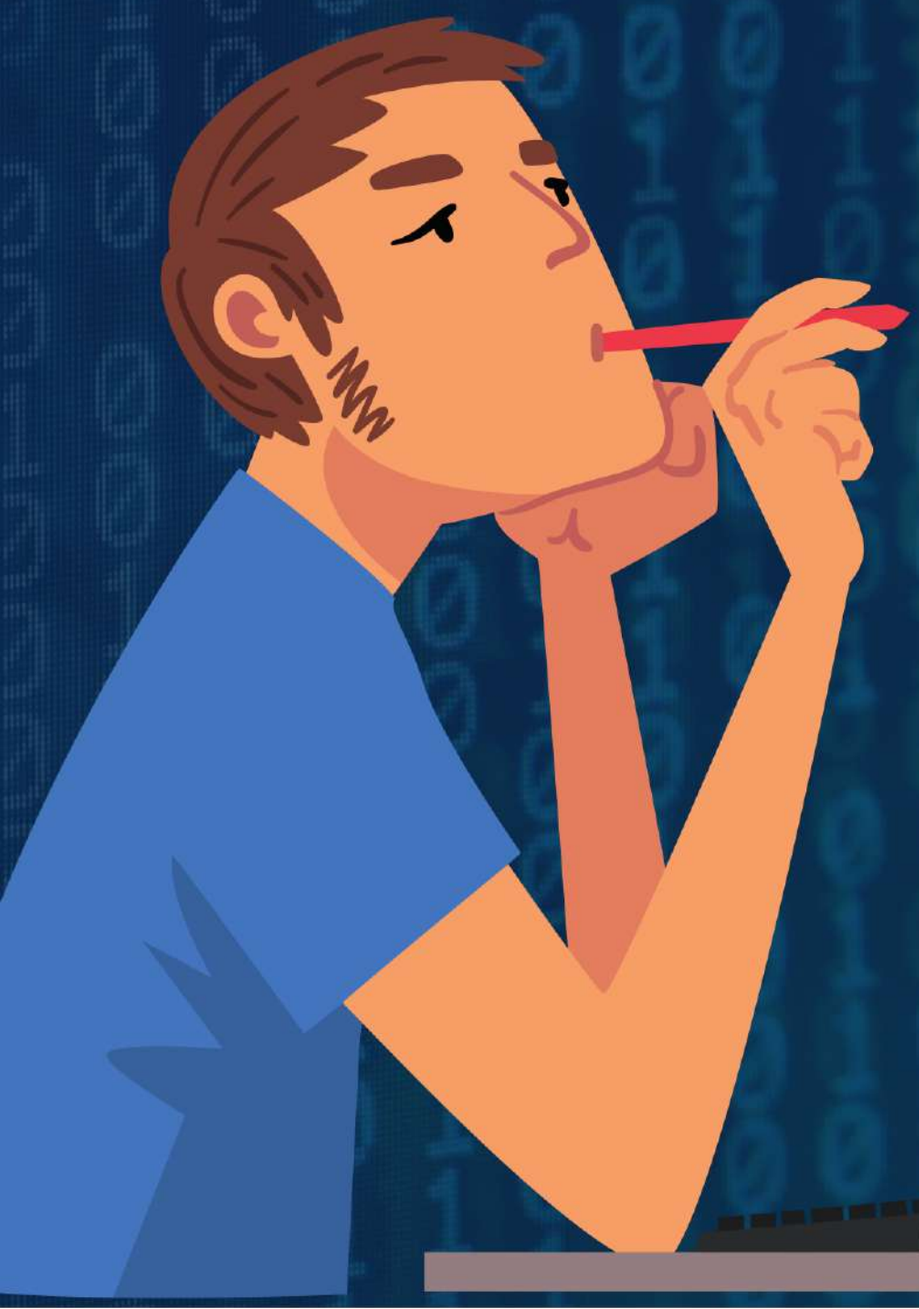
Alesandro Gonçalves Barreto
Natália Siqueira da Silva

Prefácio Ricardo Magno Teixeira Fonseca
Apresentação Laerte Peotta de Melo

É BOM DEMAIS PARA SER VERDADE?

NÃO CAIA NESSA!

- 50 TIPOS DE GOLPES
- PROTEÇÃO
- RECUPERAÇÃO DE CONTAS



São Paulo
2022

Apoio:

OBSERVATÓRIO DOS CRIMES CIBERNÉTICOS

Alesandro Gonçalves Barreto
Natália Siqueira da Silva

Prefácio Ricardo Magno Teixeira Fonseca
Apresentação Laerte Peotta de Melo

É BOM DEMAIS PARA SER VERDADE?

NÃO CAIA NESSA!

Apoio:

OBSERVATÓRIO DOS CRIMES CIBERNÉTICOS

Agradecimento

Obrigado, meu Deus, por todas as conquistas.
À minha esposa Vanubia e filhas Karolinne e Camila pelo amor e compreensão.
Ao meus pais Francisco e Graça (In Memoriam).
Meus agradecimentos aos amigos Mardem (PC-PI) e João Leonardo PC-AL), mortos em decorrência da covid 19.
Não posso deixar de mencionar o time CIBERLAB (Quesia, Nycole, Jorge, Buery, Claudia, Ivan Castillo, Leandro e Saskia). Vocês são espetaculares.
Gratulações especiais ao Ricardo Magno (PC-DF), Natalia Siqueira e Paulo Zanatta (PC-SP), Venceslau Felipe e Marcos Lacerda (PC-PI) e delegadas Sabrina Lelis (PC-GO)e Ana Cristina (PC-AM).
Por fim, gostaria de regraciar todos aqueles que direta ou indireta contribuem para meu crescimento pessoal e profissional.

