

GUIA SOBRE GOLPES VIRTUAIS E DICAS DE COMO PRESERVAR SEUS DADOS NA INTERNET



NUDECON

Núcleo de Defesa
do Consumidor

»PE-TO

DEFENSORIA PÚBLICA
ESTADO DO TOCANTINS

O QUE É O NUDECON

O Núcleo de Defesa do Consumidor (NUDECON) é um órgão da Defensoria Pública do Estado do Tocantins que possui a incumbência de tutelar e promover os direitos dos consumidores hipossuficientes a partir da premissa básica que os define juridicamente: a sua vulnerabilidade social ou econômica.

NUDECON

Núcleo de Defesa
do Consumidor

»PE·TO
DEFENSORIA PÚBLICA
ESTADO DO TOCANTINS

APRESENTAÇÃO DO GUIA

O Núcleo de Defesa do Consumidor da Defensoria Pública do Estado do Tocantins reuniu neste guia os principais golpes que estão acontecendo pela internet, redes sociais e telefone, apresentando algumas dicas para preservar seus dados.

Normalmente, não é uma tarefa simples atacar e fraudar dados em um servidor de uma instituição bancária ou comercial e, por esse motivo, golpistas vêm concentrando esforços na exploração de fragilidades dos usuários.

Os criminosos vêm utilizando técnicas de engenharia social e estão sempre aprimorando ou mudando as técnicas para envolver as vítimas e persuadi-las a fornecerem informações sensíveis ou a realizarem ações como executar códigos maliciosos e acessar páginas falsas.

Existem diversas formas de abordagem, mas os apelos são sempre os mesmos: clicar em links, comprar por meio de anúncios de redes sociais, participar de sorteios ou enviar código que chega por mensagem de texto (SMS), transferir dinheiro para alguma conta bancária ou fornecer dados pessoais, números e senhas de cartões.

Neste documento, passamos a apresentar os golpes mais comuns aplicados atualmente.

Sumário

1. WHATSAPP.....	4
2. WHATSAPP - MENSAGENS PROMOCIONAIS PELO APLICATIVO	5
3. POR TELEFONE	6
4. REDES SOCIAIS	6
5. COMPRAS ONLINE	7
6. SITES DE LOJAS QUE NÃO ACEITAM COMPRA POR MEIO DO CARTÃO DE CRÉDITO: ATENÇÃO REDOBRADA PARA OS GOLPES.....	10
7. ALUGUEL DE CONTA NO E-COMMERCE.....	11
8. GOLPE PRATICADO POR MEIO DE SITES COMO OLX E FACEBOOK.....	11
9. GOLPE DO FALSO PAGAMENTO.....	12
10. GOLPE DO BOLETO FALSO	12
11. GOLPE DO INTERMEDIÁRIO NAS COMPRAS DE VEÍCULOS	13
12. GOLPE DO VEÍCULO DE LOCADORA.....	13
13. GOLPE DO SINAL NA COMPRA DE VEÍCULO	14
14. GOLPE DA FACHADA FALSA NA COMPRA DE VEÍCULOS.....	15
15. GOLPE DO VOUCHER/CUPOM DE DESCONTOS EM RESTAURANTE	15
16. TRANSAÇÕES BANCÁRIAS.....	16
17. GOLPE DE INVESTIMENTOS	16
18. GOLPE DO MOTOBOY	17
19. FRAUDE DE ANTECIPAÇÃO DE RECURSOS	17
20. FURTO DE IDENTIDADE (IDENTITY THEFT).....	19
21. GOLPE DA MÁQUINA DE CARTÃO COM VISOR QUEBRADO	20
22. GOLPE DA SELFIE.....	20
23. GOLPE USANDO NOME DA RECEITA FEDERAL	22
24. GOLPE DO PASSE EXPRESSO NO PEDÁGIO	23
25. GOLPE DA PAQUERA VIRTUAL	23
26. DICAS E CUIDADOS PARA PRESERVAR SEUS DADOS NO AMBIENTE VIRTUAL	24

1 WHATSAPP

As principais abordagens utilizadas pelos criminosos envolvendo o WhatsApp são:

- Usam números de telefone exibidos nos anúncios para clonar a conta dos WhatsApp;
- Contam uma história para conseguir o código que chega por SMS no seu celular;
- Pedem dinheiro emprestado se passando por alguém conhecido;
- Envia mensagens com oferta de promoções pelo aplicativo.

O golpe realizado a partir dos sites usam números de telefone exibidos nos anúncios para clonar a conta do WhatsApp dos vendedores. Os golpistas entram em contato e se passam por funcionários de empresas como OLX, Mercado Livre e ZAP.

Eles alegam que precisam do código enviado por SMS para regularizar o anúncio. O código, no entanto, é um PIN de autenticação do WhatsApp que permite acionar, em outro aparelho, a conta que a vítima tem no aplicativo de mensagens.

Caso o autor do anúncio não perceba nada estranho e envie o código, o golpista clona seu WhatsApp e começa a enviar mensagens para seus contatos. Uma das práticas mais comuns é mandar mensagens pedindo dinheiro emprestado para a lista de contatos e grupos fingindo ser você.

O que fazer caso tenha sido vítima:

Denunciar o perfil falso no aplicativo WhatsApp usando o suporte@whatsapp.com ou clicar no número que enviou a mensagem e, no campo “dados do contato” clicar em denunciar.

Como evitar o golpe:

- Nunca informe o número de SMS que chega no celular para terceiros;
- Não clique em links, banners e outros anúncios recebidos por SMS, e-mail e mensagens de WhatsApp;
- Faça uma chamada de vídeo para confirmar quem está pedindo o dinheiro emprestado;
- A dica principal é ativar a verificação em duas etapas. Vá em “Ajustes”, “Conta”, “Verificação em duas etapas”, cadastre senha de 6 dígitos e o seu e-mail. Assim será solicitada a senha junto com o código de verificação sempre que a conta for configurada em um novo aparelho;
- Fique atento às mensagens de solicitação de dinheiro por conhecidos;
- Desconfie se a fotografia do perfil do WhatsApp estiver vinculada a uma linha telefônica que não esteja cadastrada nos seus contatos;
- Se a conta bancária informada para depósito de valores estiver em nome de terceiro, a chance de ser fraude é ainda maior.



