EXÉRCITO BRASILEIRO

Guia de Orientação e Prevenção a

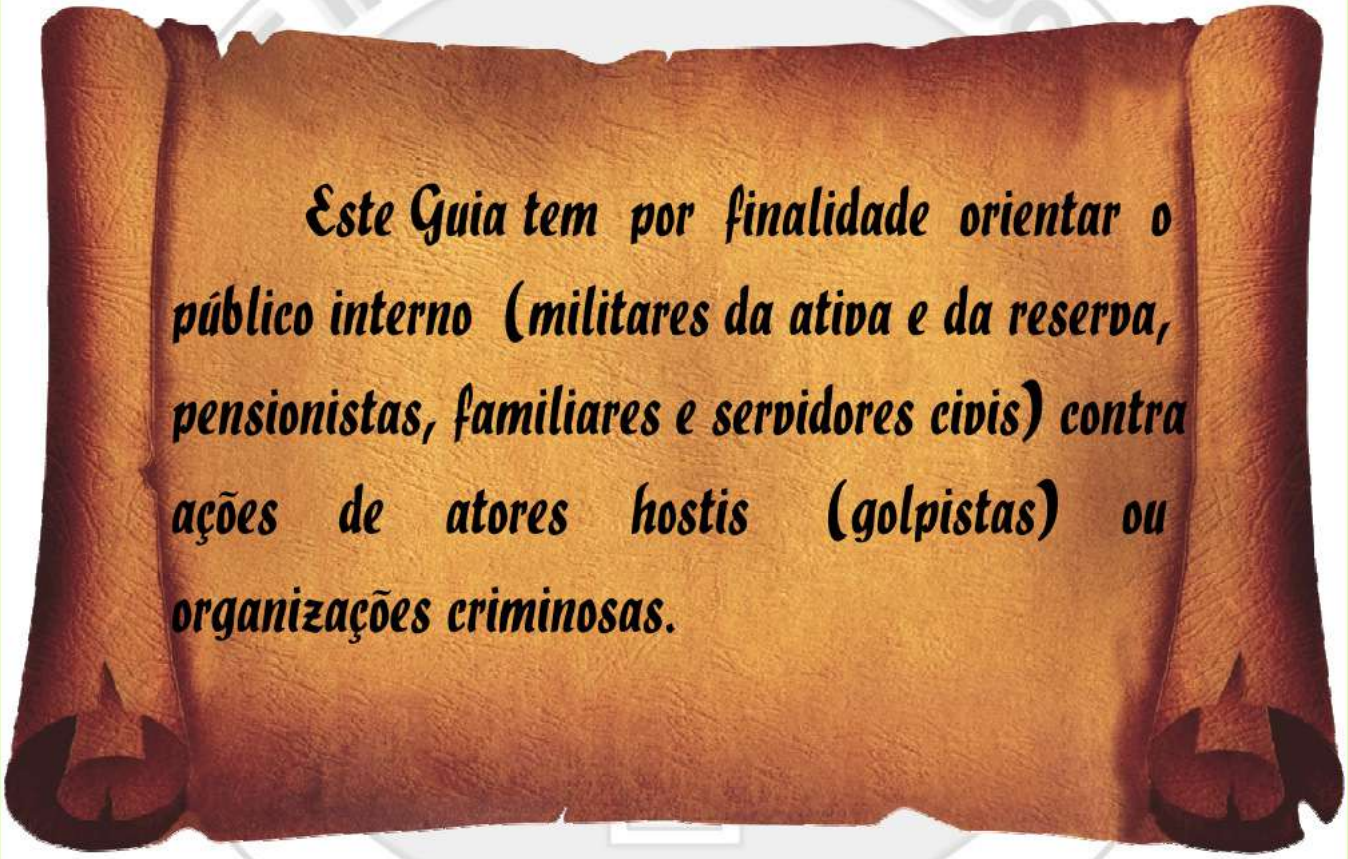
GOLPES

Prevenir a família militar

CENTRO DE INTELIGÊNCIA DO EXÉRCITO
BRASIL

Edição 2021

MENSAGEM INICIAL



ÍNDICE

INTRODUÇÃO

Diversos golpes são aplicados de forma criminosa contra a família militar, com maior incidência nos militares da reserva e pensionistas, notadamente os idosos.

