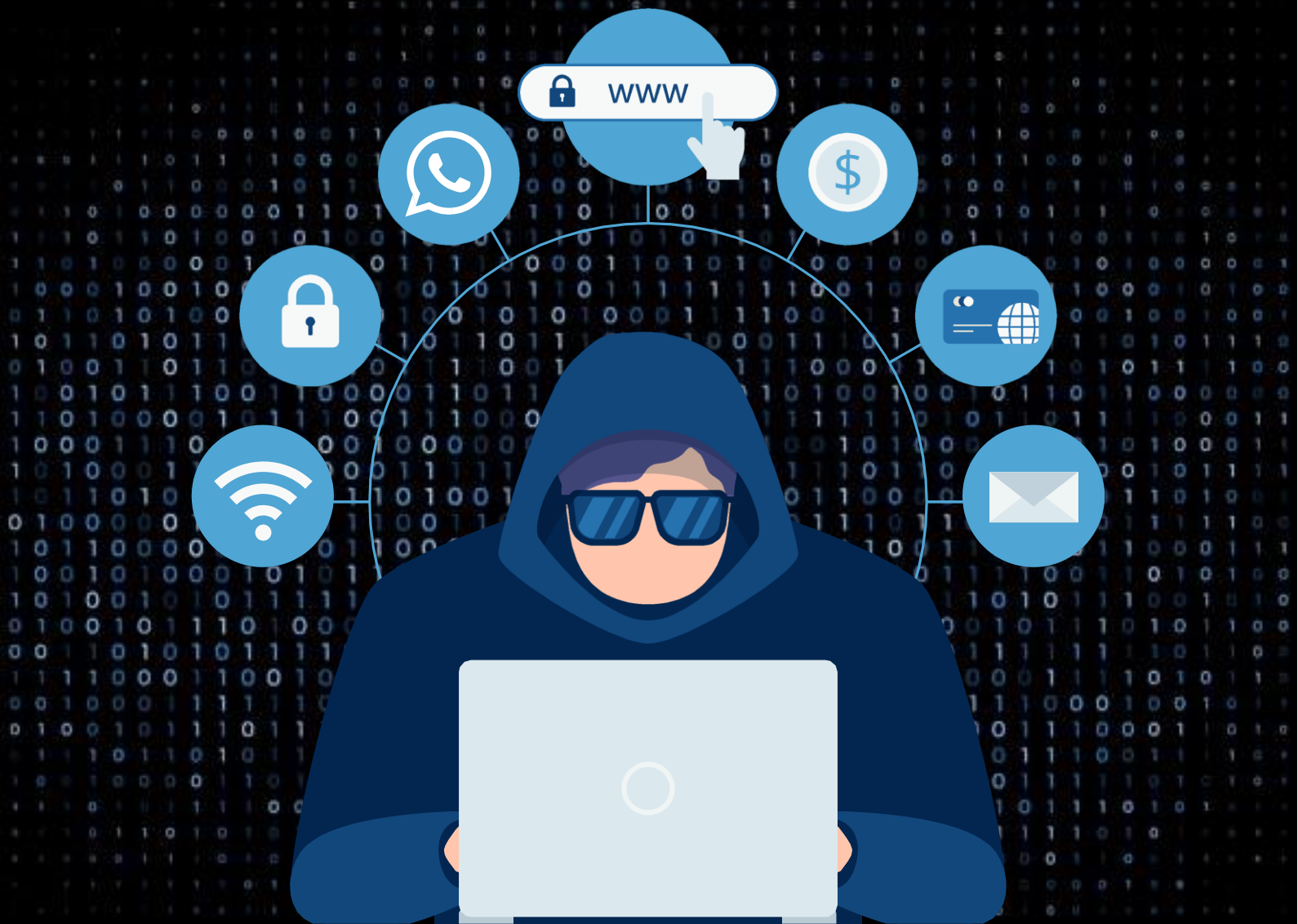
Golpes e Fraudes Desmascarados: Um Guia Abrangente para Proteger-se de Armadilhas



Sumário

"O segredo para a segurança é começar a pensar como um hacker."

Uma frase famosa atribuída a Kevin Mitnick, um renomado hacker e especialista em segurança

INTRODUÇÃO

Em um país onde a carga tributária representa 60% dos preços dos produtos, onde o sistema judiciário frequentemente falha na resolução da maioria dos crimes e onde os privilégios parecem beneficiar os infratores em detrimento dos cidadãos que obedecem à lei, o Brasil se tornou um ambiente propício para a proliferação da ilegalidade. O "jeitinho brasileiro", longe de ser apenas um traço cultural, tornou-se uma estratégia de sobrevivência em meio ao caos institucional.

Neste contexto, a cultura dos golpes se enraizou profundamente na identidade nacional. Para muitos, adaptar-se ao sistema corrupto é uma necessidade, pois pode significar a diferença entre prosperar ou ser prejudicado. Em um país como este, o desconhecimento das artimanhas do submundo pode ser fatal, enquanto o entendimento das táticas utilizadas pode ser a única defesa contra os vigaristas.

Este livreto não busca adotar um tom moralista nem encorajar práticas fraudulentas. Nosso objetivo é ampliar seu entendimento sobre as diversas manifestações desse universo obscuro e alertá-lo para os estratagemas que alguns indivíduos estão dispostos a empregar, frequentemente mirando você como alvo. Ao longo da leitura, serão apresentados diversos golpes e fraudes, cada um com sua própria narrativa e método de operação. Você perceberá que muitos seguem padrões semelhantes e aprenderá a identificá-los prontamente, mesmo diante de estratagemas desconhecidos. Este conhecimento pode ser crucial para evitar armadilhas e sair ileso.

CAPÍTULO 1 – O PERFIL DA VÍTIMA IDEAL

Os golpistas são habilidosos na arte da ilusão, utilizando mentiras de maneira estratégica para atrair suas vítimas. No entanto, o que pode parecer paradoxal à primeira vista é que muitos golpes são deliberadamente concebidos com erros gritantes, como se fossem armadilhas para atrair os mais ingênuos.

É nesse paradoxo que reside a engenhosidade dos golpes mais sofisticados. Os golpistas sabem que ao criar uma narrativa repleta de inconsistências e falhas evidentes, conseguem atrair exatamente o tipo de pessoa que procuram: aquela que está mais inclinada a acreditar no que deseja ouvir, mesmo que isso implique ignorar os sinais mais óbvios.

Esses golpes podem parecer tão absurdos e mal elaborados que é difícil acreditar que alguém poderia cair neles. No entanto, são justamente esses os que mais eficazmente funcionam.
Por quê?

Porque a natureza humana muitas vezes tende a confiar no improvável em detrimento do óbvio. Diante de algo tão inverossímil, muitas pessoas tendem a pensar: "Ninguém seria tão tolo a ponto de tentar isso se não fosse verdadeiro", e é aí que reside a armadilha.

Esses golpes exploram a vulnerabilidade humana, visando aqueles que estão mais dispostos a suspender sua descrença em troca de uma promessa tentadora. Eles apelam para a ganância, a ingenuidade e a desesperança, oferecendo soluções rápidas e fáceis para problemas complexos.

Ao encontrar uma vítima que se engaje com o golpe, apesar de todas as falhas gritantes, os golpistas sabem que encontraram a vítima perfeita.

CAPÍTULO 2 – TIPOLOGIAS DE GOLPES

Golpe do Reembolso

•**Estratégia:** Convencer empresas a conceder reembolsos mediante a alegação de erros no envio de produtos.

•**Detalhes:** Inclui a criação de números de rastreamento falsos e o aluguel massivo de livros para revenda com lucro, atividades que resultaram na prisão de indivíduos envolvidos.

O golpe frequentemente se baseia na alegação de não recebimento de produtos adquiridos ou na informação de que estes chegaram com defeitos. É comumente praticado em plataformas como Mercado Livre e Shopee, aproveitando-se da política flexível de algumas empresas de proceder com reembolsos ou novos envios sem exigir rigorosa verificação da reclamação inicial.

Ao alegar defeitos nos produtos recebidos, os golpistas muitas vezes criam números de rastreamento falsos para simular o retorno do item, enquanto o mantêm consigo. Esse expediente enganoso, por não estar registrado nos sistemas de rastreamento das lojas, geralmente leva à concessão automática de reembolsos ou substituições, em virtude das políticas de serviço ao cliente voltadas para proteger os consumidores.

Uma variante mais sofisticada deste golpe envolve o aluguel em grande escala de livros físicos da Amazon para posterior revenda. Após o aluguel, os golpistas afirmam não ter recebido o livro, lucrando substancialmente com esta prática. Um caso notório resultou na obtenção ilegal de mais de 1,5 milhões de dólares, culminando na prisão dos responsáveis.

Para informações detalhadas sobre um caso específico, recomenda-se consultar o artigo do The Register.

Compras Online com Cartões Clonados

Estratégia Utilizada por Golpistas

Método: Aquisição de cartões de crédito roubados para comprar produtos de alto valor.

Detalhes: Os golpistas utilizam VPNs, proxies residenciais e endereços falsos para evitar detecção.

Aquisição de Dados: Criminosos acessam sites como Joker's Stash ou UniCC para adquirir dados de cartões de crédito vazados.

Compra de Produtos: Com os dados em mãos, efetuam compras de itens caros, utilizando VPNs e proxies para mascarar sua localização e evitar rastreamento.

Entrega: Os golpistas solicitam a entrega dos produtos em depósitos ou áreas isoladas para ocultar seu endereço real.

Coleta: Alguns chegam ao ponto de se disfarçar com trajes de correios ou coletes fluorescentes, simulando ser entregadores legítimos, para retirar o produto sem levantar suspeitas.

Medidas de Proteção: para Varejistas
Para mitigar fraudes dessa natureza, varejistas devem adotar diversas medidas de segurança:

Monitoramento de Transações: Implementar sistemas de monitoramento de transações em tempo real que detectem atividades suspeitas, como compras de alto valor ou múltiplas tentativas de pagamento falhadas.

Autenticação Multifatorial: Exigir autenticação multifatorial (MFA) para compras online, aumentando a segurança além da simples inserção de dados do cartão de crédito.

Verificação de Endereços: Validar endereços de entrega, especialmente em casos de compras de alto valor, para identificar possíveis endereços falsos ou suspeitos.

Análise de Comportamento: Utilizar análises comportamentais para detectar padrões incomuns de compra que possam indicar fraude.
Educação e Treinamento: Treinar funcionários para reconhecer sinais de fraudes e adotar uma cultura de vigilância constante.