2 WHATSAPP: MENSAGENS PROMOCIONAIS PELO APLICATIVO

Os criminosos enviam mensagens com ofertas atrativas de promoção ou então de recarga gratuita para celular.

Para receber o crédito ou o produto ofertado na promoção o consumidor é induzido a clicar numa imagem que o redireciona para outra página na internet, onde contém o programa que se instalará no seu smartphone.

Essa imagem, geralmente de conteúdo atrativo, é na verdade um script malicioso (vírus para smartphone), contendo uma série de comandos que são executados a partir do momento em que o consumidor toca (clica) na imagem.

Ou seja, é uma linguagem de programação criada para instalar no smartphone algum aplicativo com a finalidade de roubar dados pessoais importantes.

Ao clicar na “promoção”, o consumidor fornece ao vírus programa a permissão que ele precisa para se instalar no telefone.

O exemplo de créditos gratuitos para celular é apenas um dentre dezenas de falsas promoções e ofertas.

Como evitar o golpe:

- Se você não tem grande conhecimento sobre linguagem de programação, limite-se a instalar aplicativos disponíveis nas lojas oficiais (Play Store / App Store);
- Fique atento e evite instalar programas de origem duvidosa.



3 POR TELEFONE

Como agem os criminosos:

- Se passam por funcionários do seu banco e informam que sua conta está sofrendo uma tentativa de invasão;
- Orientam a vítima a seguir um passo a passo de modo a obter seus dados, login ou senha;
- Podem, até mesmo, pedir para que você entregue seu cartão a um suposto serviço de entrega do banco, deslocado ao seu encontro;
- Fazem cobranças em nome de hospitais e instituições de caridade.

Como evitar o golpe:

- Jamais siga o passo a passo orientado pelo desconhecido ao telefone, e encurte a conversa;
- Procure pessoalmente as instituições citadas para checar a veracidade da história;
- Não retorne ligações, os criminosos conseguem interceptar;
- Oriente pessoas da sua casa e de seu convívio, especialmente idosos e crianças, sobre esses golpes e a não darem quaisquer informações pessoais a estranhos.



4 REDES SOCIAIS

Como agem os criminosos:

- Oferecem um prêmio, pedem o telefone para cadastro e enviam um código para confirmar a suposta inscrição;
- Criam anúncios falsos para a venda de produtos que não existem;
- Criam perfis falsos buscando a aproximação e a confiança da vítima.

Como evitar o golpe:

- Verifique se é o perfil oficial da marca/estabelecimento. Lembre-se que número de seguidores não significa idoneidade;
- Se for um perfil pessoal, verifique se há perfis em outras redes sociais. Se estiver presente em apenas uma rede, fique alerta, pois pode ser falso;
- Faça uma chamada de vídeo, confirme o documento do atendente e veja o produto para confirmar que ele existe;
- Não repasse informações que chegam pelo celular, como código ou voucher;
- Desconfie de preços muito baixos;
- Não divulgue dados pessoais.

5 COMPRAS ONLINE

Como agem os criminosos:

- Hackeiam sites oficiais;
- Fazem anúncios de sites falsos para ter visibilidade em ferramentas de busca como, por exemplo, o Google;
- Envia propaganda via links patrocinados anunciando descontos em sites de compras coletivas e colocando comentários falsos de clientes elogiando a mercadoria;
- Ofertam produtos muito procurados e com preços abaixo dos praticados pelo mercado.

Os golpistas normalmente criam um site fraudulento, com o objetivo específico de enganar os possíveis clientes que, após efetuarem os pagamentos, não recebem as mercadorias.

Além do comprador que paga, mas não recebe a mercadoria, esse tipo de golpe pode ter outras vítimas, como:

- uma empresa séria, cujo nome tenha sido vinculado ao golpe;
- um site de compras coletivas, caso ele tenha intermediado a compra;
- uma pessoa, cuja identidade tenha sido usada para a criação do site ou para abertura de empresas fantasmas.

Fique atento a algumas informações que deve constar num site de compra:

- Nome comercial;
- CNPJ ou CPF;
- Endereço físico do estabelecimento;
- Informações de contato;
- Links devem começar com “https”;
- Política de troca;
- Locais de entrega e respectivos prazos;
- Responsabilidade pelo custeio do frete;
- Canais de atendimento ao cliente.



Como evitar o golpe:

- Procure validar os dados de cadastro da empresa no site da Receita Federal;
- Verifique se a página das empresas nas redes sociais contém o selo de verificação;
- Evite fazer compras usando computadores compartilhados, lan houses ou cybercafés;
- Instale um antivírus e atualize-o frequentemente;
- Verifique se o domínio do endereço é registrado no Brasil(.com.br);
- Todas as transações devem ser feitas por meio do site oficial;
- Pesquise na internet sobre o site, antes de efetuar a compra, para ver a opinião de outros clientes;
- Acesse sites especializados em tratar reclamações de consumidores insatisfeitos, para verificar se há reclamações referentes a essa empresa;
- Sempre confira os dados do boleto que está pagando;
- Gere um cartão virtual pelo aplicativo do banco, que é válido apenas para uma compra;
- Jamais deixe o cartão salvo para compras futuras;
- Se o site oferecer a opção de armazenar seus dados bancários ou número do cartão de crédito não aceite;
- Faça uma pesquisa de mercado, comparando o preço do produto exposto no site com os valores obtidos na pesquisa e desconfie caso ele seja muito abaixo dos praticados pelo mercado;
- Fique atento a propagandas recebidas através de spam, seja cuidadoso ao acessar links;
- Não informe dados de pagamento caso o site não ofereça conexão segura ou não apresente um certificado confiável.

O que observar num site de compras coletivas:

- Atente para o prazo final da oferta;
- Valor do desconto;
- Número mínimo de pessoas necessárias para conclusão da oferta;
- Especificações do produto ou serviço;
- Prazo para utilização do cupom ou voucher.

Como se proteger nas compras online em sites internacionais:

- Dê preferência a sites que usam intermediadoras de pagamento, pois caso o produto não seja entregue, o valor da compra poderá ser devolvido;
- Lembre-se que o Código de Defesa do Consumidor incide sobre relações de consumo somente em sites de empresas com escritório ou representação no Brasil.