Os recentes vazamentos de dados pessoais no Brasil tornam ainda mais provável a continuidade da aplicação de golpes.

De modo geral, os criminosos evidenciam conhecimentos relevantes sobre os dados pessoais das vítimas e de seus familiares, decorrentes de vazamentos ou colhidos por meio de engenharia social (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 o ativo mais valioso da Força.

GOLPE DE CLONAGEM DA CONTA DE WHATSAPP

CRIMINOSO VIRTUAL

Liga para o celular da pessoa ou envia uma mensagem se passando por funcionário de site ou de compra e diz que estaria enviando um código promocional ou de confirmação.

Pede então que informe esse código que, na verdade, é a verificação do WhatsApp. Dessa forma, **consegue clonar a conta da vítima**.

- **Assume a conta da vítima.**
- **Acessa todos os dados armazenados no aplicativo, inclusive a lista de contatos.**
- **Manda mensagens para os contatos do aplicativo com apelos de ajuda financeira.**

VÍTIMA

Ao informar o código, perde todo o controle sobre do aplicativo de WhatsApp.

DICAS DE PREVENÇÃO

1. Ative a "Verificação em duas etapas" no aplicativo de mensagem instântanea.
2. NUNCA forneça o código verificador recebido por SMS ou por e-mail.
3. NUNCA instale apps de terceiros ou compartilhe informações pessoais a pedido de ninguém por aplicativos.
4. Desconfie de situações em que a pessoa solicita a realização de transferências ou pagamentos de urgência.
5. NUNCA instale apps de terceiros ou compartilhe informações pessoais a pedido de ninguém por aplicativos.
6. ALERTE, imediatamente, a sua rede de contatos sobre a clonagem de seu aplicativo para evitar possíveis golpes.

GOLPE DO SEQUESTRO DE DADOS

"RANSONWARE" - O QUE É?

É um vírus que "criptografa" todos os dados armazenados em um computador ou servidor até o pagamento de um resgate.

CRIMINOSO VIRTUAL

Invade o dispositivo da vítima e instala um **programa malicioso para criptografar (codificar) as informações armazenadas em um computador ou servidor corporativo.**

- **Exige pagamento de resgate.**
- **O pagamento é em criptomoeda (moeda digital).**
- **Nem sempre as chaves liberadas funcionam.**

VÍTIMA

Não consegue ter acesso aos dados armazenados em seu dispositivo ou de arquivos no servidor da instituição. Todos estão bloqueados.

DICAS DE PREVENÇÃO

1. Mantenha um ***BACKUP* atualizado** do computador em um HD externo, em pendrive ou em servidor preparado para esse fim.
2. **Não acesse sites suspeitos disponíveis na internet.**
3. **Não clique em links duvidosos ou de e-mails suspeitos.**
4. Mantenha os mecanismos de monitoramento e de proteção dos ativos atualizados (antivírus e *firewalls*).

GOLPE LIGADOS À VACINAÇÃO CONTRA COVID-19

CRIMINOSO VIRTUAL

Liga para a residência ou celular da pessoa se identificando como agente da pasta do **Ministério da Saúde (MS)** ou de uma intituição de saúde oferecendo um pré-cadastro para a vacinação, a fim de **obter dados pessoais da vítima**.

ou

Encaminha uma mensagem de texto com um link ou código para esse falso cadastro, que pode levar à **clonagem do aplicativo de WhatsApp da vítima**.

VÍTIMA

Acreditando que o contato é verdadeiro e pressionada pelo cenário de pandemia instalado no País, acaba fornecendo os dados pessoais de forma inocente.