Alesandro Barreto

Agradeço a Deus, a Ele toda Glória.
Ao meu pai Helicio, meus irmãos e Lucas por todo amor e apoio em cada nova ideia.
Especial agradecimento aos meus amigos mais próximos que sempre me incentivam e caminham ao meu lado.
Aos colegas de trabalho da PC-SP, principalmente aos companheiros de Paraguaçu Paulista.
Deixo aqui resgitrado um agradecimento às delegadas da PC- SP, Marisa Izabel Tardin e Raquel Santos de Oliveira por incentivar o desenvolvimento deste trabalho.
Ao delegado Alesandro Barreto pela oportunidade de aprender e trabalhar juntos.
Por fim, agradeço a todas as pessoas que de alguma forma me ajudam e incentivam nos projetos pessoais e profissionais, muito obrigada.

Natália Siqueira

Prefácio

É BOM DEMAIS PRA SER VERDADE? O título da presente obra resume o quão bem-vinda é esta iniciativa dos autores Alesandro Gonçalves Barreto e Natália Siqueira da Silva, policiais de carreira, conscientes dos desafios enfrentados pelos seus pares. Talvez o que se apresenta mais difícil a estes profissionais nos tempos atuais, é a compreensão acerca da dinâmica do crime na Era da Informação.

Neste admirável mundo novo, da Internet das Coisas e da Internet de Tudo, onde as tecnologias comunicacionais transformam cada vez mais relações humanas e negociais, ferramentas saem das estantes, mesas e gavetas, virtualizando-se em formato de aplicações alocadas na memória de um portável smartphone.

É verdade, a frase "o mundo na palma da sua mão", deixou de ser mera citação poética. Agenda, localizador geográfico e relógio, por exemplo, são alguns artefatos de grande importância para qualquer usuário, pois registram e orientam sua existência nas perspectivas tempo e espaço. Um aparelho celular é o companheiro indispensável para garantia desses dados. Há tempos que este deixou de ser apenas um telefone, mesmo nas versões mais simples vendidas.

Em outro plano, a vida social e financeira de uma pessoa também sofre disrupção, quando passa a ser insumo dos algoritmos das Redes Sociais e Mobile Bankings. Resumindo-se esses serviços a um único display, impera a sensação de extrema facilidade, pela acessibilidade, a qualquer momento, desses instrumentos de movimentação. Pagar e publicar nunca foram ações tão simples de realizar.

Nos últimos anos, marcados pelas limitações impostas pelos governos dos países, em razão da pandemia da COVID-19, o uso dos aplicativos de mensageria e redes sociais se ampliou exponencialmente. Em um contexto de povos isolados por necessidade sanitária, os encontros pessoais e profissionais se deram por plataformas, assim como a contratação de serviços e compras, por aplicações.

A multiplicidade de ferramentas digitais surgidas ultimamente revela um horizonte transformador, mas ao mesmo tempo, tão dinâmico quanto desconhecido. É impossível se conhecer o grau de segurança desses softwares, no tocante ao que é coletado e compartilhado, em termos de dados pessoais. Ademais, grande parte dessa segurança é atribuída ao próprio usuário, que mais preocupado com o próprio uso, se desguarda, e acaba criando seus problemas nesta seara.

Consequentemente, são assustadores os percentuais de crescimento dos chamados "golpes", contra cidadãos brasileiros de todas as unidades da Federação, resultando em prejuízos bilionários ao país.

Prefácio

Neste sentido, compreender os riscos e minimizar os ataques no ambiente dessas aplicações também são objetivos desta obra. Todavia, direcionar a força policial para a orientação do cidadão e realização dos procedimentos aplicáveis nos casos de crimes daí decorrentes, apresentam-se como primordial.

Os autores foram muito felizes em priorizar a "descomplicação", desmistificando a complexidade dos processos tecnológicos, por meio da utilização de metodologias ativas na exposição do conteúdo trazido nas páginas seguintes. Fazendo-se valer, desse modo, a expressão do pensador político e filósofo Confúcio (552 e 479 a.C.): "uma imagem vale mais que mil palavras".

Ao leitor, foi dada a imensa oportunidade de compreender, a partir do uso de recursos visuais toda a dinâmica empregada por criminosos, na realização das fraudes eletrônicas, as quais acontecem em grande parte nos aplicativos móveis, com destaque àqueles mais comuns em tempos de pandemia. Destarte, a apresentação ilustrada do "passo a passo" procedimental dentro dos diferentes cenários, indubitavelmente, contribuirá para uma atuação mais eficiente diante dessas situações, tratando-se se das melhores práticas a serem aplicadas.

Certamente, um elogiável trabalho e de grande relevância social, o qual também recomendo como referencial aos cursos de formação policial e pesquisa bibliográfica. Como profissional atuante na área, o assumo como um manual para o meu dia a dia. É ver e aprender!

Ricardo Magno Teixeira Fonseca

Policial Civil do Distrito Federal
Mestre em Segurança da Informação e Continuidade de Negócios
Especialista em Cibercrime e Cibersegurança

Apresentação

São muitas as inovações que surgiram nos últimos anos: bancos, contatos, imagens, pesquisas, um mundo de possibilidades, tudo na palma de sua mão, em qualquer lugar que estiver. Contudo, existem também riscos, riscos estes que podem ser diminuídos tomando alguns cuidados. Assim como no mundo físico você olha antes de atravessar a rua, no mundo virtual você deve estar atento, pois os criminosos estão rondando e você não quer ser a próxima vítima.

Bom demais para ser verdade? Mostrar 50 tipos de golpes pode parecer pouco, pois os criminosos diariamente criam novas formas e maneiras de enganar outras pessoas. Neste sentido, esta obra tem como objetivo apresentar, de forma clara e direta, os golpes mais utilizados atualmente. Longe de ser pretenciosa a ponto de englobar tudo que acontece, mas bem próxima do que realmente importa, orientar o leitor dos principais tipos de golpes e, ainda, trazer o que fazer para se proteger e quais ações tomar em caso de ser vítima.