Colaboração com Autoridades: Estabelecer canais de comunicação com autoridades e outras empresas do setor para compartilhar informações sobre novos métodos de fraude e cooperar em investigações.
Implementando essas estratégias de segurança, os varejistas podem reduzir significativamente o risco de serem vítimas de fraudes com cartões de crédito, protegendo seus negócios e seus clientes.

Preenchimento de Pesquisas Falsas

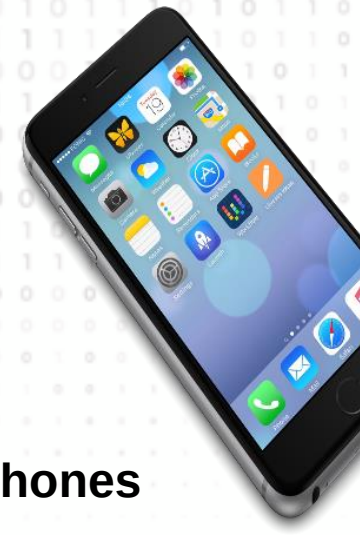
•**Estratégia:** Promoção de brindes falsos em troca de informações de cartão de crédito.

Detalhes: Utilização de influenciadores para persuadir pessoas a preencherem pesquisas, seguido pelo vazamento de dados pessoais.
Provavelmente você já se deparou com ofertas como "Preencha esta pesquisa rápida para concorrer a um iPhone ou ganhar gemas no Clash of Clans". Essas iniciativas frequentemente são promovidas por influenciadores, muitas vezes sem verificação adequada do que estão endossando.

A estratégia visa atrair especialmente crianças e idosos (selecionados pelo influenciador), com pesquisas de cerca de 10 minutos de duração - um período suficiente para manter o engajamento, mas não tão longo a ponto de desencorajar a participação. Ao final da pesquisa, solicita-se informações pessoais, incluindo dados do cartão de crédito sob o pretexto de "enviar o prêmio" ou "pagar o frete" (no caso de crianças, muitas vezes incentivadas a usar o cartão dos pais).

A lógica do "custo afundado" entra em jogo, onde a vítima, após investir tempo no preenchimento da pesquisa, é mais propensa a fornecer os dados pessoais solicitados. Este método permite que os golpistas obtenham dados de múltiplos indivíduos, que podem ser vendidos, usados para fraudes ou clonagens.

Esta prática, embora apresente um risco relativamente baixo, destaca a importância de educação e conscientização sobre segurança digital, especialmente em contextos em que a confiança é explorada para fins maliciosos.



Revenda Fraudulenta de Smartphones

•**Estratégia:** Aquisição de smartphones em lojas de telefonia mediante fraudes.

Detalhes: Revenda dos aparelhos com lucro, aproveitando-se da facilidade de obtenção através de operadoras.

O golpe envolve o recrutamento de pessoas com histórico de crédito negativo, muitas vezes moradores de rua, para comprar smartphones em nome delas em planos pós-pagos de operadoras. Estes planos frequentemente incluem a venda subsidiada do smartphone, como medida para reter clientes e evitar cancelamentos precoces.

A pessoa contratada para efetuar a compra geralmente não tem intenção de pagar as parcelas do plano, tornando o smartphone adquirido substancialmente barato. O golpista então compra o dispositivo por uma fração do seu valor real e o revende com uma margem de lucro significativa.

Em operações mais complexas, os golpistas coordenam a compra de múltiplos smartphones sob diferentes perfis, maximizando os lucros obtidos por meio deste esquema.

Este tipo de fraude representa um risco considerável tanto para as operadoras quanto para consumidores desavisados, destacando a importância de medidas rigorosas de segurança e verificação de crédito na concessão de dispositivos móveis.

Golpe de Depósito Bancário

•**Estratégia**: Utilização de informações bancárias para depositar cheques fraudulentos.

Detalhes: Impressão de cheques falsos, depósito móvel e subsequente retirada do dinheiro, deixando a vítima responsável pelo débito quando o cheque é identificado como fraudulento.

Este golpe visa explorar contas bancárias legítimas para acessar e retirar fundos antes que a instituição financeira detecte a fraude. Geralmente, os golpistas buscam indivíduos com contas bancárias que procuram maneiras rápidas de ganhar dinheiro. As vítimas são recrutadas por meio de anúncios online, redes sociais ou abordagens pessoais.

Os golpistas apresentam uma oferta atraente às vítimas, oferecendo uma oportunidade de ganho rápido em troca do depósito de cheques falsificados em suas contas bancárias. Eles prometem uma parte dos fundos depositados como compensação pela cooperação.

Após o acordo, os golpistas enviam cheques falsos às vítimas, criados com impressoras de cheques que produzem documentos aparentemente autênticos. As vítimas são instruídas a depositar esses cheques em suas contas bancárias. Os golpistas frequentemente pressionam as vítimas a agirem rapidamente, alegando urgência ou uma oportunidade limitada de ganho.

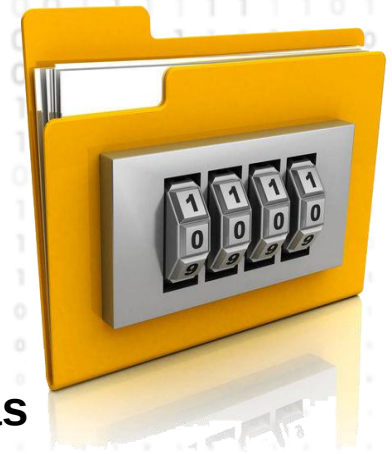
Imediatamente após o depósito, os fundos aparecem como "disponíveis" na conta da vítima antes que o banco possa verificar a autenticidade dos cheques. Isso pode levar a vítima a acreditar que o golpe foi bem-sucedido e que têm acesso aos fundos.

As vítimas são então orientadas a retirar rapidamente os fundos depositados, usualmente por transferência eletrônica, cheque ou saque em dinheiro. Os golpistas fornecem instruções detalhadas sobre como os fundos devem ser transferidos ou retirados.
Após algum tempo, o banco identifica os cheques como fraudulentos e reverte as transações. Isso deixa a vítima com saldo negativo e responsável por reembolsar o banco

pelo valor total dos cheques depositados, enquanto os golpistas desaparecem com os fundos retirados.

É importante ressaltar que nem todos os bancos liberam os fundos antes de verificar a legitimidade dos cheques. Esse golpe é eficaz apenas em instituições que realizam a verificação após o depósito dos fundos na conta.

Este tipo de fraude destaca a importância de vigilância e educação financeira para evitar ser vítima de atividades fraudulentas envolvendo depósitos bancários.



Combinação de Senhas

•**Estratégia:** Utilização de combinações de e-mails e senhas obtidas em vazamentos de dados

Detalhes: Acesso a contas e pedidos gratuitos em serviços online através de informações obtidas.

Periodicamente, determinados serviços online sofrem vazamentos de dados devido a ataques hackers. Quando isso ocorre, as informações de login e senha dos usuários são expostas publicamente. Empresas como Adobe, Sony e League of Legends já foram vítimas desses vazamentos, conhecidos como "data breaches".

A partir dos dados vazados, os fraudadores tentam utilizar as mesmas combinações de usuário e senha em outros serviços, especialmente em serviços de e-mail, que funcionam como uma chave mestra para o acesso a diversos aplicativos. Uma vez que obtêm sucesso, os fraudadores tentam converter esse acesso em ganhos monetários, seja acessando a conta bancária da vítima ou vendendo contas roubadas de jogos.

Geralmente, os vazamentos de dados ocorrem devido ao armazenamento inadequado das informações. De acordo com as melhores práticas de construção de sistemas, os servidores não deveriam lidar diretamente nem armazenar dados sigilosos dos usuários.
A conscientização sobre a importância de usar senhas únicas e seguras para cada serviço é crucial para mitigar o risco de ser vítima desse tipo de fraude.

Clonagem de WhatsApp

O golpe ocorre da seguinte forma:

O criminoso liga ou envia uma mensagem se passando por um funcionário de site de compra ou de um banco e diz que estará encaminhando um código promocional ou código de confirmação. Ele pede para que a vítima informe esse código que, na verdade, é a verificação do WhatsApp e com ele o criminoso consegue clonar a conta do consumidor.

Após a clonagem, o criminoso passa a enviar mensagens para os contatos da vítima, se passando por ela, pedindo dinheiro. As desculpas para solicitar dinheiro emprestado são as mais diversas, e na maioria das vezes os alvos principais da investida são os parentes mais próximos e amigos que, acreditando na mensagem, acabam depositando ou transferindo valores seguindo as coordenadas do criminoso.

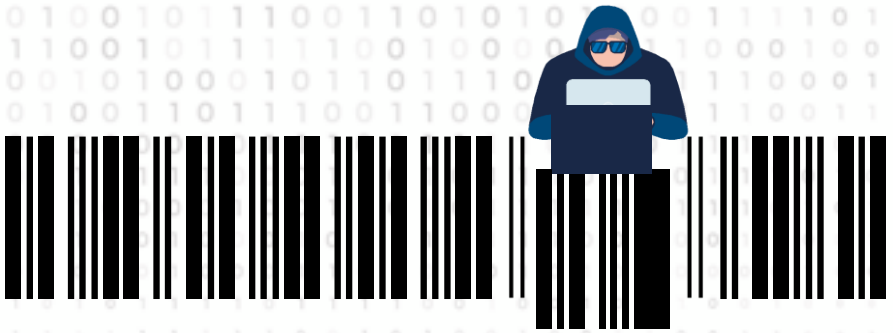
Como evitar o golpe:

a) Ative a "Confirmação em duas etapas" no WhatsApp. Acesse o link e veja como: **https://faq.whatsapp.com/general/verification/about-two-step-verification/?lang=pt_br**
b) NUNCA forneça o código verificador que você recebe via SMS em seu celular.
c) Não instale apps de terceiros ou compartilhe informações pessoais a pedido de ninguém pelo whatsapp.
d) Desconfie de situações em que a pessoa solicita a realização de transferências e pagamentos em caráter de urgência.
e) Ligue para a pessoa que solicitou o dinheiro e verifique se realmente é ela quem está solicitando a transação.

Caso tenha sido vítima, o que fazer:

Vítima do celular clonado
a) Envie um e-mail para support@whatsapp.com com o assunto "CONTA HACKEADA – DESATIVAÇÃO DE CONTA". Relate o ocorrido e siga as instruções do provedor.
b) Em posse de todas essas informações, procure a Delegacia de Polícia mais próxima de sua casa ou registre um Boletim de Ocorrência Eletrônico através do site da Delegacia Eletrônica **https://www.delegaciaeletronica.policiacivil.sp.gov.br/ssp-de-cidadao/home** na opção **OUTROS CRIMES.**
c) Peça para amigos e familiares excluírem o telefone clonado de grupos e alertarem o máximo de contatos em comum sobre o ocorrido.

