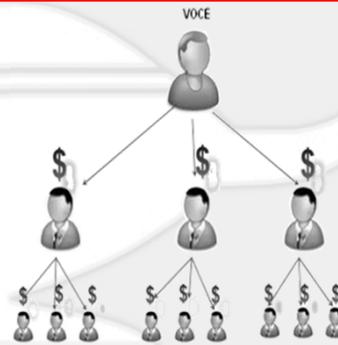
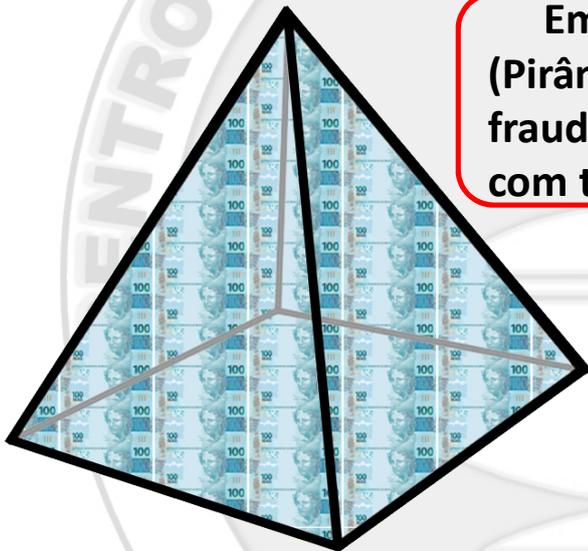
DICAS DE PREVENÇÃO

- Confirmar, junto ao banco e órgãos de proteção ao crédito, toda informação recebida por meio de correspondência.

Genericamente, consiste em um sistema, fraudulento, usado para coletar dinheiro ou benefícios por meio de um fluxo, supostamente “sem fim”, de novos participantes ou “recrutas”.

A função de cada novo participante é, sistematicamente, dar dinheiro para os golpistas/recrutadores e cooptar novos participantes para o esquema.

Em uma variante desse esquema (Pirâmide do Tipo Ponzi), os criadores da fraude costumam manter contato direto com todos os envolvidos.



DICAS DE PREVENÇÃO

➤ AS PIRÂMIDES CONSTITUEM CRIME CONTRA A ECONOMIA POPULAR PREVISTO NO ART 2º, IX DA LEI Nr 1.521/51: “IX – obter ou tentar obter ganhos ilícitos em detrimento do povo ou de número indeterminado de pessoas mediante especulações ou processos fraudulentos.”



GOLPE DA FACILITAÇÃO DE INGRESSO EM ESCOLAS MILITARES

17

ESTELIONATÁRIO

Apresenta-se, geralmente em escolas, prometendo facilitar o ingresso de jovens e adolescentes nos Estabelecimentos de Ensino Militar. Para ganhar credibilidade, levam militares fardados ou se fardam indevidamente.

Alegam que possuem ligação com as Escolas de Formação Militar e prometem facilitar o ingresso em carreiras militares, mediante pagamento de uma taxa de material de estudo e/ou matrícula em curso preparatório.

Em muitos casos, após receber valores das vítimas, os golpistas desaparecem.

DICAS DE PREVENÇÃO

- As Escolas Militares do Exército não possuem vínculo com cursos preparatórios. O ingresso nessas Escolas só é possível por meio de concurso público.
- Os interessados em ingressar em alguma carreira militar devem buscar informações nos sites do Exército e das Escolas de Formação Militar, bem como nos editais de concursos publicados nos diversos meios de comunicação.



GOLPES PELA INTERNET *PHISHING*

18

GOLPISTAS

Entram em contato com a vítima, na maioria das vezes por e-mail, passando-se por um representante de instituição conhecida (banco, empresa ou um *site* de ajuda humanitária).



Ao clicar em algum link ou ao abrir algum arquivo executável (extensão.exe) do e-mail ou da página indicada, é instalado no computador da vítima um arquivo conhecido por “Trojan” (Cavalo de Tróia).



Esses “Trojans” são capazes de capturar suas senhas, números de cartões e até mesmo alterar o endereço de destino do seu provedor de Internet, programando o discador para se conectar em outro provedor não solicitado.

DICAS DE PREVENÇÃO

Para prevenir, **FIQUE ATENTO** com ...

- E-mail com links para baixar e abrir/executar arquivos.
- Mensagem eletrônica com formulários para preenchimento de dados pessoais e financeiros.
- E-mail com aviso judicial, promoção de programa de milhagem de companhias aéreas, álbuns de fotos/vídeos, serviço de proteção de crédito e da Receita Federal.

GOLPISTAS

Exploram fragilidades pessoais, desconhecimento e falta de atenção com medidas de segurança pessoais, por parte dos usuários.

Utilizam técnicas de ENGENHARIA SOCIAL, por diferentes *meios e discursos*, procurando enganar e persuadir as vítimas a executarem ações que exponham informações pessoais e sensíveis.



**APÓS A OBTENÇÃO DOS DADOS,
O QUE FAZEM OS GOLPISTAS?**



- Efetuam transações financeiras
- Acessam sites
- Envia mensagens eletrônicas
- Criam empresas fantasmas
- Criam contas bancárias ilegítimas

DICAS DE PREVENÇÃO

➤ Muito cuidado ao fornecer dados pessoais, mesmo para conhecidos. Procure saber, sempre, o motivo do fornecimento desses dados.