Tenho certeza de que depois de entender os golpes irá se surpreender, até duvidar de como alguém cai em um golpe, mas não se iluda quanto ao poder da engenharia social, o estelionatário explora fatores humanos: medo, curiosidade e ganância. Controle esses sentimentos em tudo que recebe digitalmente, exerça sempre o questionamento do que chega pela internet, até mesmo de pessoas que você conhece. Os criminosos roubam a identidade de pessoas e usam para explorar o seu círculo de amizades e, assim, ganhar sua confiança. A dica é: desconfie sempre!

Não fique aí, começe agora a ler esta obra e nunca mais será o mesmo.

Laerte Peotta de Melo

Mestre e Doutor em Engenharia Elétrica pela Universidade de Brasília
Gerente de soluções de Cyber Segurança do Banco do Brasil

Sobre os autores

Alesandro Gonçalves Barreto é Delegado de Polícia Civil do Estado do Piauí. Mestrado em Seguridad de la Información y Continuidad de Negocio - UCAM/ESPANHA. É graduado pela Universidade Regional do Cariri (1998) e pós-graduado em Direito pela Universidade Federal do Piauí.

Coautor dos livros: "Inteligência e Investigação Criminal em Fontes Abertas", "Manual de Investigação Cibernética", "Deep Web" e Cyberdicas Eleições 2020: atribuição de autoria, preservação e remoção de conteúdo no ambiente cibernético (Brasport), "Vingança Digital" (Mallet), "Cibercrimes e os reflexos no direito brasileiro" (Juspodivm) e OPERAÇÃO LUZ NA INFÂNCIA - Protegendo Crianças e Adolescentes na Internet (Editora do Autor).

Foi Diretor da Unidade do Subsistema de Inteligência da Secretaria de Segurança Pública do Estado do Piauí de 2005 a 2016. Integrou o Grupo de Trabalho revisor da Doutrina Nacional de Inteligência de Segurança Pública. Professor de Cursos de Inteligência Cibernética pela SENASP (Secretaria Nacional de Segurança Pública) e SEOPI (Secretaria de Operações Integradas). Gestor do NUFA (Núcleo de Fontes Abertas) na Secretaria Extraordinária para Segurança de Grandes Eventos do Ministério da Justiça (SESGE-MJ) durante os Jogos Olímpicos e Paralímpicos Rio 2016. Entre os anos de 2017/18, foi Coordenador Geral de Contrainteligência da Diretoria de Inteligência e Coordenador-Geral Substituto da Polícia Judiciária e Perícia da Diretoria da Força Nacional de Segurança Pública da Secretaria Nacional de Segurança Pública.

Atualmente encontra-se mobilizado na Secretaria de Operações Integradas do Ministério da Justiça e Segurança Pública exercendo suas atividades no Laboratório de Operações Cibernéticas.

@delbarreto19

Sobre os autores

Agente na Polícia Civil do Estado de São Paulo. Graduada em Administração de Empresas pela UNIESP (2014), e Direito pela Faculdade TOLEDO de Presidente Prudente (2018) . Pós-graduada em Direito Penal pela Damásio (2021).

Atualmente lotada na Delegacia de Defesa da Mulher de Paraguaçu Paulista-SP.

@natisiqueira

Sumário

Sumário

Introdução

As fraudes são praticadas desde a antiguidade, sempre com objetivo de tirar proveito dos desatentos ou daqueles que se acham "mais espertos".

Outrora, ouvíamos falar do conto do vigário, cartas nigerianas, bilhete premiado, falso funcionário, empréstimo fraudulento e o conto da recompensa. Hoje, eles ainda persistem e algumas práticas foram aperfeiçoadas, saindo das esquinas rumo ao novo mundo interconectado. Ferramentas criadas e disponibilizadas com finalidade lícita são empregadas por estelionatários para dar vida a personagens e credibilidade às suas estórias.

Em Portugal, mais precisamente no século XIX, fraudadores apresentavam-se em cidades distantes como emissários do vigário. Diziam carregar valores expressivos nas malas que carregavam, todavia, fariam pequenas viagens e teriam que deixar as malas guardadas em local seguro e, para tanto, necessitavam de uma garantia.

Com a internet, as técnicas de engenharia social ficaram mais fáceis de obter vantagem indevida, sobretudo em tempos de pandemia. As regras de distanciamento social obrigaram-nos a migrar rapidamente para o ciberespaço, desde o trabalho remoto até consultas à distância. Entramos em quarentena, o criminoso não.

Aproveitando-se dessa interconectividade, organizações criminosas e infratores desfrutaram da pandemia do oportunismo para auferir mais lucro sem ao menos serem especialistas em tecnologia da informação para fazê-lo: o crime como serviço já fornece os recursos necessários.

As ocorrências de crimes de internet dispararam. Além daquelas comumente, verificamos novas modalidades de ataques. Baseados na confiança cega do dispositivo dos usuários, os criminosos "sequestram", agora, perfis do WhastApp e Instagram, obtendo de maneira fácil vultosas quantias:

- **Ei mãe, troquei meu número. Anota aí. Estou precisando de um favor teu. Deposita R$ 3.000,00. Devolvo até amanhã, mas faz o seguinte, transfere por este pix que minha conta está com problema;**
- **Vendo Iphone 13, urgente por 1.800,00 no meu stories. Se quiser garantir o seu faz uma transferência para esta chave pix ou venderei para outra pessoa;**
- **Parabéns, você ganhou um final de semana no nosso resort. Para cadastrar, preciso do teu nome completo, email, telefone e que você me manda de volta um link de cadastro que recebeu por SMS.**

Introdução

Dito isto, procuraremos trazer para vocês, de maneira didática e com técnicas de visual law, as principais fraudes praticadas em tempos de pandemia. Impossível esgotar o assunto, eis que, a cada dia, novas variações ou outros golpes irrompem.