Vítima foi quem fez o pagamento
a) Entre em contato com o banco e tente bloquear o valor.
b) Providencie cópia (prints) das conversas realizadas, bem como do comprovante de pagamento.
c) Em posse dessas informações, procure uma Delegacia de Polícia para o registro de Boletim de Ocorrência.



Boleto Falso

O golpe ocorre da seguinte forma:

O boleto de cobrança é um instrumento de pagamento pelo qual o emissor, denominado “Beneficiário”, receberá em sua conta o valor referente a um produto ou serviço.

O criminoso, valendo-se de engenharia social ou de um link fraudulento, **altera o código de barras** de modo que o valor caia na conta do integrante da quadrilha.

Como evitar o golpe:

a) Verifique se os dados do “Beneficiário” correspondem aos de quem lhe vendeu o produto ou serviço.
b) Confira se os três primeiros números do código de barras correspondem ao banco cuja logomarca aparece no boleto.
c) Desconfie se o código de barras estiver com falhas que apresentem espaços excessivos entre as barras ou qualquer outra alteração que impossibilite o reconhecimento pela leitora.
d) Sempre que tiver dúvidas sobre a veracidade de um boleto de cobrança, consulte diretamente o fornecedor que o emitiu.
e) Evite reimprimir boletos de cobrança em sites que não sejam do banco emissor do boleto. Evite negociar valores de descontos de boletos com pessoas estranhas, ou que se identificam como funcionários dos bancos ou de empresas de cobrança.

Caso tenha sido vítima, o que fazer:

a) Entre em contato com o banco e tente bloquear o valor.
b) Tire cópia do comprovante de pagamento e demais documentos correlatos.
c) Em posse de todas essas informações, procure a Delegacia de Polícia mais próxima de sua casa ou registre um Boletim de Ocorrência Eletrônico através do site da Delegacia Eletrônica **https://www.delegaciaeletronica.policiacivil.sp.gov.br/ssp-de-cidadao/home** na opção **OUTROS CRIMES.**

Fraudes bancárias

Alguns tipos de fraudes bancárias mais recorrentes:

Falso funcionário ou falsa central de atendimento: O estelionatário finge ser funcionário da instituição financeira e diz estar com problemas no cadastro ou irregularidades na conta. A vítima fornece informações sobre sua conta, e com isso o bandido realiza transações fraudulentas.

Falso motoboy: Integrantes da quadrilha ligam para a vítima e dizem pertencerem à central de relacionamento do banco. Afirmam que houve problemas com o cartão da vítima e pedem que ela digite sua senha numérica no teclado do telefone. Na sequência, dizem que enviaram um motoboy na casa da vítima para pegar o cartão. Em posse do cartão e a senha, realizam operações espúrias.

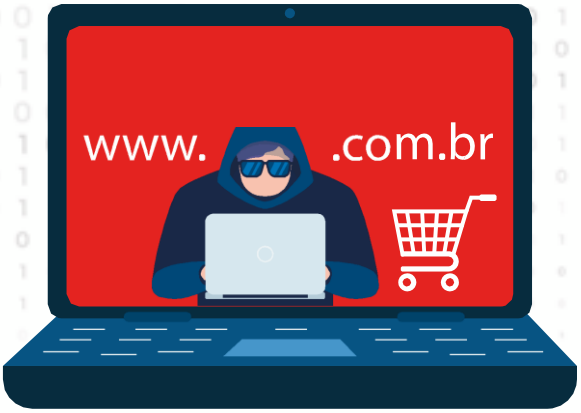
Phishing: O criminoso envia links, e-mails e SMS para a vítima com mensagens que, na maioria das vezes, exploram as emoções (curiosidade, oportunidade única, medo, etc), fazendo com que ela clique nos links e anexos que subtraem dados pessoais ou induzem a realizar cadastros ou fornecer informações.

Como evitar o golpe:

a) Evite usar computadores públicos e redes abertas de wi-fi para acessar conta bancária ou fazer compras online.
b) NUNCA abra e-mails de origem ou de procedência duvidosa.
c) Não execute programas, abra arquivos ou clique em links que estejam anexados ou no corpo desses e-mails.
d) Delete esses e-mails e, caso tenha clicado em alguma parte deste e-mail e executado um programa, comunique imediatamente ao seu banco o ocorrido e altere todas as suas senhas de acesso à sua conta bancária em outro computador confiável, ou no mesmo, após uma verificação completa de infecção de vírus por um técnico confiável;
e) NUNCA utilize seu cartão para fazer compras em sites desconhecidos.

Caso tenha sido vítima, o que fazer:

a) Entre em contato com o banco e tente bloquear o valor.
b) Tire cópia do comprovante de pagamento e demais documentos correlatos.
c) Em posse de todas essas informações, procure a Delegacia de Polícia mais próxima de sua casa ou registre um Boletim de Ocorrência Eletrônico através do site da Delegacia Eletrônica **https://www.delegaciaeletronica.policiacivil.sp.gov.br/ssp-de-cidadao/home** na opção **OUTROS CRIMES.**



Sites de comércio eletrônico fraudulentos

Prática criminosa que tem como alvo clientes de sites de comércio eletrônico.

O golpe ocorre da seguinte forma:

Nessa modalidade, o golpista cria uma página na internet muito semelhante à verdadeira, levando a vítima a acreditar que está efetuando uma compra legítima. Após selecionar os produtos e efetuar o pagamento, a vítima não recebe a mercadoria, quando então percebe que “caiu em um golpe”.

Para aumentar as chances de sucesso, o estelionatário utiliza artifícios, tais como: envio de spams, oferta de produtos com valor abaixo do valor de mercado, propagandas através de links patrocinados, dentre outros.

Além do comprador, as empresas que tiveram seus nomes utilizados indevidamente, ou ainda, as pessoas que tiveram seus dados utilizados para criação do site ou para a abertura de “empresas fantasmas”, também são vítimas.

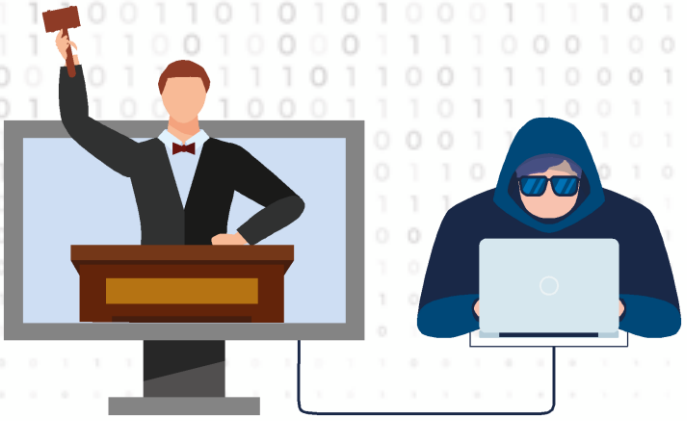
Como evitar o golpe:

Algumas dicas são indispensáveis, para que possamos ter a certeza que estamos fazendo uma compra legítima, com segurança:

a) Procure utilizar terminais (computador, smartphone, tablet) que sejam seguros;
b) Leia atentamente as informações dos sites e do produto que deseja comprar. Normalmente, sites fraudulentos podem conter erros de português ou ainda sobre as informações técnicas do produto. Verifique também se há CNJP cadastrado na página ou canais de comunicação;
c) Faça uma pesquisa de mercado do valor do produto que deseja adquirir. Desconfie de preços muito baixos;
d) Realize pesquisas na internet para obter informações a respeito da reputação do site em que deseja efetuar compras. Essas informações podem ser obtidas através do Reclame Aqui ou de redes sociais. É possível ainda verificar a lista de sites reprovados, disponibilizada pelo Procon (https://www.procon.sp.gov.br/).
e) Verifique se o site é seguro, localizando o ícone de um cadeado, ao lado do endereço do site (URL). Ao clicar no cadeado, será exibido o certificado de segurança da página;
f) Evite clicar em links que direcionam a navegação diretamente ao site de compras. Ao invés disso, prefira digitar o endereço do site (URL) junto à barra de endereço de seu navegador. **Atenção:** os sites fraudulentos geralmente possuem o endereço muito semelhante ao site verdadeiro. Exemplo: www.americanas.com.br (site verdadeiro) e www.lojasamercanas.com.br (site falso – exemplo fictício). Note que no exemplo do site falso foi incluído o nome “lojas” e a letra “i” do nome “americanas” foi suprimida.

Caso tenha sido vítima, o que fazer:

a) Verifique se o site ainda está ativo e copie seu endereço (URL);
b) Faça um print da página e do produto anunciado;
c) Providencie uma cópia do boleto ou dados bancários utilizados para o pagamento, bem como do comprovante do pagamento;
d) Em posse de todas essas informações, procure a Delegacia de Polícia mais próxima de sua casa ou rregistre um Boletim de Ocorrência Eletrônico através do site da Delegacia Eletrônica **https://www.delegaciaeletronica.policiacivil.sp.gov.br/ssp-de-cidadao/home** na opção **OUTROS CRIMES.**



Golpe do falso leilão ou falso empréstimo

O golpe ocorre da seguinte forma:

O Golpe do Falso Leilão trata-se de crime praticado pela internet, no qual o estelionatário cria um site falso, contendo fotografias de veículo para simular um leilão online. Após efetuar o lance, a vítima recebe a informação de que venceu o leilão e recebe um termo de arrematação, contendo instruções para a retirada do veículo e pagamento. Após transferir o valor para a conta indicada no termo de arrematação, a vítima não consegue mais nenhuma forma de contato com a empresa que realizava o leilão, quando percebe que caiu em um “golpe”.

Os falsos sites de leilão podem possuir informações de Leiloeiro que já atua no mercado, sem que ele tenha conhecimento de que seus dados estejam sendo utilizados indevidamente. As informações contidas nos sites falsos e os procedimentos adotados pela empresa durante o leilão induzem a vítima a acreditar que está realizando uma transação legítima. Assim como nos casos dos falsos sites de comércio eletrônicos, os preços baixos dos veículos leiloados atraem as vítimas.