Envolve o redirecionamento da navegação do usuário para *sites* falsos.

Quando a vítima tenta acessar um *site* legítimo, o seu navegador *Web* é redirecionado para uma página falsa.



COMO SABER SE O SITE É FALSO?

- Desconfiar se, ao digitar uma URL (WWW....), for redirecionado para outro *site*, que sugira abrir um arquivo ou a instalação de um programa;
- Desconfiar se o *site* de comércio eletrônico ou *Internet Banking* não estiver utilizando conexão segura (exemplo – https).
- Observar se o certificado apresentado corresponde ao do *site* verdadeiro.



GOLPES NO COMÉRCIO ELETRÔNICO SITES FRAUDULENTOS

21

GOLPISTAS

Criam um site fraudulento com o objetivo de enganar clientes (vítimas) que, após efetuarem os pagamentos, não recebem as mercadorias correspondentes.

Costumam utilizar artifícios como: enviar *spam*, fazer propaganda via *links* patrocinados, anunciar descontos em sites de compras coletivas e ofertar produtos muito procurados e com preços abaixo dos praticados pelo mercado.

DICAS DE PREVENÇÃO

- Comparar o preço do produto exposto no site com os valores de mercado.
- Pesquisar na internet sobre o site, antes de efetuar a compra.
- Verificar se há reclamações referentes ao site em fóruns de compradores.
- Ter cuidado com propagandas recebidas por meio de *spam*.
- Procurar validar os dados de cadastro da empresa no site da Receita Federal.



GOLPES NO COMÉRCIO ELETRÔNICO SITES DE LEILÃO E VENDA DE PRODUTOS

22

GOLPISTA

Como comprador ou vendedor, age de má fé e não cumpre com as obrigações acordadas ou utiliza os dados pessoais e financeiros dos envolvidos na transação comercial para outros fins.

Normalmente, envia e-mails falsos, em nome do sistema de gerenciamento de pagamentos, como forma de fingir comprovar a realização do pagamento ou o envio da mercadoria que, na realidade, não foi realizado.

DICAS DE PREVENÇÃO

- Não confiar apenas, faça pesquisa de mercado e desconfie caso o produto esteja com valor muito baixo.
- Não confiar em e-mails recebidos, referentes a assuntos financeiros ou comerciais, pois podem ser falsos.
- Acessar *sites* diretamente do navegador, sem clicar em *links* recebidos em mensagens.
- Efetuar pagamentos pessoalmente, por meio de boletos bancários.



CONCLUSÃO

REGRAS BÁSICAS DE PROTEÇÃO CONTRA GOLPES

- 1.** Nunca aceite ajuda de estranhos, especialmente em bancos.
- 2.** Não forneça ou confirme dados particulares por telefone, pois você não sabe quem está do outro lado da linha. Oriente seus familiares e sua empregada doméstica a respeito.
- 3.** Cuidado com sua documentação pessoal.
- 4.** Desconfie de ofertas generosas.
- 5.** Procure tratar pessoalmente de assuntos com as instituições financeiras credenciadas.
- 6.** Não seja ingênuo. Dinheiro fácil não existe. Seja prudente quando tratar de assuntos financeiros.
- 7.** Nunca deposite dinheiro na conta de desconhecidos.
- 8.** Controle sua ambição.
- 9.** Nunca guarde o cartão e a senha no mesmo lugar.
- 10.** Evite senhas fáceis ou ligadas a dados pessoais (datas especiais, iniciais dos nomes e sobrenomes, locais de nascimento e etc.)



CONCLUSÃO

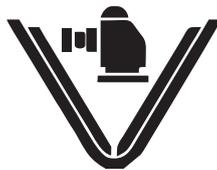
REGRAS BÁSICAS DE PROTEÇÃO CONTRA GOLPES NA INTERNET

1. Desconfiar se, ao digitar uma URL (WWW...), for redirecionado para outro *site*, que sugira abrir um arquivo ou a instalação de um programa;
2. Desconfiar se o *site* de comércio eletrônico ou *Internet Banking* não estiver utilizando conexão segura (exemplo - https).
3. Observar se o certificado apresentado corresponde ao do *site* verdadeiro.
4. Ao realizar compras pela internet
 - a. Comparar o preço do produto exposto no site com os valores de mercado.
 - b. Pesquisar na internet sobre o site, antes de efetuar a compra.
 - c. Verificar se há reclamações referentes ao site em fóruns de compradores
 - d. Ter cuidado com propagandas recebidas por meio de spam.
 - e. Procurar validar os dados de cadastro da empresa no site da Receita Federal.



MENSAGEM FINAL

Nunca acredite em pessoas estranhas com propostas muito vantajosas. As instituições financeiras, as seções de inativos e pensionistas e outras organizações não enviam funcionários à residência de ninguém, solicitando qualquer tipo de recurso ou valor em dinheiro.



EGGCF

Desde 1949

"Gráfica do Exército" - Compromisso com a Qualidade

Impresso no EGGCF - "Gráfica do Exército"

Al. Mal. Rondon -Setor de Garagens- QGEx- SMU - CEP:70630-901 - Brasília - DF

Tel: 3415-4248- RITEX: 860-4248 - Fax: 3415-5829

Site: <http://www.eggcf.eb.mil.br> - E-mail: divcom@eggcf.eb.mil.br



PREVENIR, ORIENTAR E PROTEGER.