Tratamos, ainda, das melhores práticas de recuperação de contas, além de procedimentos pelas vítimas de golpes. Por fim, destacamos as principais medidas de mitigação implementadas pelos usuários, sobretudo, desconfiar sempre. A oferta é tentadora? Caia fora, é fraude.


PRINCIPAIS GOLPES
E
OUTROS DELITOS

WHATSAPP

SEQUESTRO DO WHATSAPP SIMSWAP

Objetivo:

Invasão da conta da vítima e envio de mensagens para os contatos e solicitação de pix.

MODUS OPERANDI

Criminoso faz o simswap do número da vítima e solicita a portabilidade ou o downgrade do plano com o fornecimento de dados ou, ainda, a participação de funcionários das empresas de telefonia;

Se o usuário não possuir a verificação em duas etapas, o infrator assume sua identidade e, alegando emergências, pede depósitos pix;

Durante a invasão, ele assume a identidade da vítima para convencer seus contatos;

As contas transferidas são de "laranjas" e o dinheiro é rapidamente sacado ou transferido;

Particularidade:
a vítima perde acesso ao telefone e WhatsApp.

SEQUESTRO DO WHATSAPP ENGENHARIA SOCIAL

Objetivo:

Invasão da conta do WhatsApp e solicitação de pix para terceiros.

MODUS OPERANDI

Criminoso utiliza técnicas de engenharia social para convencer o usuário a passar os códigos SMS sob o pretexto de receber alguma oferta ou bonificação;

Na verdade, o criminoso pede para instalar o WhatsApp noutro smartphone. Quando a vítima repassa o código, ele entra no WhatsApp dela e solicita valores na conta de terceiros;

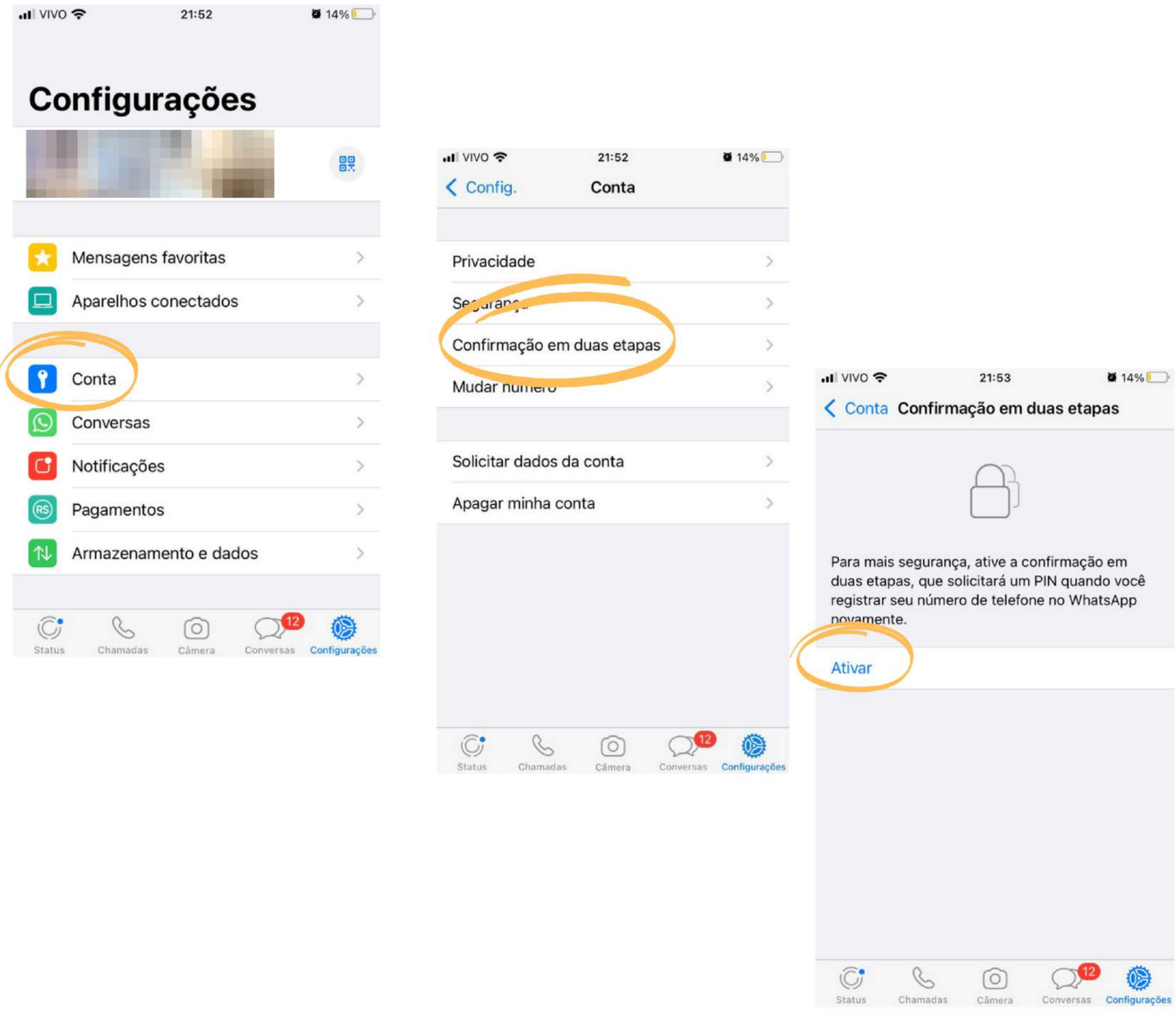
Particularidade:
a vítima perde acesso apenas ao WhatsApp.
O telefone continua funcionando normalmente.

Engenharia Social

- **Hospedagens gratuitas;**
- **Festa vip;**
- **Auxílio emergencial;**
- **Atualização cadastral em plataformas de comércio eletrônico (OLX, Mercado Livre);**
- **Sites de venda de imóveis;**
- **Descontos em supermercados e restaurantes;**
- **SMS por engano e solicitação de envio para terceiro.**

PROTEÇÃO
SEQUESTRO DO WHATSAPP POR SIMSWAP OU ENGENHARIA SOCIAL.