Como evitar o golpe:

Algumas dicas são indispensáveis para que possamos ter a certeza que estamos fazendo uma compra legítima, com segurança:

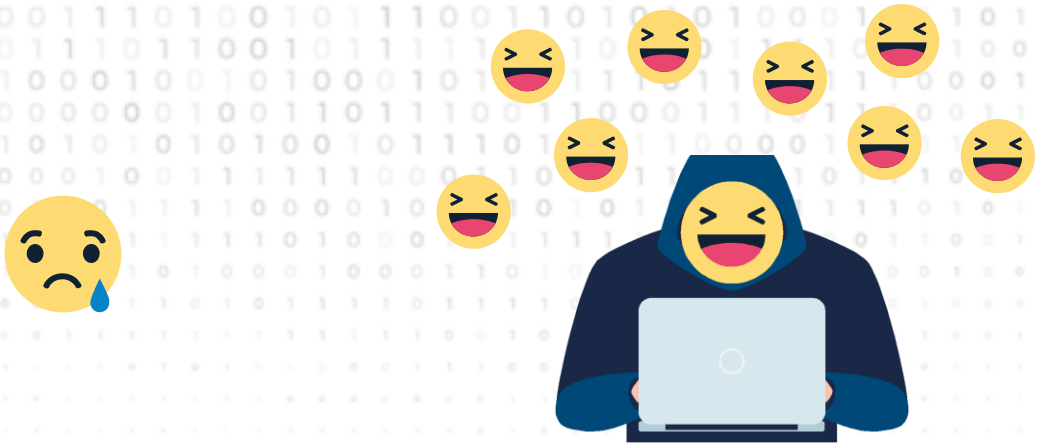
a) Procure utilizar terminais (computador, smartphone, tablet) que sejam seguros;
b) Leia atentamente as informações contidas no site e do veículo que deseja arrematar. Normalmente sites fraudulentos podem conter erros de português e erros nas especificações técnicas do veículo leiloado.
c) Pesquise o CNPJ e do endereço informados junto ao site;
d) Desconfie de preços muito baixos e faça uma pesquisa em relação ao veículo que deseja arrematar;
e) Realize pesquisas na internet para obter informações a respeito da reputação do site. Essas informações podem ser obtidas através do Reclame Aqui ou de redes sociais. É possível ainda verificar a lista de sites reprovados, disponibilizada pelo Procon (**https://www.procon.sp.gov.br/**);
f) Verifique se o site é seguro, localizando o ícone de um cadeado, ao lado do endereço do site (URL). Ao clicar no cadeado, será exibido o certificado de segurança da página;
g) Confira para quem o pagamento está sendo realizado. No termo de arrematação, a conta bancária informada para a transferência deve estar em nome do Leiloeiro. Não efetue o pagamento, caso haja qualquer divergência;
h) Evite clicar em links que direcionam a navegação diretamente ao site de leilão online. Ao invés disso, prefira digitar o endereço do site (URL) junto à barra de endereço de seu navegador.

Atenção: os sites fraudulentos geralmente possuem o endereço muito semelhante ao site verdadeiro, sendo modificado de forma quase imperceptível, portanto, verifique atentamente o endereço a fim de se certificar se o site em que está se conectando é o site verdadeiro.

Caso tenha sido vítima, o que fazer:

a) Verifique se o site ainda está ativo e copie seu endereço (URL);
b) Faça um print da página e do produto anunciado;
c) Providencie uma cópia do termo de arrematação, boleto ou dados bancários utilizados para o pagamento, bem como do comprovante do pagamento;
d) Em posse de todas essas informações, procure a Delegacia de Polícia mais próxima de sua casa ou registre um Boletim de Ocorrência Eletrônico através do site da Delegacia Eletrônica **https://www.delegaciaeletronica.policiacivil.sp.gov.br/ssp-de-cidadao/home** na opção **OUTROS CRIMES.**

Importante: Realize contato com a instituição bancária utilizada para efetuar o pagamento, para verificar a possibilidade de bloquear o valor na conta beneficiada.



Crimes contra a honra

O golpe ocorre da seguinte forma:

Infelizmente as redes sociais têm sido utilizadas por criminosos para ofender a honra de outrem ou até mesmo para cometer ameaças a integridade física de pessoas de bem. A honra, na concepção comum, pode ser entendida como um conjunto de atributos morais, intelectuais e físicos de uma pessoa.

O Direito Penal protege o bem jurídico da honra objetiva, por meio da caracterização do crime de **calúnia**, que diz respeito a conduta da pessoa que imputa, falsamente, fato tipificado e penalizado como crime a outrem.

Da mesma forma há reprimenda legal para conduta da pessoa que denegrir a imagem ou reputação de outra pessoa, divulgando algum fato ofensivo, assim estaremos diante do delito de **difamação**.

Agora, quem ofende o decoro de outrem, incitando atributos ou qualidades negativas, defeitos, poderá responder pelo crime de **injúria**.

Caso tenha sido vítima, o que fazer:

a) Se a conversa ocorreu em rede social, salve o nome do perfil e o link completo do perfil (endereço completo que aparece ao se clicar na barra de endereço);
b) Em posse de todas essas informações, procure a Delegacia de Polícia mais próxima de sua casa ou registre um Boletim de Ocorrência Eletrônico através do site da Delegacia Eletrônica https://www.delegaciaeletronica.policiacivil.sp.gov.br/ssp-de-cidadao/home na opção **OUTROS CRIMES.**
c) O Código Civil assegura a reparação dos danos morais e físicos sofridos e oriundos de ato ilícito, portanto, procurar um advogado para ingressar com ação civil pertinente.

“Ransonware” (sequestro de dados)

O golpe ocorre da seguinte forma:

O ransomware é um vírus que “tranca” os seus dados até o pagamento de um resgate.

Na maioria das vezes a invasão ocorre no período da noite ou madrugada, momento em que um criminoso virtual invade o dispositivo da vítima e instala um software capaz de criptografar (codificar) as informações de seu computador. Ao acessar o computador após tal procedimento, a vítima receberá uma mensagem de que seus dados foram criptografados e se ela não realizar um pagamento exigido pelo criminoso, normalmente em bitcoins, a vítima perderá todos os dados do computador invadido.

Como evitar o golpe:

a) Mantenha *backup* atualizado do computador, de preferência em HD externo ou *pen drive* e nunca os deixe espetados no computador, pois também poderão ser invadidos ou infectados;
b) Mantenha antivírus e *firewalls* sempre ativados e atualizados;
c) Evite acesso a sites suspeitos;
d) Não clique em *links* duvidosos de *e-mails* suspeitos.

Caso tenha sido vítima, o que fazer:

a) Não apague os *e-mails* e/ou mensagens recebidas do criminoso;
b) Se houver conversa com o criminoso via rede social, salve o nome do perfil e o *link* completo do perfil (endereço completo que aparece ao se clicar na barra de endereço);
c) Em caso de contato por telefone, faça uma relação todos os números de telefone utilizados pelo criminoso, contendo data e horário das conversas;
d) Anote os dados de eventuais contas bancárias, inclusive carteiras eletrônicas de bitcoins informados pelo criminoso;
e) Em posse de todas essas informações, procure a Delegacia de Polícia mais próxima de sua casa ou registre um Boletim de Ocorrência Eletrônico através do site da Delegacia Eletrônica https://www.delegaciaeletronica.policiacivil.sp.gov.br/ssp-de-cidadao/home na opção **OUTROS CRIMES.**

Loverboy Scam / Golpe do amor / Golpe sentimental

O golpe ocorre da seguinte forma:

Pessoas que estão em busca de um relacionamento amoroso, utilizam plataformas digitais para encontrar o par perfeito. Desta forma, criminosos criam perfis falsos nesses *sites* de relacionamento e, a princípio, por meio de conversas sedutoras e juras de amor, tentam ganhar a confiança da vítima.

Em um segundo momento, após envolver a vítima com declarações de amor, o golpista cria inverdades com intuito de obter vantagem econômica, em prejuízo da vítima.

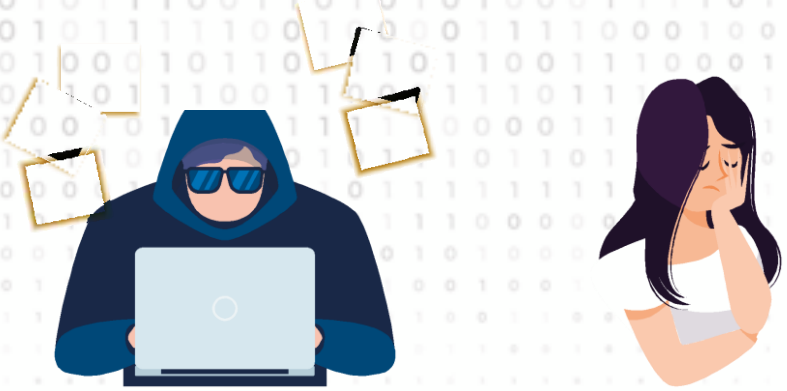
As mentiras utilizadas pelos criminosos são as mais diversas como, por exemplo, usar a desculpa de que deseja conhecer pessoalmente a vítima e então pedir dinheiro emprestado a ela para comprar supostas passagens; ou então o estelionatário diz que está enviando um presente (jóia, ouro, dólares), mas que para retirar o pacote será necessário pagar uma taxa, fornecendo então uma conta bancária de pessoas de confiança do próprio golpista.

Como evitar o golpe:

a) Procure marcar encontros **pessoais** com o namorado(a) e, preferencialmente, em **locais públicos**;
b) Desconfie da solicitação de empréstimo de altos valores, independentemente da situação relatada;
c) Dialogue com parentes e amigos sobre o seu relacionamento e peça opinião deles sobre qualquer pedido de valor;

Caso tenha sido vítima, o que fazer:

a) Não apague nenhuma da conversas realizadas com o possível criminoso;
b) Tire cópia de todas estas conversas e comprovantes de depósitos ou transferências bancárias realizadas;
c) Anote os dados das contas bancárias para as quais o dinheiro foi enviado, entre em contato com o gerente de sua conta bancária e tente bloquear o valor.
d) Em posse de todas essas informações, procure a Delegacia de Polícia mais próxima de sua casa ou registre um Boletim de Ocorrência Eletrônico através do site da Delegacia Eletrônica https://www.delegaciaeletronica.policiacivil.sp.gov.br/ssp-de-cidadao/home na opção **OUTROS CRIMES.**



Sextorsão

O que é?

É a ameaça de se divulgar imagens ou vídeos íntimos para forçar alguém a fazer algo, seja por vingança, humilhação ou para obter vantagem financeira. É uma forma de violência grave que pode levar a consequências extremas como o suicídio da vítima.

O golpe ocorre da seguinte forma:

As vítimas podem compartilhar uma imagem por um impulso, podem ter tido um relacionamento com o agressor, ou apenas acreditam que ele já tenha alguma imagem íntima delas porque ele insiste que tem; há casos de adolescentes que acreditam estarem conversando com outros adolescentes e enviam fotos íntimas, mas na verdade estão conversando com um criminoso; A obtenção de imagens ou vídeos íntimos também pode acontecer após invasão de contas e/ou dispositivos (hack) ou mediante falsas ofertas de emprego em agências de modelos, em que se pedem fotos e vídeos íntimos. Após obtenção do conteúdo íntimo, as vítimas são ameaçadas para enviarem mais fotos/vídeos, para participarem de um encontro sexual real ao vivo ou para pagarem determinada quantia em dinheiro, tudo em troca de não terem suas imagens íntimas expostas.