Como evitar o golpe em sites de compras coletivas:

- Evite comprar por impulso apenas para garantir o produto ofertado;
- Faça pesquisas prévias, pois há casos de produtos anunciados com desconto, mas que na verdade, apresentam valores superiores aos de mercado;
- Pesquise na Internet sobre o site de compras coletivas, antes de efetuar a compra, para ver a opinião de outros clientes e observar se foi satisfatória a forma como os possíveis problemas foram resolvidos.



Em caso de aquisição de produtos em sites de compras coletivas quem é o responsável por defeitos no produto ou serviços adquiridos?

A responsabilidade é solidária, ou seja, se o consumidor não conseguir resolver o problema diretamente com o fornecedor, fabricante ou vendedor pode entrar em contato com o site que efetuou a compra.

O consumidor pode desistir da compra online?

Nos casos de compras online, o consumidor tem um prazo de 7 (sete) dias para se arrepender da compra a partir da data de celebração do contrato ou da entrega do produto.

Se o produto vier com defeito, avariado, violado, diferente do que foi pedido ou não chegar o que o consumidor pode fazer?

O consumidor poderá registrar reclamação junto ao vendedor ou por meio de seus canais de atendimento (SAC ou Ouvidoria), usar o portal **www.consumidor.gov.br** ou recorrer ao Procon de sua cidade para reclamar.

Caso não tenha êxito na resolução pelos meios extrajudiciais poderá ainda procurar advogado particular ou a Defensoria Pública para acionar a Justiça para solucionar o problema.

O que fazer se após efetuar a compra online for informado que não há disponibilidade do produto ou serviço?

Em caso de indisponibilidade do produto ou serviço o consumidor poderá:

- Exigir o cumprimento forçado da oferta;
- Escolher outro produto ou serviço equivalente;
- Cancelar o contrato e exigir a devolução do valor pago;
- Além disso poderá pleitear ainda perante o judiciário indenização por eventuais perdas e danos decorrentes dessa situação.



6 SITES DE LOJAS QUE NÃO ACEITAM COMPRA POR MEIO DO CARTÃO DE CRÉDITO: ATENÇÃO REDOBRADA PARA OS GOLPES

Normalmente o consumidor utiliza o cartão de crédito como meio de pagamento nas compras realizadas pela internet tanto que a maioria das vendas online é concluída dessa forma.

Então, ao se deparar com um site de loja que não oferece essa opção de pagamento, desconfie da existência desse negócio, pois muitas fraudes na internet acontecem justamente por meio de transferências bancárias ou pagamentos por boletos. Por essas razões é preciso desconfiar quando a opção de pagamento por meio do cartão de crédito não está disponível.



Como evitar o golpe

- Procure validar os dados de cadastro da empresa no site da Receita Federal;
- Verifique se a página da empresa nas redes sociais contém o selo de verificação;
- Todas as transações devem ser feitas por meio do site oficial;
- Pesquise na internet sobre o site, antes de efetuar a compra, para ver a opinião de outros clientes;
- Acesse sites especializados em tratar reclamações de consumidores insatisfeitos, para verificar se há reclamações referentes a essa empresa;
- Sempre verifique os dados do boleto que está pagando.



7 ALUGUEL DE CONTA NO E-COMMERCE

No Aluguel de Conta, o golpista entra em contato com os usuários oferecendo uma quantia para alugar sua conta em plataformas de e-commerce. Atraídos pela oportunidade de ganhos, as pessoas informam usuário e senha.

As contas são utilizadas para aplicar golpes em outros consumidores. Os usuários devem ficar atentos, pois além de infringirem as regras de uso das plataformas, são responsáveis pela utilização de suas contas e, por sua vez, podem ser indiciados criminalmente por crimes praticados com a sua utilização.

Como evitar o golpe:

- Nunca compartilhe seu login e senha com terceiros, escolha senhas fortes e as troque regularmente, além de informar imediatamente às plataformas caso tenha sido abordado.



8 GOLPE PRATICADO POR MEIO DE SITES COMO OLX E FACEBOOK

A dinâmica do golpe é simples, mas efetiva. Os criminosos procuram potenciais vítimas pelos sites de compra e venda, como OLX e Facebook Market, buscando por negociações verdadeiras. Se passando por outras pessoas - em geral, por policiais -, abordam o vendedor, demonstrando interesse pelo produto.

Iniciada as negociações, geralmente não questionam o preço e começam a organizar a logística para entrega do produto. Marcam um dia para pegar, mas desmarcam em cima da hora, normalmente criando alguma história trágica ou urgente como desculpa.

Em seguida, afirmam que, mesmo desmarcando, ainda têm muito interesse no produto e remarcam a entrega para um outro horário, bem em cima da hora da conversa. Encaminham um comprovante de TED falso, encontram o vendedor rapidamente e fogem com o produto.

Como evitar o golpe:

- Fique atento aos falsos comprovantes de pagamento;
- Desconfie se o comprador está muito apressado, nervoso ou impaciente; antes de se encontrar ou enviar o item ao comprador, busque informações que possam ajudar a identificá-lo; com os dados sobre o comprador, faça uma pesquisa nas mídias sociais;
- Nos casos de pagamento espere compensar e creditar o valor na conta antes de efetuar a entrega/envio do produto.

9 GOLPE DO FALSO PAGAMENTO

O golpista neste caso se passa por comprador, demonstra interesse em um produto vendido nas plataformas de e-commerce e fecha o negócio. No entanto, ela utiliza comprovantes de pagamento falsos para concluir a compra.

Como evitar o golpe:

- Confirme, antes de enviar o produto, com o seu banco ou com a plataforma, quando estiver usando a intermediação de pagamento do site, se o valor já está disponível em sua conta;
- Desconfie de negociações por e-mail ou aplicativos de mensagens, mantendo a negociação no ambiente das plataformas de compra e venda. Só entregue o produto após ter o pagamento confirmado na sua conta.