Habilite a verificação em duas etapas no aplicativo.
Acesse: configurações> conta> e confirmação em duas etapas;



Foi atacado, avise imediatamente seus familiares e contatos;

Nunca deposite dinheiro quando solicitado por mensagens. Procure fazer a verificação do pedido por um meio alternativo;

RECUPERAÇÃO DE CONTA
SEQUESTRO DO WHATSAPP POR SIMSWAP

Envie um Email para: support@whatsapp.com

Coloque no assunto:

URGENTE - WHATSAPP CLONADO: Por favor, desativem minha conta.

Utilize esse modelo:

URGENTE - WHATSAPP CLONADO: "Por favor, desative minha conta".

support@whatsapp.com

URGENTE - WHATSAPP CLONADO: "Por favor, desative minha conta".

WhtasApp Clonado: +55_____

Prezado(a)

Meu nome é _____; Na data de hoje meu número do WhatsApp foi clonado.

Gostaria que a conta fosse desativada e o link de recuperação fosse enviado novamente para meu número vinculado.

Cidade-UF e data.

Agradecido

FOI VÍTIMA DESTE GOLPE?
VEJA O QUE FAZER

Registre boletim de ocorrência e informe:

- **Dia e hora que ocorreu o fato com a descrição do problema;**
- **Modus operandi;**
- **Período no qual ficou sem acesso ao telefone e aplicativo;**
- **Email e telefone utilizado pelo infrator e vítima;**
- **Contas bancárias ou chaves pix para transferência;**
- **Identificação das vítimas e valores depositados.**

Ação Judicial contra a Operadora de Telefonia por falha na prestação do serviço no caso de SIMSWAP - Art. 14 do CDC.

Informe à instituição financeira que a conta do infrator é utilizada para prática de fraudes:

- **Fundamentação Legal- Lei Complementar 105/2001, art. 1º, § 3º,inc. IV;**
- **Envie cópia do boletim de ocorrência.**

PERFIL FAKE

Objetivo:

Criação de perfil fake a fim de solicitar depósitos pix para familiares e contatos próximos do usuário.

MODUS OPERANDI

Criminoso acessa bancos de dados ilegais de consumidores e obtém informações do usuário, familiares e contatos;

Procura por imagens do usuário em redes sociais, mecanismos de busca ou no WhatsApp quando não há configuração de privacidade;

Cria uma conta no WhatsApp com um número de telefone diferente da vítima e passa a mandar mensagens para os contatos mais próximos;

Alega emergência e diz que sua conta bancária está com problemas para justificar a transferência para terceiros;

Os valores são sacados ou transferidos logo em seguida;

Particularidade:

O WhatsApp e telefone da vítima continuam funcionando normalmente.

PROTEÇÃO
PERFIL FAKE WHATSAPP

Avise aos parentes (especialmente os idosos) e amigos para nunca depositarem dinheiro quando solicitado por mensagem;

Advirta para desconfiarem sempre sobre mensagens com mudanças de telefone;

Configure sua privacidade no WhatsApp para que apenas seus contatos tenham acesso à sua foto de perfil, visto por último e adicionar a grupos;

Nunca deposite dinheiro quando solicitado por mensagem;

DESATIVAÇÃO DA CONTA PERFIL FAKE DO WHATSAPP

Envie um Email para: support@whatsapp.com

Coloque no assunto:

URGENTE - PERFIL FAKE: Por favor, desativem a conta +55 (DDD) + número de telefone que está se passando por você.

Utilize esse modelo:

Perfil Fake - URGENTE - Desative a Conta (+55 + DDD+ numer...

support@whatsapp.com

Perfil Fake - URGENTE - Desative a Conta (+55 + DDD+ numero de telefone)

Prezado(a);

O número +55__(numero de telefone) criou uma conta e está utilizando minha imagem no perfil para solicitar valores para meus contatos.
Por favor desative essa conta em razão da utilização para prática de crimes previstos na legislação brasileira, bem como ferir os termos do serviço.
Quaisquer dúvidas estarei à disposição para esclarecimento através do meu WhatsApp nº +55__(número de telefone).

Agradeço sua atenção.

_____
Nome e telefone

Sans Serif

FOI VÍTIMA DESTE GOLPE? VEJA O QUE FAZER

Registre boletim de ocorrência e informe:

- **Dia e hora que ocorreu o fato com a descrição do problema;**
- **Modus operandi;**
- **Período no qual ficou sem acesso ao telefone e aplicativo, com a individualização do perfil;**
- **Email e telefone utilizado pelo infrator;**
- **Contas bancárias ou chaves pix para transferência;**

Identificação das vítimas e valores depositados.

Eventual demora na desativação da conta pode gerar o dever de indenizar por prejuízos causados a terceiros - art. 14 do CDC;

Informe à instituição financeira que a conta do infrator é utilizada para prática de fraudes:

- **Fundamentação Legal- Lei Complementar 105/2001, art. 1º, § 3º,inc. IV;**
- **Envie cópia do boletim de ocorrência.**

INSTAGRAM

SIMSWAP E SEQUESTRO DE PERFIL

Objetivo:

Invadir o Instagram, assumir a identidade da vítima e oferecer produtos ou serviços com pagamento por pix.

MODUS OPERANDI

O infrator faz um ataque simswap contra a vítima. Utilizando técnicas de engenharia social ou com apoio de funcionários das empresas de telefonia, solicita o downgrade ou portabilidade do chip, coloca noutro telefone e reseta a senha do Instagram, WhatsApp e email vinculado;

De posse do perfil, modifica email e senha e coloca o aplicativo autenticador para dificultar a recuperação da conta;

Assume a identidade do perfil, faz algumas postagens para dar maior credibilidade e oferta produtos e serviços com descontos imperdíveis;

O usuário, acreditando falar com o proprietário, transfere valores por pix;

A vítima não consegue recuperar a conta de imediato e alguns seguidores são lesados;

Em alguns casos, os criminosos utilizam os dados das vítimas para abrir contas em bancos digitais.