Como evitar o golpe:

a) Evite compartilhar fotos e vídeos íntimos;
b) Evite manter fotos e vídeos íntimos em seu celular – caso ele seja roubado o criminoso poderá ter acesso a esse conteúdo;
c) Desconfie de pedidos de amizade vindos de desconhecidos;
d) Evite participar de chamadas de vídeo com desconhecidos e lembre-se que a imagem da pessoa que você está vendo pode ser falsa!
e) Tenha sempre antivírus instalado em seu terminal.

Caso tenha sido vítima, o que fazer:

a) Não apague as conversas mantidas com o criminoso;
b) Se a conversa ocorreu em rede social, salve o nome do perfil e o link completo do perfil (endereço completo que aparece ao se clicar na barra de endereço);
c) Em caso de contato por telefone, faça uma relação todos os números de telefone utilizados pelo criminoso, contendo data e horário das conversas;
d) Anote os dados de eventuais contas bancárias informados pelo criminoso;
e) Em posse de todas essas informações, procure a Delegacia de Polícia mais próxima e sua casa ou registre um Boletim de Ocorrência Eletrônico através do site da Delegacia Eletrônica **https://www.delegaciaeletronica.policiacivil.sp.gov.br/ssp-de-cidadao/home** na opção **OUTROS CRIMES.**

Golpes envolvendo PIX

As recomendações com relação às transações PIX são, em geral, as mesmas para proteger o acesso a serviços financeiros já utilizados, como TED e DOC.

Não entre em sites ou instale no celular aplicativos desconhecidos;

Não há sites ou aplicativos do Banco Central ou do Pix criados exclusivamente para cadastramento das chaves, nem para a realização das transações Pix;

O cadastramento das chaves é realizado em ambiente logado no aplicativo ou site da sua instituição de relacionamento, o mesmo que já é utilizado para as demais transações financeiras, como consultar saldo, fazer transferências ou tomar dinheiro emprestado;

O cadastramento das chaves requer o consentimento do cliente e para cadastrar a chave Pix é feita uma validação em duas etapas. O cadastro do número de celular ou do e-mail como chave Pix depende da confirmação por meio de um código que será enviado, por exemplo, por SMS ou para o e-mail informado.

Já o CPF/CNPJ só pode ser usado como chave se estiver vinculado à conta, informação necessária no momento de sua abertura, comprovada por meio de documento.

Se o usuário tem dúvidas, procure se informar através do site da sua instituição de relacionamento.

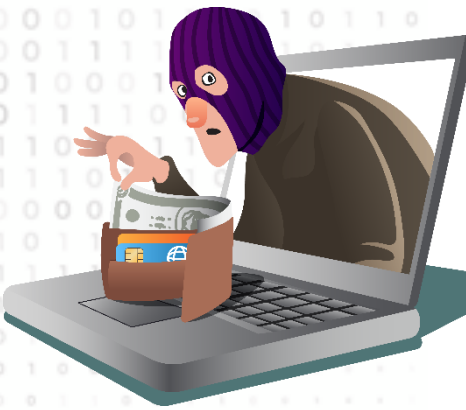
Não há prazo para o cadastramento das chaves, começou em 05/10 e estará sempre disponível.

Caso tenha sido vítima, o que fazer:

1) Reunir toda documentação da transação (extratos, comprovantes, etc)

2) Registre um Boletim de Ocorrência Eletrônico através do site da Delegacia Eletrônica https://www.delegaciaeletronica.policiacivil.sp.gov.br/ssp-de-cidadao/home na opção **OUTROS CRIMES** ou registre os fatos presencialmente no Distrito Policial mais próximo da residência.

3) Cientificar o prestador de serviço de pagamento para eventual ressarcimento, após análise dos documentos.



Apropriação de Identidade

•**Estratégia:** Obtenção de informações pessoais para solicitar cartões de crédito em nome de terceiros.

A apropriação de identidade envolve a obtenção de informações pessoais comprometidas, como números de RG e perfis de crédito. Utilizando esses dados, os golpistas se apropriam da identidade da vítima para solicitar cartões de crédito e realizar compras e empréstimos, sem a intenção de pagar as faturas.

Este esquema é sofisticado e de alto risco, exigindo múltiplas etapas para ser executado com sucesso, minimizando rastros deixados. Alguns golpistas obtêm empregos em empresas de telemarketing ou atendimento ao cliente para coletar dados pessoais de clientes através de sistemas como Lemit e InTouch.

Com acesso a esses dados, o golpista pode facilmente cruzar informações e assumir a identidade de clientes, criando contas em bancos digitais ou até mesmo realizando procurações falsas em nome da vítima para abrir contas em bancos físicos.

A sofisticação deste tipo de fraude destaca a importância de medidas rigorosas de proteção de dados e vigilância constante sobre o uso de informações pessoais para evitar a apropriação de identidade.

Acesso a Canais de Comunicação Empresarial

•**Estratégia:** Tentativa de acesso a canais corporativos com informações financeiras sensíveis.
Detalhes: Obtenção de informações e tentativa de alteração de instruções financeiras para desviar fundos.

Descrição da Ameaça
O golpe de acesso a canais de comunicação empresarial é similar ao golpe de phishing de bancos. O fraudador envia um e-mail para um funcionário da empresa, contendo um link falso para login na conta de comunicação corporativa. Os canais mais visados incluem Microsoft Teams, Slack, Google Workspace, Meta, e Skype. O objetivo é obter as credenciais do funcionário para que o fraudador possa acessar sua conta e descobrir informações internas e confidenciais da empresa.

Possíveis Consequências
Extorsão e Chantagem: Com acesso a informações sensíveis, o fraudador pode chantagear a empresa, exigindo um resgate para não divulgar os dados.

Uso de Informações Privilegiadas: Em empresas de capital aberto, o fraudador pode operar ações na bolsa com base em informações privilegiadas.

Alterações e Movimentações Financeiras: Dependendo do nível de permissão da conta do funcionário, o fraudador pode fazer alterações diretas e até mesmo movimentações financeiras, desviando fundos.

Medidas Preventivas
Educação e Treinamento: Realizar treinamentos regulares para funcionários sobre segurança digital e como identificar e-mails de phishing.

Autenticação Multifator (MFA): Implementar MFA para todos os acessos a sistemas corporativos, dificultando o acesso indevido.

Monitoramento Contínuo: Utilizar ferramentas de monitoramento para detectar atividades suspeitas em contas corporativas.
Atualizações e Patches: Manter todos os sistemas e softwares atualizados com as últimas patches de segurança.

Conclusão
A segurança da comunicação empresarial é crucial para proteger informações sensíveis e evitar perdas financeiras significativas. Implementar estratégias de prevenção e conscientização é fundamental para mitigar os riscos associados a esses tipos de ataques.

Skimming ou Chupa Cabra

•**Estratégia:** Clonagem de cartões das vítimas
Detalhes: Utilização de máquinas de venda e/ou caixas de lojas com dispositivos de cartão adulterados

Descrição da Ameaça

O golpe de clonagem de cartões envolve a duplicação das informações de cartões legítimos para realizar compras fraudulentas. Para isso, os golpistas utilizam dispositivos chamados "skimmers", que copiam os dados dos cartões. Originalmente, esses dispositivos eram usados para cartões que precisavam ser inseridos nas máquinas. Atualmente, com a popularização dos cartões de aproximação, os skimmers mais comuns são os de RFID (Radio Frequency Identification).

Possíveis Consequências

Perda Financeira: Realização de compras fraudulentas em nome da vítima, resultando em perdas financeiras.

Dificuldade na Detecção: Devido ao uso frequente de cartões em diferentes locais, é difícil identificar o ponto exato onde a clonagem ocorreu.

Comprometimento de Dados Pessoais: Clonagem de informações sensíveis que podem ser utilizadas para outras fraudes.
Exemplos de Skimmers

Estratégias dos Golpistas

Máquinas de Venda Adulteradas: Muitos golpistas adquirem máquinas de venda automática especificamente para clonar informações de cartões. Essas máquinas frequentemente bloqueiam outros métodos de pagamento, como PIX e dinheiro.

Funcionários Corruptos: Algumas pessoas trabalham como caixas em drive-thrus e lojas de varejo apenas para clonar cartões, utilizando skimmers disfarçados.

Medidas Preventivas

Verificação de Máquinas: Suspeitar de máquinas de venda que aceitam exclusivamente pagamentos por cartão, recusando outros métodos como PIX ou dinheiro.
Monitoramento de Transações: Acompanhar regularmente as transações bancárias para identificar rapidamente quaisquer atividades fraudulentas.

Uso de Cartões Virtuais: Sempre que possível, utilizar cartões virtuais para compras online ou em locais menos conhecidos.

Educação e Conscientização: Informar os consumidores sobre os riscos e métodos de prevenção contra clonagem de cartões.

Conclusão

A clonagem de cartões é uma ameaça real e crescente, facilitada pelo uso de dispositivos tecnológicos sofisticados. A conscientização e a adoção de práticas preventivas são essenciais para proteger informações financeiras e reduzir o risco de fraudes.

Fraude de Títulos

•**Estratégia:** Alteração de registros de propriedade de terceiros
Detalhes: Suborno de funcionários para acesso e modificação de registros de propriedade no sistema

Descrição da Ameaça

A fraude imobiliária tem suas raízes na prática histórica de grilagem no Brasil. Antigamente, falsificava-se uma escritura de propriedade e deixava-se o documento em uma gaveta com grilos. Os grilos liberavam uma enzima que amarelava o papel, dando-lhe uma aparência envelhecida e, portanto, mais credível. Daí vem o termo "grilagem".

Estratégias Modernas

Atualmente, a fraude de títulos envolve a cooptação de funcionários de cartórios de registro de imóveis para alterar registros de propriedade no sistema. Alguns indivíduos prestam concursos públicos especificamente para assumir posições que lhes permitam cometer este tipo de fraude. Outros subornam funcionários existentes, oferecendo uma fração do valor da propriedade em troca da alteração dos registros.

Possíveis Consequências

Transferência Ilegal de Propriedade: Os registros alterados podem transferir propriedades valiosas ilegalmente, resultando em perdas significativas para os proprietários legítimos.
Litígios e Complicações Legais: A descoberta da fraude pode levar a longas batalhas legais para recuperar a propriedade, envolvendo altos custos e complicações jurídicas.
Desconfiança no Sistema: Tais fraudes abalam a confiança no sistema de registro de imóveis, prejudicando a credibilidade das instituições envolvidas.