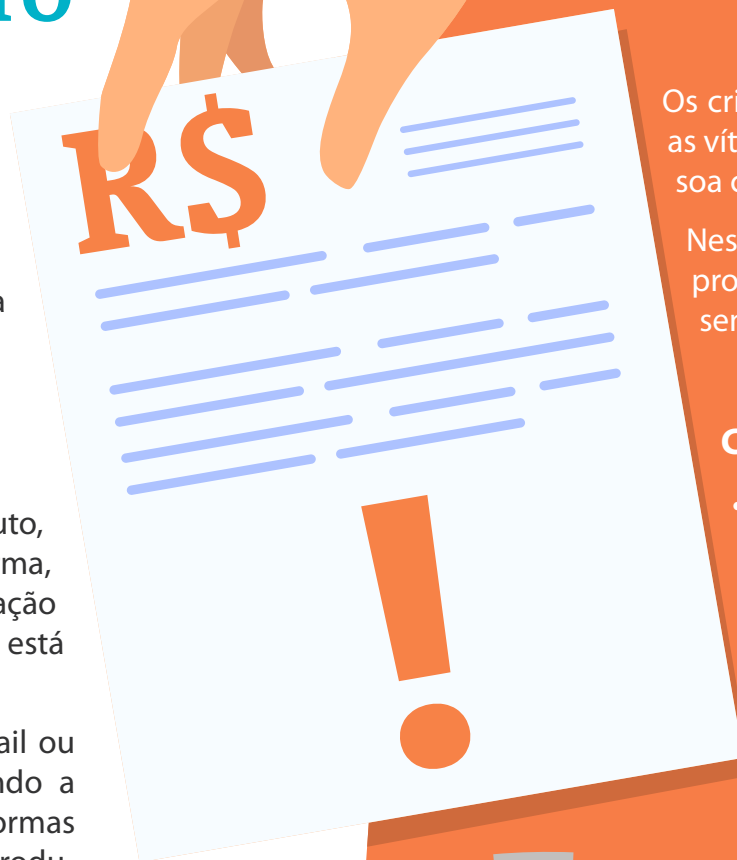
10 GOLPE DO BOLETO FALSO

Os criminosos emitem um boleto falso e enviam para as vítimas usando o nome de uma empresa que a pessoa confia ou que possui algum vínculo comercial.

Nestes casos a vítima acha que está pagando por um produto ou serviço, quando na verdade não representa nenhuma compra.

Como evitar o golpe

- Verifique sempre os dados do beneficiário e do pagador se eles estão corretos e não apresentam nenhum erro de grafia;
- Fique atento ao e-mail remetente do boleto para verificar se realmente provem de site oficial da empresa, para se certificar que o boleto é verdadeiro.



11 GOLPE DO INTERMEDIÁRIO NAS COMPRAS DE VEÍCULOS

No golpe do intermediário, os fraudadores se utilizam de anúncios de terceiros para negociar veículos usados ou seminovos, utilizando informações de anúncios reais e recebendo o pagamento do comprador interessado pelo veículo.

Como evitar o golpe:

- Evite intermediários, negocie sempre diretamente com comprador/vendedor;
- Desconfie de ofertas muito atrativas e veículos com preços abaixo dos valores de mercado;
- Fique atento com conversas em que o interessado, se passando pelo vendedor/comprador, diz que está negociando o veículo para um amigo/parente com quem tem uma dívida.



12 GOLPE DO VEÍCULO DE LOCADORA

O golpe mais recente do mercado envolve as locadoras de veículos. O indivíduo vai até uma empresa e aluga um carro por certo período de tempo. Depois, cria um documento falso com ajuda de um despachante clandestino e anuncia o veículo locado na internet.

O comprador entra em contato, confere o documento em nome do vendedor e faz a transferência do dinheiro para o dito proprietário. Quando chega o vencimento do contrato, a locadora bloqueia o carro e entra na justiça.

Como evitar o golpe

- Entre em contato com o vendedor, evite negociações com terceiros;
- Certifique-se de que o vendedor é o proprietário legítimo do veículo;
- Verifique pelo Renavam se o veículo tem multas e cobranças pendentes de IPVA;
- Desconfie de negociações em que o vendedor não possa ou não queira compartilhar os dados do veículo.

- Evite realizar qualquer tipo de depósito antecipado (pagamento de entrada) sem antes ver o veículo de perto, conferir se ele está em bom estado de conservação e com todos os acessórios anunciados;
- Fique atento e desconfie se o vendedor estiver muito apressado, nervoso ou impaciente para fechar o negócio. Não tenha receios de tirar qualquer dúvida sobre o veículo;
- Desconfie se o veículo estiver em perfeito estado com valores muito abaixo do mercado;
- Fique atento se o vendedor, após anunciar na OLX, alegar que ganhou o veículo em uma promoção/sorteio, que é ex-funcionário de uma empresa, ou se diz trabalhar nas montadoras de veículos e que, a partir disso, conseguiu o automóvel mais barato;
- Faça uma revisão com um mecânico de confiança antes de efetuar o pagamento;
- Cuidado com anúncios que oferecem frete grátis para a entrega do veículo;
- Lembre-se os golpistas fazem o possível para que a negociação pareça legítima;
- Para não correr esse risco, o indicado é procurar o histórico do carro.



13

GOLPE DO SINAL NA COMPRA DE VEÍCULO

É comum que anunciantes mal-intencionados divulguem, na internet, veículos com baixo valor de mercado para atrair a atenção de compradores. Quando um deles demonstra real interesse em adquirir o carro e marca um encontro para observá-lo fisicamente, o golpista solicita um “sinal”.

A justificativa é que um outro interessado surgiu e está querendo levar o automóvel. É aí que passam a conta corrente de um laranja para que seja feito o depósito. Esse é o golpe mais comum do mercado e acontece com grande frequência.

Como evitar o golpe

- Evite efetuar o pagamento antes de promover a checagem do veículo;
- Não efetue pagamento em conta de terceiros.

14 GOLPE DA FACHADA FALSA NA COMPRA DE VEÍCULOS

Os criminosos neste caso costumam tirar fotos da fachada de uma concessionária e, com um programa de edição de imagens, promovem alteração no número de telefone que aparece na placa.

O número continua sendo um fixo e quando o interessado liga, o processo é bastante profissional, com secretária e transferências de ramal. O que gera “credibilidade”.