ENGENHARIA SOCIAL E SEQUESTRO DE PERFIL 1

Objetivo:

Invadir a conta do Instagram para vendê-la em fóruns da internet ou extorquir para pagamento em criptoativos.

MODUS OPERANDI

Inicia com envio de mensagens pelo direct;

- **Recebimento de selo azul;**
- **Violação da política de direitos autorais;**
- **Uso indevido de imagens do perfil por terceiros.**

Ao clicar no link, o usuário é direcionado para uma página falsa e termina por fornecer suas credenciais de acesso;

Por padrão, a primeira senha colocada pelo usuário será sempre rejeitada, obrigando-o a repeti-la;

Preenchido os dados, o invasor altera o email, telefone e idioma do perfil para turco;

Por fim, exigem valores em criptoativos para devolução ou a conta é vendida em fóruns da internet.

ENGENHARIA SOCIAL E SEQUESTRO DE PERFIL 2

Objetivo:

O criminoso invade o Instagram, assume a identidade da vítima e oferece produtos ou serviços com descontos incríveis para receber transferências pix.

MODUS OPERANDI

O infrator aborda a vítima pelo direct do Instagram e avisa que ela foi contemplada com um prêmio ou desconto;

Solicita nome completo, email e número de telefone para envio de link para cadastro;

Requer o envio do link para ele sob o pretexto de cadastro;

Após isso, a vítima perde o acesso à conta;

O criminoso mandou, na realidade, o link de reset da senha do perfil da vítima;

A partir daí, assume a identidade da vítima e oferta produtos e serviços com super descontos;

O processo de recuperação da conta invadida é lento, ocasionando prejuízos a terceiros

PERFIL FAKE E SEQUESTRO DO WHATSAPP

Objetivo:

Invadir o WhatsApp, assumir o perfil da vítima e solicitar transferências pix.

MODUS OPERANDI

O invasor cria um perfil falso (hotelaria, supermercados, lojas, restaurantes) e utiliza as postagens deles para dar maior credibilidade;

Após o usuário fazer um comentário no perfil verdadeiro, ocorre o envio de mensagem da conta fake via direct com ofertas ou descontos;

Para cadastro, é solicitado o nome completo, email e telefone de contato;

Em seguida, ele instala o WhatsApp da vítima em outro smartphone e solicita o SMS sob o pretexto de cadastro na promoção;

Após o fornecimento do código, a vítima perde acesso ao WhatsApp;

O criminoso assume a identidade dela e solicita transferências pix.

PERFIL FAKE E RESERVA EM ESTABELECIMENTO DE HOTELARIA

Objetivo:

Obter vantagem ilícita através de depósitos de falsas reservas em resorts, hotéis e pousadas.

MODUS OPERANDI

Criação de perfis fakes de estabelecimentos de hotelaria;

Com pouco engajamento, estes perfis utilizam as fotos de hotéis e resorts conhecidos no intuito de enganar o usuário;

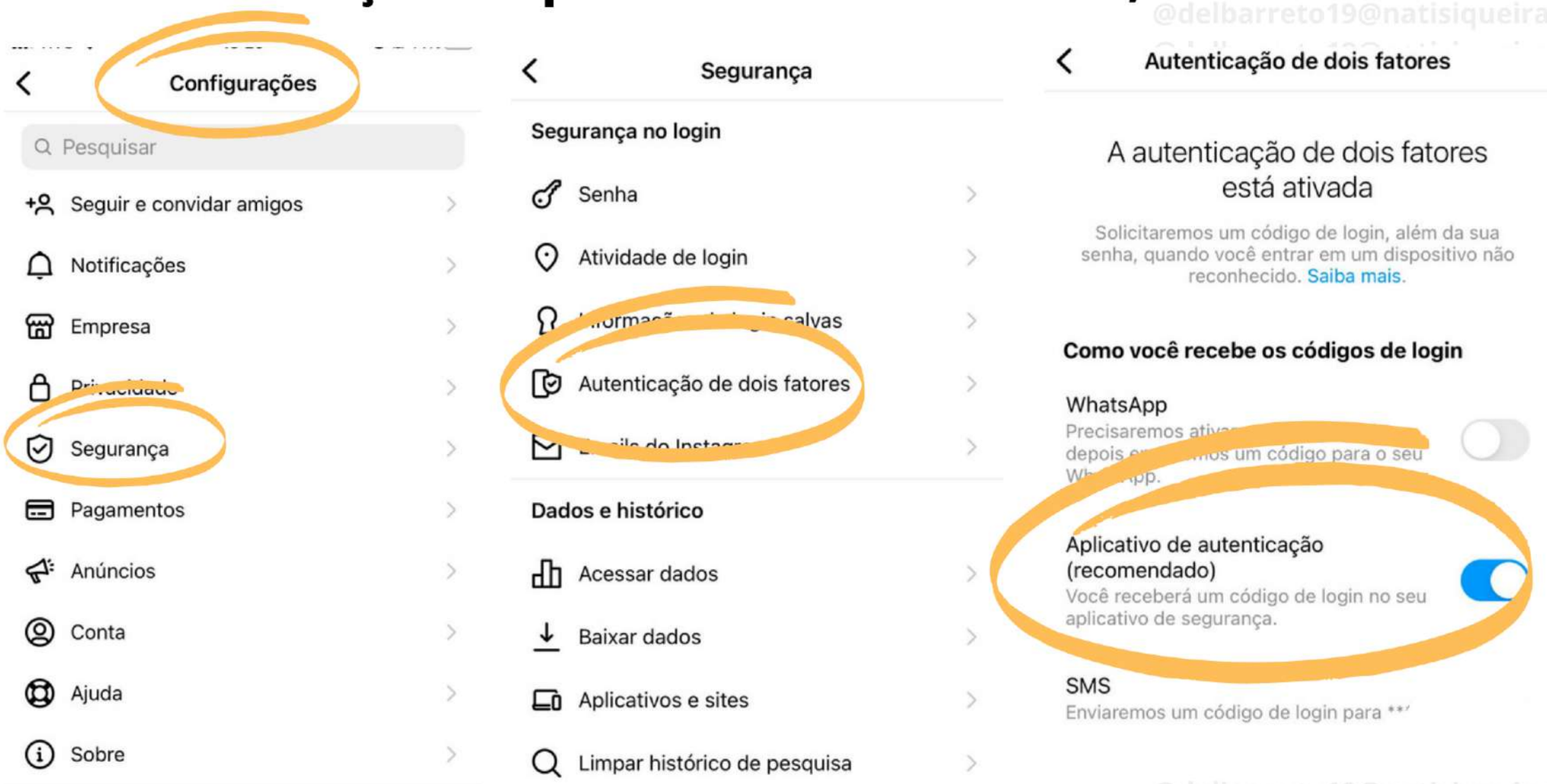
Há o contato via WhatsApp e o pedido de dados para realizar a reserva;