Medidas Preventivas

Auditorias e Verificações Regulares: Implementar auditorias frequentes e rigorosas nos registros de propriedade para detectar e prevenir alterações fraudulentas.
Treinamento e Conscientização: Capacitar funcionários de cartórios sobre ética e integridade, além de reforçar a importância de seguir protocolos de segurança.
Tecnologia de Segurança: Utilizar tecnologias avançadas de segurança, como blockchain, para assegurar a integridade dos registros de propriedade.

Denúncia Anônima: Estabelecer canais de denúncia anônima para que funcionários possam relatar tentativas de suborno ou atividades suspeitas sem medo de retaliação.

Conclusão

A fraude de títulos é uma ameaça grave com potencial de causar perdas financeiras massivas e danos à confiança no sistema de registro de imóveis. A implementação de medidas preventivas robustas, juntamente com auditorias rigorosas e tecnologias de segurança avançadas, é essencial para proteger os registros de propriedade e garantir a integridade do sistema.

Sim Swapping (Troca de Chip SIM)

•**Estratégia:** Troca involuntária do número de celular da vítima
Detalhes: O golpista liga para a operadora de telefonia da vítima e solicita a troca do chip para um número em sua posse

Descrição da Ameaça

No golpe de SIM Swapping, o fraudador utiliza dados pessoais e o número de celular da vítima para entrar em contato com a operadora de telefonia, se passando por ela. O golpista solicita a troca do chip SIM para um novo, que está em sua posse.

Execução do Golpe

Devido aos métodos inseguros que muitas operadoras utilizam para a troca de números, este procedimento muitas vezes é suficiente para que a troca seja realizada sem verificação adicional.

Possíveis Consequências

Interceptação de Mensagens: Após a troca, todos os SMS e mensagens destinadas ao número original da vítima são direcionados ao golpista.

Acesso a Contas: Com acesso às mensagens de autenticação de dois fatores (2FA), o golpista pode acessar contas de e-mail, redes sociais e bancos da vítima.

Roubo de Identidade: O controle do número de telefone permite ao golpista realizar diversas outras fraudes, explorando a identidade da vítima.

Medidas Preventivas

Autenticação Multifator: Utilizar métodos de autenticação multifator que não dependam apenas do número de telefone, como aplicativos autenticadores ou chaves de segurança.
Segurança com a Operadora: Solicitar à operadora de telefonia a implementação de senhas adicionais ou verificações de segurança para qualquer solicitação de troca de chip SIM.

Monitoramento de Contas: Acompanhar regularmente as atividades de suas contas bancárias e de e-mail para identificar rapidamente quaisquer acessos não autorizados.
Educação e Conscientização: Informar os usuários sobre os riscos do SIM Swapping e os métodos de proteção disponíveis.

Conclusão

O SIM Swapping é um método de fraude que explora falhas na segurança das operadoras de telefonia para obter acesso a informações sensíveis e contas pessoais. A conscientização sobre este golpe e a implementação de medidas preventivas são essenciais para reduzir o risco e proteger informações pessoais e financeiras.

Shotgun Scam (Golpe do Tiro Espalhado)

•**Estratégia:** Requisição de vários empréstimos e financiamentos simultaneamente

Detalhes: Aproveitamento do atraso na atualização do cadastro de crédito para obter múltiplos empréstimos antes da atualização

Descrição da Ameaça

O método "shotgun" explora a demora na atualização do score de crédito para obter múltiplos empréstimos e financiamentos simultaneamente. Normalmente, ao aceitar uma oferta de empréstimo, o cadastro de crédito do solicitante é alterado, dificultando a obtenção de outro empréstimo antes da quitação do primeiro.

Execução do Golpe

Solicitação Simultânea: O golpista solicita vários empréstimos e financiamentos ao mesmo tempo, aproveitando o atraso na atualização do score de crédito.

Recebimento dos Fundos: Com o cadastro de crédito ainda não atualizado, o golpista consegue aprovações para várias ofertas de crédito antes que o sistema registre as novas dívidas.

Possíveis Consequências

Sobreendividamento: O golpista pode acumular uma quantidade de dívidas que não consegue pagar, resultando em problemas financeiros severos.
Impacto no Crédito: O atraso no pagamento dos múltiplos empréstimos afetará negativamente o score de crédito a longo prazo.
Prejuízos para Instituições Financeiras: As instituições financeiras podem sofrer perdas significativas devido à incapacidade do golpista de honrar os compromissos.

Medidas Preventivas

Monitoramento em Tempo Real: Implementar sistemas de monitoramento em tempo real para atualizações de crédito, reduzindo o atraso entre a concessão de um empréstimo e a atualização do cadastro.

Verificação Adicional: Realizar verificações adicionais para pedidos simultâneos de crédito, identificando comportamentos suspeitos.
Educação Financeira: Informar os consumidores sobre os riscos de solicitar múltiplos empréstimos simultaneamente e promover práticas financeiras responsáveis.

Conclusão

O "shotgun scam" é uma fraude que tirar vantagem das falhas na atualização de cadastros de crédito para obter múltiplos empréstimos simultaneamente. A conscientização sobre este golpe e a implementação de sistemas de monitoramento em tempo real são essenciais para proteger tanto os consumidores quanto as instituições financeiras de prejuízos significativos.

Príncipe da Nigéria

•**Estratégia:** Apelo emocional e promessa de ganhos rápidos

Detalhes: Promessa de uma herança substancial, exigindo apenas um "pequeno pagamento" para sua liberação

Descrição da Ameaça

O golpe do Príncipe da Nigéria é um dos mais conhecidos e persistentes. Um golpista entrará em contato com a vítima, alegando que um príncipe da Nigéria (ou de qualquer lugar remoto) faleceu recentemente, deixando uma herança significativa. Após verificar que a vítima é a única beneficiária possível, o golpista oferece a oportunidade de receber essa herança, solicitando apenas um pequeno pagamento para liberar os fundos.

Execução do Golpe

Manipulação Emocional: O golpista utiliza apelos emocionais, como a promessa de uma herança substancial, para atrair a vítima.

Incremento da Credibilidade: Para ganhar a confiança da vítima, o golpista pode criar uma fachada elaborada, fazendo-a crer que há uma estrutura legítima por trás da operação.

Pedido de Pagamentos: Após estabelecer confiança, o golpista solicita transferências financeiras significativas sob pretexto de cobrir custos burocráticos. Uma vez que recebe os pagamentos, desaparece sem deixar rastros.

Consequências Potenciais

Perda Financeira: A vítima pode sofrer perdas financeiras substanciais ao realizar transferências para cobrir os falsos custos burocráticos.

Exploração Emocional: Além das perdas financeiras, a vítima também pode experimentar uma exploração emocional significativa devido à manipulação psicológica envolvida no golpe.

Medidas Preventivas

Verificação Rigorosa: Sempre verificar a autenticidade de ofertas de heranças ou prêmios inesperados antes de tomar qualquer ação.

Desconfiança de Promessas Fáceis: Desconfiar de promessas de ganhos rápidos e benefícios inesperados que exigem pagamento antecipado.

Educação e Conscientização: Informar-se sobre golpes comuns e compartilhar informações com amigos e familiares para ajudar na prevenção.

Conclusão

O golpe do Príncipe da Nigéria continua a ser um perigo significativo devido à sua capacidade de explorar a ganância e a ingenuidade das pessoas. A vigilância contínua, a educação sobre práticas seguras e a desconfiança de ofertas suspeitas são essenciais para proteger-se contra este e outros tipos de fraudes.

Cobrança Falsa de Domínio

Estratégia: Envio de cobrança fictícia de domínio de site

Detalhes: O golpista envia cobranças falsas para proprietários de domínios, na esperança de que alguns paguem sem questionar

Descrição da Ameaça

O golpe de cobrança falsa de domínio visa explorar a falta de conhecimento dos proprietários de sites sobre os detalhes do registro e vencimento de domínios.

Execução do Golpe

Identificação de Vítimas: O golpista pesquisa aleatoriamente domínios registrados e acessa informações públicas no Whois, como nome completo, CPF/CNPJ e data de expiração do domínio.

Envio da Cobrança Falsa: Próximo à data de vencimento do domínio, o golpista envia uma carta de cobrança falsa, simulando ser de um provedor de hospedagem conhecido. A carta inclui um valor para renovação do domínio, muitas vezes inflacionado.

Exploração da Desinformação: Muitos proprietários de sites podem não verificar cuidadosamente os detalhes da cobrança ou o CNPJ associado à empresa cobradora. Isso leva à possibilidade de pagamento para o beneficiário incorreto.

Consequências Potenciais

Perda Financeira: As vítimas podem acabar pagando por um serviço que não precisam, transferindo fundos para contas fraudulentas.

Exposição a Golpes Adicionais: Ao fornecer informações de pagamento, as vítimas podem ficar expostas a futuros golpes financeiros.

Medidas Preventivas

Verificação de Cobranças: Sempre verifique cuidadosamente as cobranças recebidas, comparando-as com registros anteriores e contatando diretamente o provedor de hospedagem se houver dúvidas.

Confirmação de CNPJ: Certifique-se de que o CNPJ da empresa cobradora corresponde ao provedor de serviços esperado.

Conscientização sobre Segurança: Eduque-se sobre práticas seguras de navegação na internet e transações financeiras para evitar ser vítima de golpes.

Conclusão

O golpe de cobrança falsa de domínio aproveita-se da desinformação e da confiança dos proprietários de sites. A vigilância contínua e a verificação cuidadosa de todas as cobranças recebidas são essenciais para evitar cair nesse tipo de fraude e proteger-se contra perdas financeiras desnecessárias.

Cobrança Falsa para Empresas

Estratégia: Envio de cobrança fictícia de taxa para empresas

Detalhes: Golpistas enviam e-mails em massa com cobranças falsas, visando proprietários de pequenas empresas desavisados.

Descrição do Golpe

O golpe de cobrança falsa para empresas segue um padrão semelhante ao golpe de domínio, porém direcionado a pequenos negócios desprotegidos.

Execução do Golpe

Identificação de Vítimas: Usando sites de consulta empresarial como o Econodata, os golpistas obtêm informações como porte da empresa, capital social e contatos. Ferramentas como Lemit e Intouch permitem acessar também o e-mail da empresa.

Envio da Cobrança Falsa: E-mails são enviados em massa para CNPJs de pequenas empresas, alegando a existência de uma taxa em atraso que precisa ser regularizada. Os golpistas frequentemente incluem um boleto anexo ao e-mail, às vezes imitando o modelo do SIMPLES, para facilitar o pagamento.