É anunciado um carro que aparece na fachada da loja e quando o interessado entra em contato, solicitam um “sinal” ou até o pagamento integral também em conta de terceiros. Por fim, quando o comprar vai buscar ou ver o carro na loja, percebe que foi enganado.

Como evitar o golpe

- Verifique as informações recebidas no site oficial da empresa;
- Procure a imagem da concessionária pelo Google Maps e faça conferência do número informado;
- Não faça depósitos na conta de terceiros nem efetue o pagamento integral de um veículo sem antes vistoriá-lo.

15 GOLPE DO VOUCHER/CUPOM DE DESCONTOS EM RESTAURANTE

O criminoso entra em contato com a vítima via direct no Instagram se passando por representante de um restaurante de sua preferência.

Após breve conversa, um link malicioso contendo um suposto voucher/cupom de desconto é enviado para a vítima. Esse link, se acessado, pode coletar os dados constantes no seu celular.

Como evitar o golpe:

- Suspeite de contatos que oferecem voucher/cupom de descontos de restaurantes a serem utilizados em plataformas de delivery;
- Não clique no link fornecido nessas conversas antes de confirmar diretamente com o restaurante a veracidade do desconto.



16

TRANSAÇÕES BANCÁRIAS



Como agem os criminosos:

- Furtam linhas telefônicas e habilitam dispositivos eletrônicos para movimentações bancárias;
- Clonam cartões nos caixas eletrônicos.

Como evitar o golpe:

- Remova os equipamentos que estão habilitados para movimentações em contas correntes que você não reconhece ou que você não usa mais;
- Mude senhas caso a linha telefônica pare de funcionar;
- Cancele o cartão caso ele fique preso no caixa eletrônico.

17

GOLPE DE INVESTIMENTOS

Os criminosos usam pessoas jurídicas com aparente credibilidade para oferecer investimentos pessoais com ganhos e taxas de juros acima dos comumente praticados no mercado.

Eles alegam que atuam no mercado de ações ou que possuem algum produto de grande valia.

As vítimas fazem aportes de dinheiro, em diversos níveis e momentos distintos, e com esses valores os criminosos pagam investimentos daqueles que entraram antes, apresentando uma suposta credibilidade no modelo de negócio.

Assim, os primeiros investidores, animados com seus ganhos, acabam trazendo outros que também fazem aportes. Dessa forma, fazem girar o sistema financeiro criado pelos criminosos, até o momento em que estes “quebram” o esquema, desviando milhares de reais dos investidores.

Não se trata da conhecida “pirâmide financeira”, pois não há o recrutamento voluntário progressivo que caracteriza essa modalidade de sistema como forma de auferir ganhos. O golpe de investimento independe de qualquer recrutamento a ser feito pelo investidor.

Como evitar o golpe:

- Sempre suspeitar de ofertas de investimentos com ganhos acima daqueles praticados pelo mercado bancário regular, ainda que apresentados por empresas com aparente credibilidade, ou por pessoas conhecidas e familiares, que podem estar na base do sistema e por isso receberem algum “rendimento”, os fazendo crer na rentabilidade do negócio;
- Verificar se existe autorização do Banco Central e fiscalização do Conselho de Valores Mobiliários. Lembre-se, esse esquema a qualquer momento pode ser interrompido e quebrado, deixando inúmeras vítimas.

18 GOLPE DO MOTOBOY

A vítima recebe ligação telefônica supostamente da área de segurança do banco e é questionada sobre uma compra realizada com seu cartão de crédito.

Diante da resposta negativa, o interlocutor confirma alguns dados pessoais, informa que o cartão de crédito foi clonado, mas que já está cancelado. Explica que, para comodidade do cliente, um funcionário da agência, devidamente identificado com crachá, irá comparecer à residência da vítima para pegar o cartão de crédito cancelado e também uma declaração de não reconhecimento de compra.

Na posse do cartão, o criminoso realiza saques e diversas compras em nome da vítima. Suspeite de ligações telefônicas que questionem compras realizadas com o cartão de crédito.

Como evitar o golpe:

- Não forneça por telefone dados pessoais tais como endereço e senha de cartão bancário;
- Os bancos não dispõem de serviço de delivery, ou seja, não enviam funcionários a residências de clientes para pegar documentos e cartões.



19 FRAUDE DE ANTECIPAÇÃO DE RECURSOS

A fraude de antecipação de recursos, ou advance fee fraud, é aquela na qual um golpista procura induzir uma pessoa a fornecer informações confidenciais ou a realizar um pagamento adiantado, com a promessa de futuramente receber algum tipo de benefício.

Por meio do recebimento de mensagens eletrônicas ou do acesso a sites fraudulentos, a pessoa é envolvida em alguma situação ou história mirabolante, que justifique a necessidade de envio de informações pessoais ou a realização de algum pagamento adiantado, para a obtenção de um benefício futuro. Após fornecer os recursos solicitados a pessoa percebe que o tal benefício prometido não existe, constata que foi vítima de um golpe e que seus dados/dinheiro estão em posse de golpistas.

A fraude de antecipação de recursos possui diversas variações que, apesar de apresentarem diferentes discursos, assemelham-se pela forma como são aplicadas e pelos danos causados. Algumas dessas variações são:

Loteria internacional: você recebe um e-mail informando que foi sorteado em uma loteria internacional, mas que para receber o prêmio a que tem direito, precisa fornecer seus dados pessoais e informações sobre a sua conta bancária.

Crédito fácil: você recebe um e-mail contendo uma oferta de empréstimo ou financiamento com taxas de juros muito inferiores às praticadas no mercado. Após o seu crédito ser supostamente aprovado você é informado que necessita efetuar um depósito bancário para o ressarcimento das despesas.

Doação de animais: você deseja adquirir um animal de uma raça bastante cara e, ao pesquisar por possíveis vendedores, descobre que há sites oferecendo esses animais para doação. Após entrar em contato, é solicitado que você envie dinheiro para despesas de transporte.

Oferta de emprego: você recebe uma mensagem em seu celular contendo uma proposta tentadora de emprego. Para efetivar a contratação, no entanto, é necessário que você informe detalhes de sua conta bancária.