DICAS DE PREVENÇÃO

- Não forneça nenhum dado pessoal por meio de ligação ou mensagens recebidas.
- Busque informações nos órgãos oficiais do governo ou nas secretarias de saúde de seu município ou estado.
- Não acesse falsas plataformas ou links suspeitos, mesmo que tenham sido indicadas por conhecidos.
- Ative os mecanismos de segurança de verificação em duas etapas de seu aplicativo ou e-mail.
- Faça a DENÚNCIA junto às entidades oficiais e registre um Boletim de Ocorrência em uma Delegacia Policia.

GOLPE ENVOLVENDO CADASTRO OU TRANSAÇÕES COM PIX

5

O QUE É?

É a mais nova modalidade de pagamento e transferência criada pelo Banco Central, que possibilita maior agilidade nas operações financeiras pelos canais eletrônicos das instituições financeiras.

COMO OCORRE O GOLPE

A vítima **recebe links por redes sociais**, **SMS** ou **e-mail** com ofertas de cadastro no serviço de pagamentos com o PIX.

- podem estar infectados por ***malware.***
- podem direcionar para **sites falsos**.

DICAS DE PREVENÇÃO

- Certifique-se de que esteja logado no aplicativo ou site de sua agência bancária.
- Nunca faça o seu cadastro por meio de link recebidos por SMS, WhatsApp ou e-mail.
- Nunca repasse a outra pessoa nenhum código fornecido por SMS ou imagem de um QR Code.
- Confira se o QR Code está apontando para o endereço correto para o pagamento antes de inserir a sua chave de autorização do PIX.
- Na dúvida, entre em contato com sua agência bancária para os esclarecimentos necessários relacionados ao PIX.

powered by Banco Central

O **BANCO CENTRAL DO BRASIL** disponibilizou um link de consulta gratuita a relatórios de chaves PIX, empréstimos e financiamentos, contas em banco e outros.

https://www.bcb.gov.br/cidadaniafinanceira/registrato

GOLPE DO NUDES OU SEXTORSÃO

GOLPISTA

Aborda uma vítima nas mídias sociais para iniciar um **bate papo de amizade**. Após **ganhar confiança**, as conversas ficam mais picantes e é **solicitado imagens** ou **vídeos íntimos da vítima.**

VÍTIMA

Por impulso e estar empolgado(a) com a evolução das conversas nas mídias sociais, **acaba enviando fotos e vídeos íntimos**. A partir desse momento **são ameaçadas ou chantageadas para fazerem um depósito em dinheiro para as imagens não serem divulgadas na internet**.

DICAS DE PREVENÇÃO

- **Desconfie de pedidos de amizade ou mensagens de pessoas desconhecidas.**
- **Evite compartilhar fotos ou vídeos íntimos, hábitos ou rotinas nas redes sociais.**
- **Não armazene fotos e vídeos íntimos no seu celular, *notebook* ou no computador. Esses materiais, quando recolhidos para manutenção ou roubados, podem permitir que outras pessoas tenham acesso a esses arquivos.**
- **Evite participar de chamadas de vídeo com desconhecidos e lembra-se que a imagem da outra pessoa pode ser falsa.**
- **Caso tenha sido vítima não apague as conversas (elas possuem informações necessárias) mantidas com o golpista e procure uma Delegacia de Polícia para registrar um Boletim de Ocorrência (BO).**

GOLPE DA FALSA BATIDINHA NO TRÂNSITO

GOLPISTA/CRIMINOSO

O meliante dirigindo atrás do automóvel da vítima, normalmente em carro roubado, **encosta atrás dando uma pequena "batidinha"**, com o propósito de pará-lo.

- **É comum esse evento ocorrer em LOCAIS ISOLADOS.**
- **O objetivo é roubar o veículo e seus pertences.**
- **Essa situação pode ser um RISCO DE VIDA.**

VÍTIMA

Inocentemente estaciona o veículo para verificar o prejuízo causado pela batida e conversar com o ocupante do outro veículo.

- **Maior ocorrência com mulheres.**
- **Veículos de luxo são os mais visados.**

DICAS DE PREVENÇÃO

Dependendo da situação e lugar, o melhor é não descer e ficar no prejuízo. Não vale a pena por sua vida em risco por um pequeno dano.