Por fim, o criminoso alega problemas na conta da empresa e pede para o depósito ser realizado para terceiros;

Muitas vezes, a vítima só descobre o golpe quando chega no hotel.

PROTEÇÃO INSTAGRAM

Habilite a verificação em duas etapas no aplicativo e no email vinculado. A ativação por SMS ou WhatsApp não irá garantir segurança. Recomendamos apenas a utilização de aplicativos autenticadores;



No aplicativo acesse Configurações - Conta - Informações Pessoais e deixe vinculado apenas o email para evitar ataques simswap;

Se possuir telefone na BIO, ele não deve ter vínculo com a conta. Dê preferência a números voip;

O Instagram não manda mensagens via direct. Toda e qualquer comunicação será realizada apenas por email do app;

Você não ganhou fim de semana em hotel, desconto em restaurante ou iphone com preços muito baixos. Recebeu uma oferta tentadora, ignore;

Desconfie de mensagens de selo azul ou violação da política de direitos autorais e possua senha fortes e únicas para o aplicativo.

RECUPERAÇÃO DE CONTA INSTAGRAM INVADIDO

- **Suporte do Instagram;**
- **Notificação Extrajudicial para o Facebook;**
- **Email para security@mail.instagram.com;**
- **Ordem judicial;**
- **Página de suporte do Facebook Business.**

RECUPERAÇÃO DE CONTA SUPORTE DO INSTAGRAM IPHONE

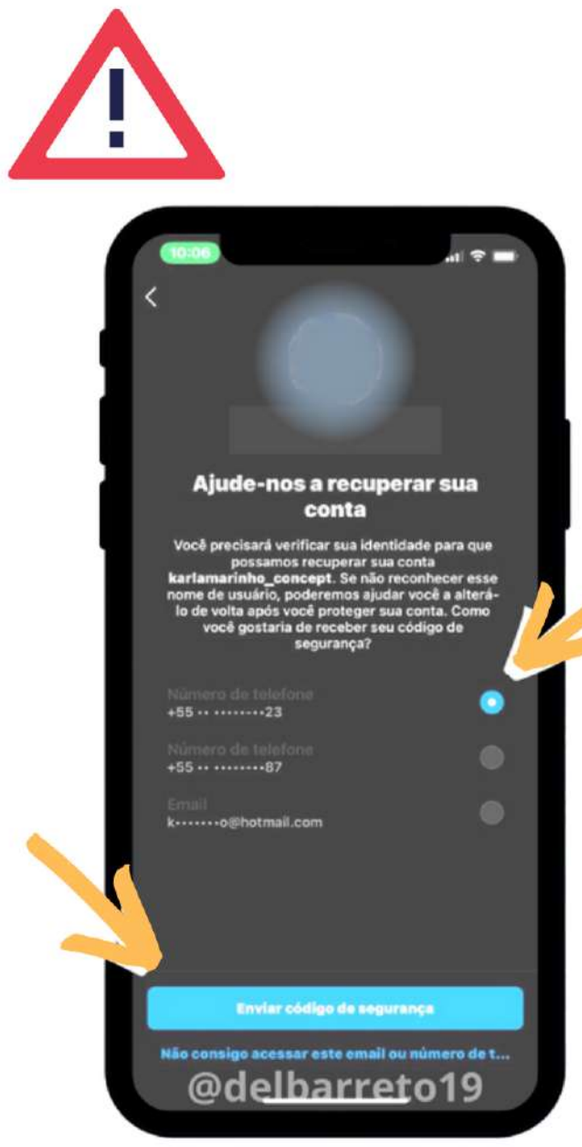
1- Crie uma nova conta de Email;

2- Saia de todas as contas que estiver logado;

3- Acesse o aplicativo Instagram;