Aparência de Legitimidade: Os e-mails são bem redigidos, contendo imagens e links que direcionam para sites governamentais reais (como gov.br), aumentando a verossimilhança da cobrança.
Ação após o Pagamento: Se a vítima realiza o pagamento, o golpista lucra. Caso contrário, eles simplesmente partem para a próxima tentativa.

Consequências Potenciais

Prejuízo Financeiro: Empresas desavisadas podem pagar por uma taxa inexistente, transferindo dinheiro para contas fraudulentas.

Exposição a Golpes Futuros: Ao fornecer informações financeiras, as empresas ficam vulneráveis a futuros ataques de fraude.

Medidas Preventivas

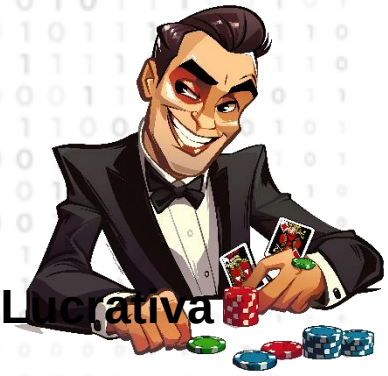
Verificação Detalhada: Sempre verifique cuidadosamente a legitimidade das cobranças recebidas, comparando-as com registros anteriores e consultando diretamente os órgãos responsáveis, se necessário.

Validação do CNPJ: Confirme se o CNPJ do remetente da cobrança corresponde à empresa esperada.

Conscientização da Equipe: Eduque os funcionários sobre práticas seguras de segurança cibernética e financeira, para evitar ser vítima desses golpes.

Conclusão

O golpe de cobrança falsa para empresas explora a falta de conhecimento e a urgência de pequenos negócios. A vigilância constante e a verificação meticulosa de todas as cobranças recebidas são essenciais para evitar ser enganado e proteger-se contra fraudes financeiras significativas.



Cassino Bugado: Uma Armadilha Lucrativa

Estratégia: Aproveitar a frustração de vítimas de golpes anteriores

Detalhes: Direcionado a pessoas que perderam dinheiro em cassinos online e estão em busca de uma oportunidade de vingança contra o sistema.
Com o crescimento exponencial dos cassinos online no Brasil, muitos jogadores enfrentam significativas dificuldades ao tentar retirar seus ganhos. Essa insatisfação gerou uma oportunidade para o surgimento dos "metagolpistas" — indivíduos que se aproveitam das frustrações dos jogadores para aplicar seu próprio golpe elaborado.

Como o Golpe Funciona
Atração Inicial: O golpista se apresenta como alguém que descobriu uma falha no sistema dos cassinos online que pode ser explorada para grandes ganhos. Utilizando redes sociais, websites de apostas e fóruns de discussão, ele exibe uma vida de luxo ostensiva para atrair potenciais vítimas, sem revelar sua verdadeira identidade.

Promessa de Vantagens: Usando uma narrativa convincente, o golpista afirma ter encontrado um "bug" no sistema do cassino que permite aos jogadores obter lucros exorbitantes de maneira consistente. Ele usa exemplos falsos de supostos ganhos para aumentar a credibilidade de sua história e atrair mais vítimas.

Aplicativo Falso: Para executar o golpe, o golpista direciona as vítimas a baixarem um aplicativo de apostas supostamente desenvolvido para explorar essa falha no sistema. O aplicativo é projetado para parecer legítimo e funcional, com interface atraente e promessas de altos retornos sobre o investimento.

Simulação de Ganhos: Algumas versões do golpe podem até mostrar o "bug" funcionando, exibindo saldos fictícios aumentando rapidamente na conta da vítima dentro do aplicativo. No entanto, qualquer dinheiro depositado vai diretamente para o golpista, enquanto o saldo mostrado no aplicativo não pode ser retirado de fato.

Desaparecimento Rápido: Ao contrário de cassinos online legítimos que permitem saques, o golpe é projetado para desaparecer rapidamente após os depósitos serem feitos. Uma vez que as vítimas tentam recuperar seus ganhos, descobrem que o aplicativo foi

desativado ou as contas foram bloqueadas, impossibilitando qualquer tentativa de recuperação do dinheiro perdido.

Reaparecimento e Ciclo de Golpe: Após o golpe ser descoberto, o golpista pode mudar de identidade, criar novos aplicativos ou redes sociais falsas, comprar seguidores e recomeçar o ciclo, visando novas vítimas desavisadas.

Consequências e Medidas Preventivas

Prejuízo Financeiro: As vítimas enfrentam a perda total dos fundos depositados, muitas vezes sem possibilidade de recuperação.

Prevenção: Verifique sempre a reputação de aplicativos e sites de apostas antes de fazer qualquer depósito. Utilize avaliações de usuários confiáveis, pesquise informações sobre a empresa por trás do aplicativo e consulte reguladores de jogos para garantir que estão devidamente licenciados.

Proteja-se Contra Golpes de Cassino

Pesquisa Detalhada: Sempre investigue a reputação do cassino online ou aplicativo de apostas antes de se inscrever ou depositar dinheiro.

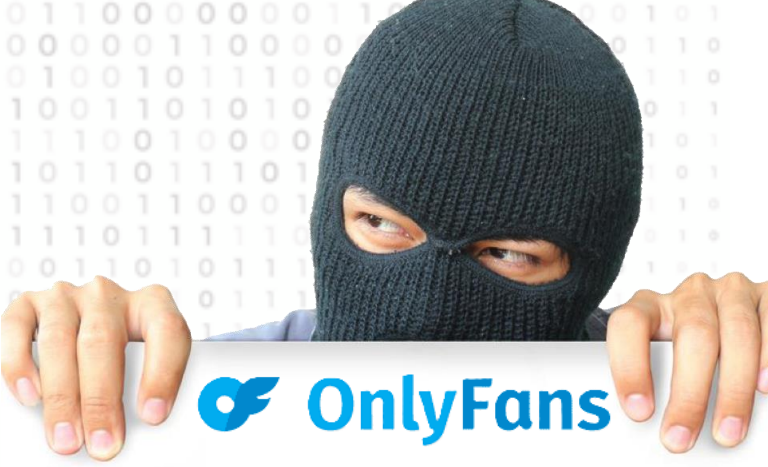
Desconfie de Promessas Exageradas: Fique atento a promessas de lucros fáceis e rápidos, especialmente se exigirem depósitos antecipados.

Verificação de Licenciamento: Certifique-se de que o cassino online possui licenças válidas e regulamentação adequada em jurisdições reconhecidas.

Relate Suspeitas: Se suspeitar de atividades fraudulentas ou encontrar indícios de golpe, denuncie imediatamente às autoridades competentes e às plataformas de reclamação de consumidores.

Conclusão e Alerta

O golpe do cassino bugado explora a esperança e a vulnerabilidade dos jogadores, oferecendo uma falsa promessa de lucros significativos enquanto direciona seu dinheiro para os golpistas. Mantenha-se vigilante e informado para evitar cair em armadilhas online desse tipo. Se você ou alguém que conhece foi vítima de um golpe semelhante, é fundamental reportar o incidente para prevenir que outros caiam na mesma fraude. A educação contínua e a conscientização são suas melhores defesas contra esses esquemas fraudulentos.



Modelo OnlyFans Falsa

Estratégia: Venda de conteúdo adulto fictício

Detalhes: Criação de perfis falsos de modelos usando inteligência artificial e bots para extorquir dinheiro de clientes.

Desde os primórdios da internet, golpistas têm se passado por mulheres atraentes para enganar homens desavisados. Esse tipo de fraude continua a evoluir até os dias de hoje, adaptando-se às novas tecnologias e à crescente aceitação de modelos que vendem conteúdo adulto.

Com o aumento da demanda por conteúdo adulto na internet, o número de perfis femininos atrativos também cresceu, o que normalizou essa prática. Hoje, perfis que antes seriam rapidamente identificados como falsos devido ao apelo excessivo podem agora parecer autênticos, levando as vítimas a acreditar que estão interagindo com mulheres reais que produzem conteúdo adulto.

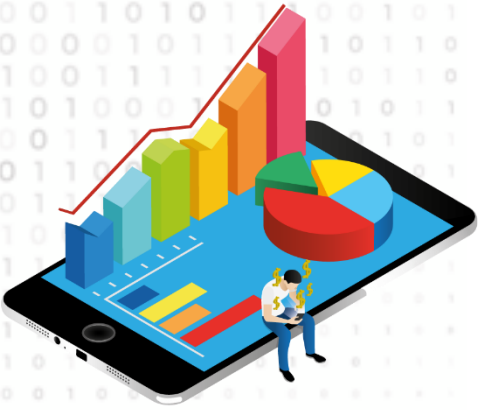
Aproveitando essa lacuna, muitos golpistas criam perfis falsos em redes sociais e plataformas como Onlyfans. Anteriormente, eles copiavam fotos de modelos reais pouco conhecidas ou criavam montagens com imagens de mulheres que não estão envolvidas na indústria adulta. Contudo, essas práticas arriscadas deram lugar a novos métodos.

Atualmente, a maioria dos perfis falsos é gerada usando inteligência artificial avançada, como a Stable Diffusion. Esses golpistas criam imagens fictícias que parecem realistas em diferentes ângulos e iluminações, e até mesmo geram vozes simuladas por IA. Para vídeos, utilizam vídeos deepfake, que são vídeos falsos criados com o rosto da modelo fictícia.

Em vez de usar plataformas como Onlyfans e Privacy, alguns golpistas preferem vender diretamente aos clientes via WhatsApp para evitar taxas. Eles usam bots para continuar a conversa, enviando áudios gravados por IA e conduzindo todo o processo de vendas.

Durante a transação, o golpista fornece seu Pix, geralmente registrado em nome de uma pessoa laranja com nome feminino, que também é o nome usado pela modelo fictícia.

Esse golpe não apenas engana as vítimas financeiramente, mas também viola a privacidade e a confiança pessoal, explorando a vulnerabilidade emocional e sexual de indivíduos. É essencial que os consumidores estejam cientes desses esquemas e tomem medidas para verificar a autenticidade dos perfis e das transações.



Manipulação de Mercado: Estratégias e Impactos

Estratégia: Recomendação de investimentos para influenciar valorizações no mercado

Detalhes: Compra estratégica de ativos, recomendação pública para impulsionar seu valor e posterior venda durante picos de alta.
Em 2021, Elon Musk provocou uma reviravolta no mercado de criptomoedas ao declarar que a Tesla, uma de suas empresas, não mais aceitaria Bitcoin devido ao alto consumo energético associado à mineração. Como resultado, o preço do Bitcoin despencou aproximadamente 30%. Musk então passou a promover o Dogecoin como uma alternativa mais eficiente energeticamente, levando essa moeda a valorizações significativas em poucos dias.