Noiva russa: alguém deixa um recado em sua rede social contendo insinuações sobre um possível relacionamento amoroso entre vocês. Essa pessoa mora em outro país, geralmente a Rússia, e após alguns contatos iniciais sugere que vocês se encontrem pessoalmente, mas, para que ela possa vir até o seu país, necessita de ajuda financeira para as despesas de viagem.

Como evitar o golpe:

A melhor forma de se prevenir é identificar as mensagens contendo tentativas de golpes. Uma mensagem desse tipo, geralmente, possui características como:

- Oferecer quantias astronômicas de dinheiro;
- Solicitar sigilo nas transações;
- Solicitar que você a responda rapidamente;
- Apresenta palavras como “urgente” e “confidencial” no campo de assunto;
- Apresenta erros gramaticais e de ortografia (muitas mensagens são escritas por meio do uso de programas tradutores e podem apresentar erros de tradução e de concordância);
- Desconfie de situações onde é necessário efetuar algum pagamento com a promessa de futuramente receber um valor maior (pense que, em muitos casos, as despesas poderiam ser descontadas do valor total).



20 FURTO DE IDENTIDADE (IDENTITY THEFT)

No seu dia a dia, sua identidade pode ser furtada caso, por exemplo, alguém abra uma empresa ou uma conta bancária usando seu nome e seus documentos. Na Internet isso também pode ocorrer, caso alguém crie um perfil em seu nome em uma rede social, acesse ou falsifique sua conta de e-mail e envie mensagens se passando por você.

Quanto mais informações você disponibiliza sobre a sua vida e rotina, mais fácil se torna para um golpista furtar a sua identidade, pois mais dados ele tem disponível e mais convincente ele pode ser. Além disso, o golpista pode usar outros tipos de golpes e ataques para coletar informações sobre você, inclusive suas senhas.

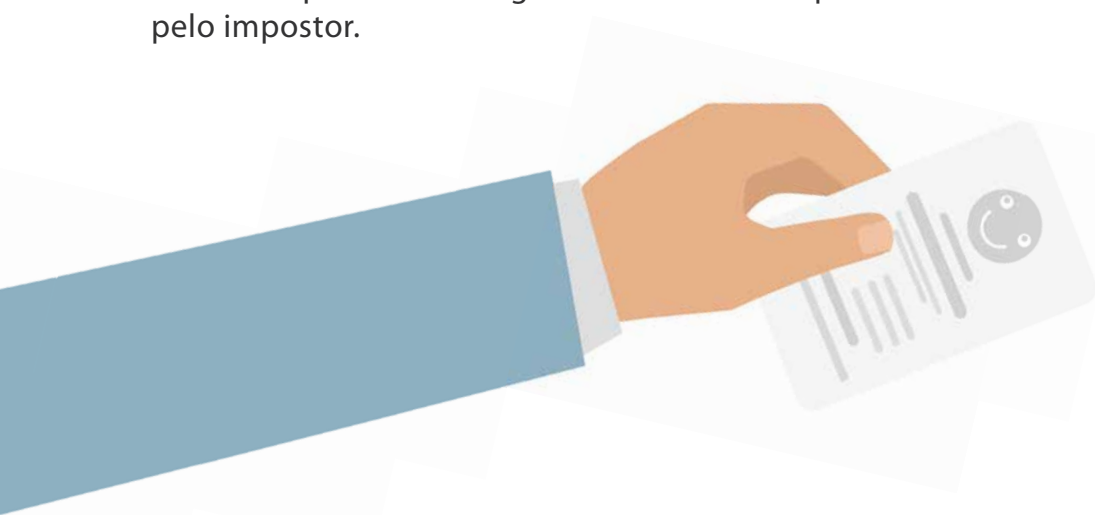
Caso a sua identidade seja furtada, você poderá arcar com consequências como perdas financeiras, perda de reputação e falta de crédito. Além disso, pode levar muito tempo e ser bastante desgastante até que você consiga reverter todos os problemas causados pelo impostor.

Como evitar o golpe:

A melhor forma de impedir que sua identidade seja furtada é evitar que o impostor tenha acesso aos seus dados e às suas contas de usuário. Além disso, para evitar que suas senhas sejam obtidas e indevidamente usadas, é muito importante que você seja cuidadoso, tanto ao usá-las quanto ao elaborá-las.

É necessário também que você fique atento a alguns indícios que podem demonstrar que sua identidade está sendo indevidamente usada por golpistas, tais como:

- Começar a ter problemas com órgãos de proteção de crédito;
- Receber o retorno de e-mails que não foram enviados por você;
- Verificar nas notificações de acesso que a sua conta de e-mail ou seu perfil na rede social foi acessado em horários ou locais em que você próprio não estava acessando;
- Ao analisar o extrato da sua conta bancária ou do seu cartão de crédito você percebe transações que não foram realizadas por você;
- Receber ligações telefônicas, correspondências e e-mails se referindo a assuntos sobre os quais você não sabe nada a respeito, como uma conta bancária que não lhe pertence e uma compra não realizada por você.



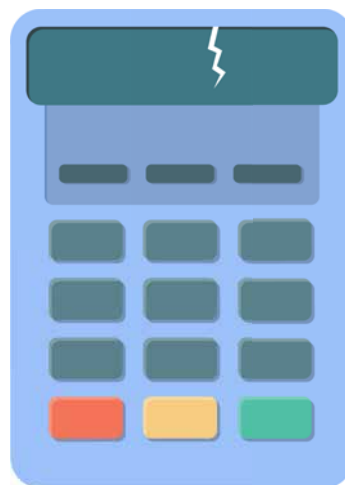
21 GOLPE DA MÁQUINA DE CARTÃO COM VISOR QUEBRADO

Os criminosos tentam persuadir a vítima no ato de entrega de delivery informando ao cliente que, devido à crise do coronavírus, o aplicativo cobra uma taxa adicional de R\$ 1,90 que deveria ser paga no cartão de débito.

O entregador então digita um valor muito acima do informado em uma maquininha com o visor quebrado/embaçado. Sem saber o valor da transação, o cliente digita a senha e confirma o pagamento.