Quando em viagem, se o problema não interferir no funcionamento do veículo, **parar somente em locais seguros** como posto policial, posto de gasolina, povoados etc.

Se possível, sempre informe a uma pessoa de confiança ou familiar o seu trajeto e localização durante a viagem.

GOLPE DO PECÚLIO OU AÇÃO JUDICIAL

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.

GOLPE DO PARENTE EM DIFICULDADE

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

GOLPISTA

Telefona para familiares de paciente internado em hospital e, se passando por profissional de saúde, diz que é necessário realizar um depósito bancário, em uma 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, causando prejuízo à vítima.

DICAS DE PREVENÇÃO

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

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

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 essa 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

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, a 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

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 um 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

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

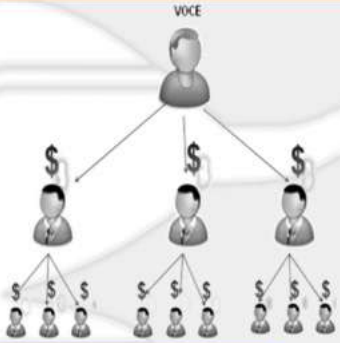
- Confirmar, junto ao banco e órgãos de proteção ao crédito, toda informação recebida por meio de correspondência.

GOLPE DA PIRÂMIDE OU PROGRAMA DE AJUDA MÚTUA

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

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, assim como nos editais de concursos publicados nos diversos meios de comunicação.

GOLPES PELA INTERNET
(PHISHING)

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.

GOLPES PELA INTERNET (ENGENHARIA SOCIAL)

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
- Enviam 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.

GOLPES PELA INTERNET
(*PHARMING*)

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)

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)

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 comprovar a realização do pagamento ou o envio da mercadoria que, na realidade, não foi realizado.

DICAS DE PREVENÇÃO

- Não confiar apenas. Fazer 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.

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 vindas 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 na 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

ESTELIONATÁRIO

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

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

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

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.

Nessas 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.

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 não se sabe quem está do outro lado da linha. Oriente seus familiares e empregados a respeito.

3. Cuidado com sua documentação pessoal.

4. Desconfie de ofertas generosas.

5. Procure tratar pessoalmente 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 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.

f. Sempre que possível, realize compras utilizando o cartão virtual.

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.

REFERÊNCIAS

MINISTÉRIO DA DEFESA. EXÉRCITO BRASILEIRO. Comando do Exército. **Manual de Campanha Contrainteligência – EB70-MC-10.220.** Brasília, 1ª Edição, 2019.

Golpes ligados à vacinação contra Covid-19 tentam roubar dados e clonar WhatsApp. **Anna Satie, da CNN em São Paulo**, São Paulo, 19 de jan. de 2021. Disponível em: < https://www.cnnbrasil.com.br/tecnologia/2021/01/19/golpes-ligados-a-vacinacao-contra-covid-19-tentam-roubar-dados-e-clonar-whatsapp>. Acesso em: 1º de fev. de 2021.

Cadastro do Pix é isca de sites falsos para roubar dados. Golpe utiliza mais de 30 domínios falsos usando o Pix como isca; entenda e saiba se proteger. **Clara Fabro, para o TechTudo**, 07 de out. de 2020. Disponível em: <https://www.techtudo.com.br/noticias/2020/10/cadastro-do-pix-e-isca-de-sites-falsos-para-roubar-dados.ghtml>. Acesso em: 10 de fev de 2021.

Delitos praticados por meios eletrônicos - Perguntas e respostas. **Polícia Civil de São Paulo**, São Paulo. Disponível em: <https://www.policiacivil.sp.gov.br/portal/imagens/CRIMES%20CIBERN%C3%89TICOS%20-%20PERGUNTAS%20E%20RESPOSTAS%20V2.pdf>. Acesso em: 14 de fev. de 2021.

Guia de Orientação e Prevenção a Golpes

(1ª atualização e revisão - FEV 2021)

Edição - 2021

PREVENIR, ORIENTAR E PROTEGER.

DIVISÃO DE CONTRAINTELIGÊNCIA

DCI

CIE