Após uma série de tweets reforçando suas opiniões, Musk eventualmente voltou atrás e anunciou que a Tesla retomaria os pagamentos com Bitcoin. Curiosamente, desde então, ele evitou discutir novamente a eficiência energética das criptomoedas. Essa sequência de eventos levanta suspeitas de manipulação de mercado.

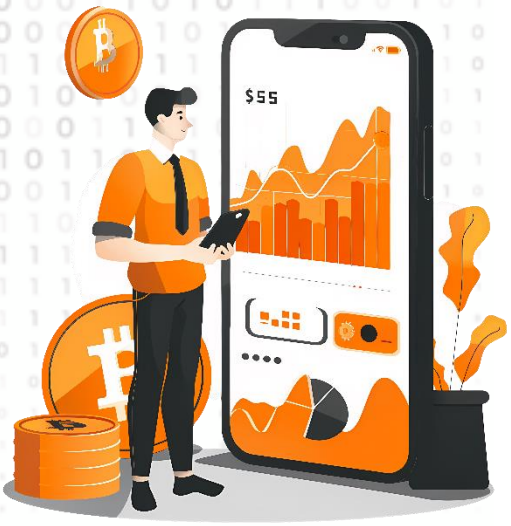
A hipótese é que Musk poderia ter comprado Dogecoins antes de seus tweets, utilizando sua influência para provocar uma valorização expressiva da moeda e, posteriormente, lucrar com a venda antes de abandonar o assunto.

Embora esse exemplo envolva uma figura pública de grande influência como Musk, a manipulação de mercado não é exclusiva de indivíduos famosos. Existem casos de pequenos YouTubers com menos de 20 mil inscritos que conseguem impactar mercados de criptomoedas, recomendando moedas específicas e observando valorizações consideráveis devido à natureza de mercados de nicho.

Além das criptomoedas, a manipulação de mercado também é observada em jogos online, onde criadores de conteúdo influentes em comunidades menores podem direcionar o valor de itens ao recomendar sua compra.

É importante ressaltar que, fora do ambiente regulatório da bolsa de valores, a manipulação de mercado não é estritamente ilegal, mas pode resultar na perda gradual da credibilidade e influência do manipulador conforme as pessoas se tornam mais céticas em relação às suas recomendações.

Manipular mercados é um dos métodos mais lucrativos e controversos de investimento, destacando a necessidade de transparência e vigilância por parte dos investidores para evitar armadilhas financeiras.



Rugpull

Estratégia: Especulação de criptomoedas em que o promotor é o proprietário

Detalhes: Construção de credibilidade como investidor de criptomoedas para recomendar seu próprio projeto scam.

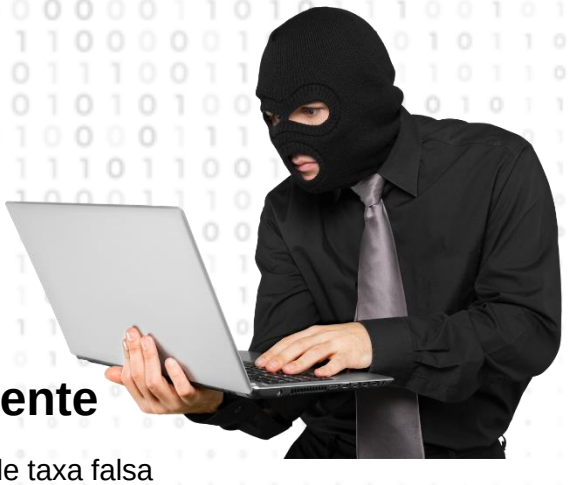
O rugpull se tornou um golpe frequente no mercado de criptomoedas, onde YouTubers e influenciadores começam a promover entusiasticamente uma nova criptomoeda, destacando suas supostas vantagens e inovações. Muitas vezes, esses promotores já ganharam reputação ao promover projetos legítimos anteriormente, o que faz com que o novo projeto pareça confiável e promissor.

Após atrair investidores e impulsionar o preço da criptomoeda através de suas plataformas, o promotor (que secretamente é o proprietário do projeto) desaparece repentinamente, levando consigo todo o dinheiro investido pelos seguidores. Muitos desses golpistas criam canais e constroem suas reputações apenas para executar esses esquemas fraudulentos, ilustrando o quão lucrativo esse tipo de golpe pode ser.

Durante a alta dos NFTs, também houve casos de rugpulls em projetos de jogos, nos quais os desenvolvedores incentivavam os jogadores a investir em moedas específicas do jogo para obterem benefícios dentro da plataforma. No entanto, após alguns meses, a maioria desses jogos desaparecia junto com os investimentos dos jogadores.

Um exemplo notório envolve o influenciador americano Logan Paul, acusado de conduzir um golpe similar. Nesse caso específico, o jogo prometido sequer foi lançado, mas Paul conseguiu captar investimentos antecipados de seus seguidores sem cumprir as promessas feitas.

Em muitos casos de rugpulls, os responsáveis pelos projetos permanecem anônimos, operando através de transações criptografadas que dificultam a identificação e responsabilização. Isso torna praticamente impossível para os investidores recuperarem os fundos perdidos.



Falso Gerente

Estratégia: Oferta de empréstimo com cobrança de taxa falsa

Detalhes: O golpista se apresenta como gerente de um banco e oferece um empréstimo à vítima, exigindo uma taxa de serviço falsa como condição para liberar os fundos.
O golpe envolvendo o falso gerente de banco segue um padrão bem definido: o golpista entra em contato com a vítima, prometendo a obtenção de um empréstimo vantajoso. Para ganhar a confiança da vítima, o golpista solicita informações confidenciais, como comprovantes de identidade, para confirmar sua identidade como representante legítimo do banco.

Após estabelecer essa falsa credibilidade, o golpista envia um link para uma página falsa do banco, onde a vítima é instruída a inserir dados pessoais sensíveis, como número da conta e agência. Quando o dinheiro do empréstimo é realmente depositado na conta da vítima, o golpista exige o pagamento imediato da taxa combinada.

A conta fornecida para o pagamento da taxa é geralmente uma conta laranja, usada para evitar rastreamento e identificação do golpista. A página falsa do banco serve apenas para capturar e validar os dados da vítima, que posteriormente podem ser vendidos ou utilizados em outros golpes.

Se a vítima hesitar em pagar a taxa exigida, o golpista pode recorrer a táticas de chantagem emocional para pressionar o pagamento. No entanto, se a vítima continuar resistindo, o golpista geralmente desiste e parte para tentar aplicar o mesmo golpe em outras pessoas que possuam empréstimos aprovados no mesmo banco.

Esse golpe explora a confiança das vítimas em instituições financeiras e a urgência financeira que muitas vezes acompanha a necessidade de um empréstimo, destacando a importância de verificar sempre a autenticidade das informações e a segurança das transações antes de realizar qualquer pagamento.

Reflexões Finais

No cenário contemporâneo, onde a sofisticação e complexidade dos crimes frequentemente dificultam a identificação dos culpados, a busca por justiça se torna um desafio constante. Quando finalmente os responsáveis são descobertos, a severidade das punições reflete a necessidade de dissuasão e retribuição.

Historicamente, a severidade das penas tem servido como um poderoso instrumento de dissuasão. Desde a Idade Média, punições cruéis e públicas como a crucificação, o enforcamento e a guilhotina eram utilizados não apenas para punir, mas também para enviar uma mensagem clara aos potenciais infratores sobre o custo de desafiar a ordem estabelecida.

Embora vivamos em um mundo muito diferente, os ecos dessa abordagem punitiva ainda podem ser observados em nossos sistemas legais. A exposição pública dos crimes e a severidade das sentenças visam, em parte, alertar a sociedade sobre as consequências de violar a lei.

Curiosamente, os crimes contra o patrimônio, muitas vezes vistos como menos graves que os crimes violentos, são aqueles que mais frequentemente resultam em identificação e punição dos culpados. Isso se deve, em grande medida, à eficácia dos órgãos estatais dedicados à proteção econômica e financeira, como a Polícia Federal e a Receita Federal. Equipados com tecnologia avançada e acesso a vastos bancos de dados, esses órgãos são capazes de rastrear e identificar os responsáveis com notável precisão.

É interessante notar que a eficiência desses órgãos em proteger os interesses do Estado também contribui significativamente para a manutenção da justiça. No entanto, a verdadeira segurança patrimonial começa com a vigilância individual. Utilizar o conhecimento disponível para proteger a si mesmo e a seus bens é essencial em um mundo onde a prevenção é muitas vezes a melhor forma de proteção.

Em suma, a busca por justiça em um mundo complexo requer tanto a atuação eficaz das autoridades quanto a conscientização e precaução individual. Manter-se informado e vigilante é fundamental para garantir a segurança própria.

AVISO

A Polícia Federal agora oferece o Comunica PF, um canal online dedicado à comunicação de crimes que são de sua competência investigativa. Este serviço visa facilitar o processo de denúncia, garantindo maior agilidade e eficiência na apuração de crimes.

COMUNICA PF: Comunicação de Crimes

Entre as categorias de crimes que podem ser reportados estão:

- Invasão e/ou Interrupção de Serviço de Rede de Computadores
- Fraudes Bancárias Eletrônicas
- Abuso Sexual Infantojuvenil

"O Comunica PF é um canal que permite a comunicação online de crimes de atribuição investigativa da Polícia Federal, conforme estabelecido pelo § 1º do art. 144 e art. 109 da Constituição Federal, na Lei 10.446/2022 e de acordo com o § 3º do art. 5º do Código de Processo Penal (CPP).

É importante destacar que grande parte das comunicações de crimes recebidas não são de atribuição da Polícia Federal. Portanto, antes de enviar a comunicação, o interessado deve verificar se o fato narrado está entre as atribuições criminais da Polícia Federal, conforme os dispositivos legais abaixo. Caso não esteja, a comunicação de crime deverá ser feita na Delegacia de Polícia Civil mais próxima do local onde os fatos ocorreram."

Para utilizar o Comunica PF, siga os passos abaixo:

- Acesse o portal oficial da Polícia Federal.
- Navegue até a seção do Comunica PF.
- Selecione a categoria do crime a ser comunicado.
- Preencha o formulário com todas as informações necessárias, incluindo detalhes do crime, envolvidos e evidências disponíveis.
- Envie o formulário e aguarde o recebimento de um protocolo de atendimento.

O serviço é seguro e confidencial, garantindo que as informações fornecidas sejam utilizadas exclusivamente para fins investigativos. O Comunica PF reforça o compromisso da Polícia Federal em combater crimes de alta complexidade e proteger a sociedade brasileira.