Como evitar o golpe:

- Fique atento ao realizar compras por aplicativos de delivery;
- Procure realizar o pagamento pela plataforma de pedidos;
- Evite pagar valores a mais do que foi ofertado independente do motivo informado pelo entregador;
- Em caso de dúvidas, entre em contato com a central do aplicativo utilizado antes de realizar o pagamento.



22 GOLPE DA SELFIE

Alguns bancos e serviços online começaram a solicitar dos seus clientes o envio de selfies segurando um documento de identidade (RG ou CNH) para a abertura de conta bancária ou emissão de um cartão de crédito.

O que era para ser uma forma descomplicada para autenticar a identidade dos clientes e evitar deslocamentos e filas de espera, acabou virando uma nova forma de enganar as pessoas.

Os criminosos se adaptaram a essa nova prática e passaram a aplicar golpes solicitando a vítima o envio de selfies segurando um documento de identidade (RG ou CNH).

Os golpistas enviam e-mails de phishing se passando por um banco, empresa de pagamentos ou redes sociais. As mensagens pedem que, por medidas de segurança, os usuários confirmem sua identidade por meio de link. Ao clicar, a vítima é redirecionada à uma página de um formulário que solicita informações pessoais como endereço e número de telefone, além do upload de uma selfie com um documento de identidade oficial visível – até mesmo foto com cartão de crédito ou passaporte.

Com os dados das vítimas em mãos, eles podem criar contas bancárias visando a troca de criptomoedas, por exemplo – que servirá para lavar dinheiro de suas atividades.

Além disso, é importante frisar que uma selfie com um documento de identidade tem um valor muito alto no mercado negro em comparação com uma imagem digitalizada do mesmo documento.

Como evitar o golpe

- Verifique o texto do e-mail enviado, bem como as informações disponibilizadas. Um indicativo de fraude são erros gramaticais, palavras omitidas e erros de ortografia;
- Fique atento, pois os e-mails fraudulentos normalmente possuem endereços registrados em provedores gratuitos ou pertencem a empresas que não têm relação nenhuma com a mencionada no corpo da mensagem. Verifique de onde vem a mensagem e para onde o link leva;
- Verifique o endereço do remetente, pois embora pareça legítimo, é provável que o host do formulário de phishing esteja hospedado em um domínio mal-intencionado ou não relacionado, portanto veja os detalhes, pois muitas vezes o endereço pode ser muito parecido, mas ainda assim existem diferenças, e em outros, a diferença é notória;
- Desconfie de e-mails contendo mensagens “alerta” ou “urgência”. Ofertas muito atrativas são utilizadas pelos golpistas para tentar apressar o destinatário e persuadi-lo a fornecer informações;
- Fique atento a pedido de informações formalizados por terceiros online, para dados que você já tenha fornecido presencialmente. Normalmente no caso de bancos sua identidade já foi confirmada quando você abriu a conta, logo não faz sentido, o pedido formalizado virtualmente para confirmação. Nesse caso, é importante procurar informações no site oficial da empresa;
- Muitas soluções oferecem opções avançadas – incluindo de segurança – em troca de informações pessoais, mas na sua conta pessoal na web, não por e-mail. E, normalmente, é uma oferta que pode ser recusada. Porém, na forma em que o link de e-mail fraudulento é enviado, há apenas um botão como se sugerisse que não há outra opção além de enviar uma selfie. Em caso de dúvida, ligue para o atendimento ao cliente. Mas não use o número fornecido na mensagem: encontre-o no site oficial da empresa.



23 GOLPE USANDO O NOME DA RECEITA FEDERAL

Alguns fraudadores vêm utilizando um novo golpe para captar dados dos contribuintes utilizando o nome da instituição.

As principais formas de abordagens são:

- Encaminhar e-mails falsos utilizando o nome da instituição informando que “Consta um saldo residual do seu último IRPF”;
- Encaminhar e-mail falso usando o nome do fisco contendo a descrição de recebimento de intimação/comunicação da Receita Federal de inquérito ou notificação. Sempre acompanhado de anexo para atrair o clique do usuário no documento, visando com isso roubar os dados da vítima;
- Utilizar redes sociais e telefone para o envio de mensagens informando que existe uma encomenda contendo parte da sua mudança para o país ou algo de valor enviado a título de presente que está retido na Alfandega onde solicitam da vítima reiterados depósitos ou transferências em conta corrente para conseguir sua liberação.

A Receita Federal não encaminha e-mail ou mensagens, de qualquer tipo, que contenham dados do contribuinte, solicitem informações pessoais ou informem trâmites de imposto de renda e processo em andamento.

Segundo o fisco, a única mensagem que o contribuinte poderá receber, em seu e-mail ou celular, é um alerta sobre a existência de mensagens importantes no e-CAC (Centro de Atendimento Virtual). Nesse caso, ele deve acessar o e-CAC com sua senha para visualizar a mensagem.

Caso o e-mail recebido contenha valores e links para acesso, o contribuinte deve desconfiar de fraude.

Como evitar o golpe

Para evitar transtornos, a Receita Federal recomenda que o cidadão não clique em qualquer link em e-mail recebido em nome da instituição, mesmo que pareça legítimo. Abra o Portal e-CAC direto no site da Receita Federal e acesse com seu login e senha.



24 GOLPE DO PASSE EXPRESSO NO PEDÁGIO

Na tentativa de roubar o controle de contas de WhatsApp, bandidos têm usado o nome de algumas empresas que administram pedágio para enganar vítimas.

O criminoso entra em contato para falar sobre uma suposta cobrança duplicada e durante a conversa envia um suposto código de validação, cujo objetivo é clonar o celular e roubar dados pessoais.

Com essa pratica o cybercriminoso passa a ter acesso remoto do aplicativo de troca de mensagens WhatsApp e assim começa a se passar pela vítima e pedir dinheiro emprestado a parentes e amigos dos seus contatos.

Como evitar o golpe

- Nunca informe para terceiros qualquer número ou código que chegar via SMS no seu celular;
- Não clique em links, banners e outros anúncios recebidos por SMS, e-mail e mensagens de WhatsApp.



25 GOLPE DA PAQUERA VIRTUAL

Algumas formas de abordagem nos casos de relacionamento ou paquera virtual:

- Fazem perfis em aplicativos de namoro e tentam seduzir as vítimas para tirar proveito delas;
- Buscam identificar pessoas mais suscetíveis, mas TODOS são alvos em potencial;
- Fazem juras de amor de maneira precoce ou inapropriada;
- Buscam convencer as vítimas de inúmeras qualidades e, com isso, afastar possíveis desconfianças.

Como evitar o golpe

- Se for encontrar alguém, marque em um local público;
- Avise alguém da sua confiança sobre o encontro;
- Repasse informações sobre a pessoa que vai encontrar;
- Procure o perfil da paquera em outras redes sociais. Se só tiver perfil cadastrado em uma rede, fique alerta;
- Desconfie se a pessoa não atender ligações e chamadas de vídeo;
- Mantenha o seu perfil o mais privado possível;
- Informações pessoais ajudam na abordagem dos golpistas;
- Frases como “Nós temos que confiar um no outro” são frequentemente utilizadas pelos golpistas;
- Jamais dê dinheiro a alguém que conheceu pela internet e só mantém contatos virtuais.

26

DICAS E CUIDADOS PARA PRESERVAR SEUS DADOS NO AMBIENTE VIRTUAL

Enumeramos uma lista com algumas dicas de cuidados para preservar seus dados



1. CERTIFIQUE-SE QUE O SITE É SEGURO - É importante verificar se o site oferece segurança no registro dos dados pessoais e do número do cartão de crédito. Atente-se para a figura de um cadeado no canto direito superior da página na Internet e se o domínio do endereço é registrado no Brasil;

2. PROCURE IDENTIFICAR O VENDEDOR - O consumidor pode procurar na página dados como endereço, e-mail, e ainda o CNPJ ou CPF e fazer uma consulta no site da Receita Federal para ver se está ativo;

3. NÃO FAÇA DEPÓSITO NA CONTA DE PESSOA FÍSICA - Se você está comprando de uma loja, o pagamento deve ser feito à loja e não a terceiros. Ao receber boletos verifique os dados e certifique-se que estão de acordo com os dados do site;

4. EVITE CLICAR EM LINKS ENVIADOS POR TERCEIROS (SPAM) - Podem conter programas mal-intencionados capazes de capturar senhas e outras informações pessoais suas para uso indevido;

5. EVITE FAZER COMPRAS USANDO COMPUTADORES COMPARTILHADOS, LAN HOUSES OU CYBERCAFÉS;

6. INSTALE UM ANTIVÍRUS E ATUALIZE-O FREQUENTEMENTE;

7. AO EFETUAR COMPRAS ONLINE PRIORIZE A UTILIZAÇÃO DE CARTÃO VIRTUAL GERADO PELO APLICATIVO DO BANCO, que é válido apenas para uma compra;

8. JAMAIS DEIXE O CARTÃO SALVO PARA COMPRAS FUTURAS;**9. SE O SITE OFERECER A OPÇÃO DE ARMAZENAR SEUS DADOS BANCÁRIOS OU NÚMERO DO CARTÃO DE CRÉDITO NÃO ACEITE;**

10. VERIFIQUE OS PROCEDIMENTOS PARA RECLAMAÇÃO, DEVOLUÇÃO DO PRODUTO, PRAZO PARA ENTREGA – Procure no site as informações e os procedimentos que devem ser observados antes de concluir a compra;

11. GUARDE TODOS OS DADOS DA COMPRA - Armazene em meio físico ou eletrônico todas as informações pertinentes a compra como nome do site, itens adquiridos, valor pago e forma de pagamento, número de protocolo da compra ou do pedido, confirmação do pedido, e-mails trocados com o fornecedor que comprove a compra e suas condições;

12. VERIFIQUE SE HÁ DESPESAS COM FRETES E TAXAS ADICIONAIS, bem como o prazo de entrega da mercadoria ou execução do serviço;

13. NÃO COMPRE SE NÃO HOUVER SEGURANÇA - Se um site oferece uma excelente condição de compra, mas não preencher os requisitos de segurança, desista do negócio, por mais tentador que seja, e procure outro site ou vá a uma loja física.

14. VERIFIQUE A REPUTAÇÃO DA EMPRESA EM PLATAFORMAS COMO CONSUMIDOR.GOV ou RECLAME AQUI ANTES DE EFETUAR A COMPRA - Se a empresa apresenta um grande número de queixas e reclamações é bem provável que você seja o próximo a ter problemas.

15. PROPOSTAS MUITO ATRATIVAS PODEM SER ARMADILHAS – Faça uma análise da proposta e veja se o preço ofertado está dentro da média de mercado. Desconfie se o valor estiver muito abaixo, pode ser indicativo de armadilha;

16. NA COMPRA DE ELETRODOMÉSTICOS FIQUE ATENTO AS ESPECIFICAÇÕES COMO VOLTAGENS E VERIFIQUE SE HÁ REDE DE ASSISTÊNCIA TÉCNICA NA SUA REGIÃO;

17. NA COMPRA DE PRODUTOS VEJA TODAS AS ESPECIFICAÇÕES COMO TAMANHO, COR E ETC;

18. FIQUE ATENTO AO COMPROVANTE APÓS FINALIZAR COMPRA - A loja deverá enviar um comprovante do pedido e do pagamento. Se não receber, o consumidor deve exigir imediatamente. O comprovante será fundamental para eventual reclamação junto ao Procon ou em ação judicial;

19. VERIFIQUE OS DADOS DO BOLETO QUE ESTÁ PAGANDO PARA AFERIR SUA VERACIDADE;

20. JAMAIS SIGA O PASSO A PASSO ORIENTADO PELO DESCONHECIDO AO TELEFONE, e encurte a conversa;

21. NÃO RETORNE LIGAÇÕES, OS CRIMINOSOS CONSEGUEM INTERCEPTAR;

22. NÃO FORNEÇA INFORMAÇÕES PESSOAIS A ESTRANHOS informe pessoas da sua casa e de seu convívio, especialmente idosos e crianças sobre esses golpes e os oriente a não darem quaisquer informações pessoais a estranhos.





DefensoriaTO

| www.defensoria.to.def.br

NUDECON

Núcleo de Defesa
do Consumidor

»PE·TO

DEFENSORIA PÚBLICA
ESTADO DO TOCANTINS