4- Coloque o nome de usuário da conta invadida e clique em: Esqueceu a senha

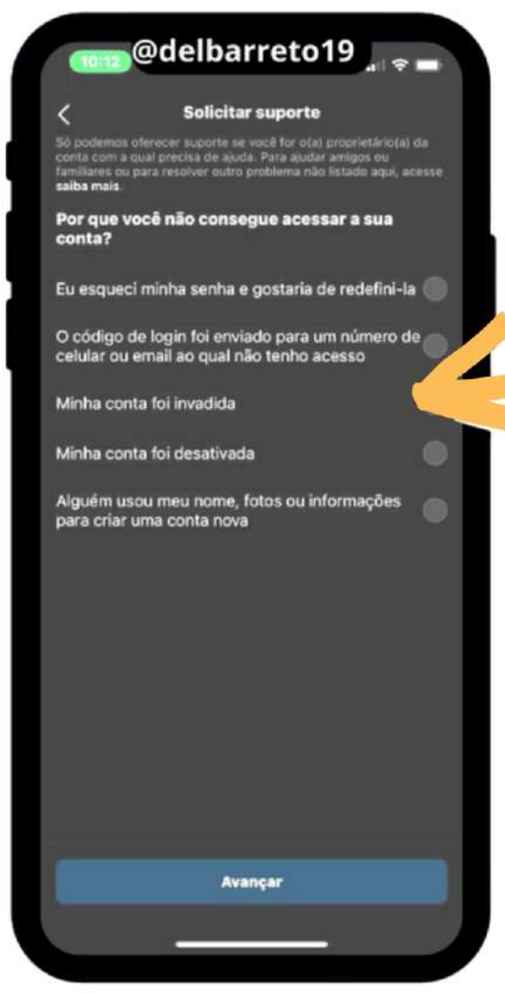
5- Coloque seu nome de usuário e marque: Preciso de mais ajuda.



6- Aparecerá a opção de receber uma mensagem com o final do seu telefone. Marque e solicite o código de segurança. Se o criminoso não tiver habilitado a verificação em duas etapas, você já poderá redefinir sua senha.

7- Se a verificação em duas etapas estiver habilitada, marque: tentar de outra forma.

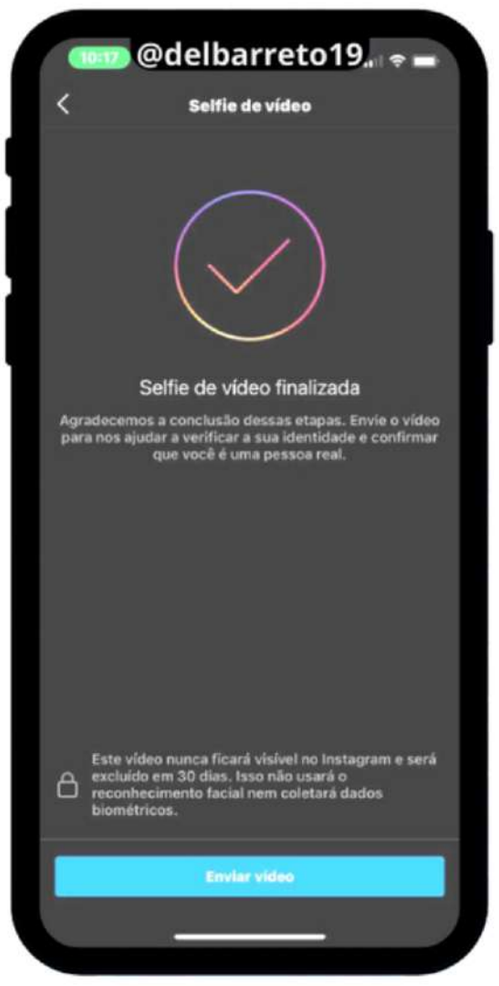
8- Escolha: obter suporte.



9-Marque: Minha conta foi invadida.

10- Se você tem uma foto sua no perfil, marque a primeira opção. Caso seja uma conta comercial e não tenha dado identificador, assinale a segunda alternativa.

11- Agora coloque o email novo que criou. Opte por um email novo. Conta antiga, geralmente, vai dar erro.



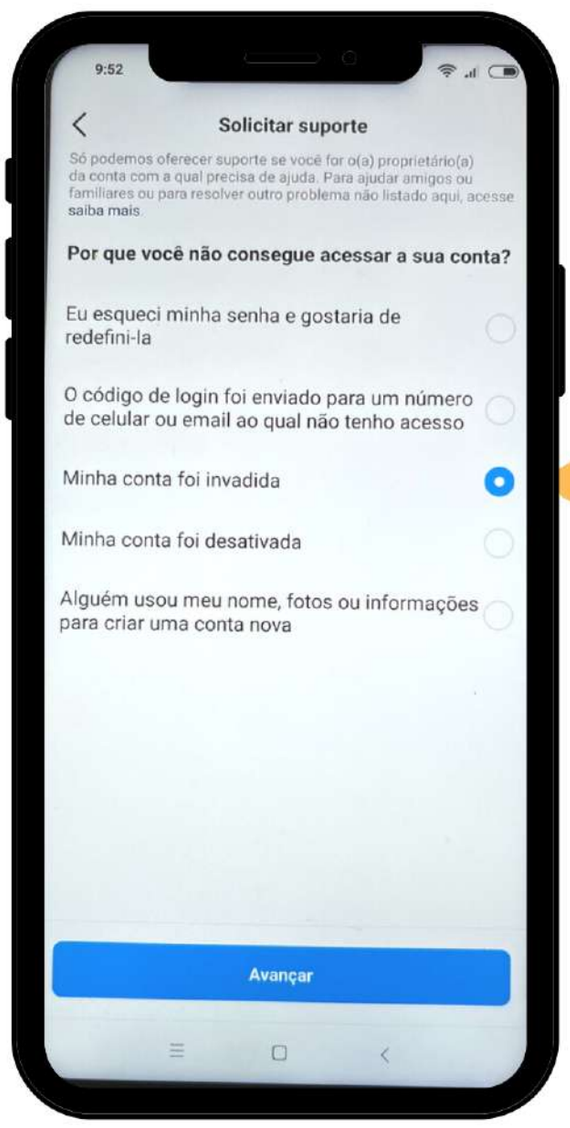
12- Faça um selfie de vídeo em local claro e clique em enviar. Você receberá uma confirmação. Acompanhe o email informado para recebimento do link de recuperação. Caso eles não aceitem o vídeo, reenvie.

RECUPERAÇÃO DE CONTA SUPORTE DO INSTAGRAM ANDROID

1- Acesse o Instagram e coloque o nome do usuário. Se o criminoso mudou, coloque o novo. Clique em: "Obtenha ajuda para entrar"

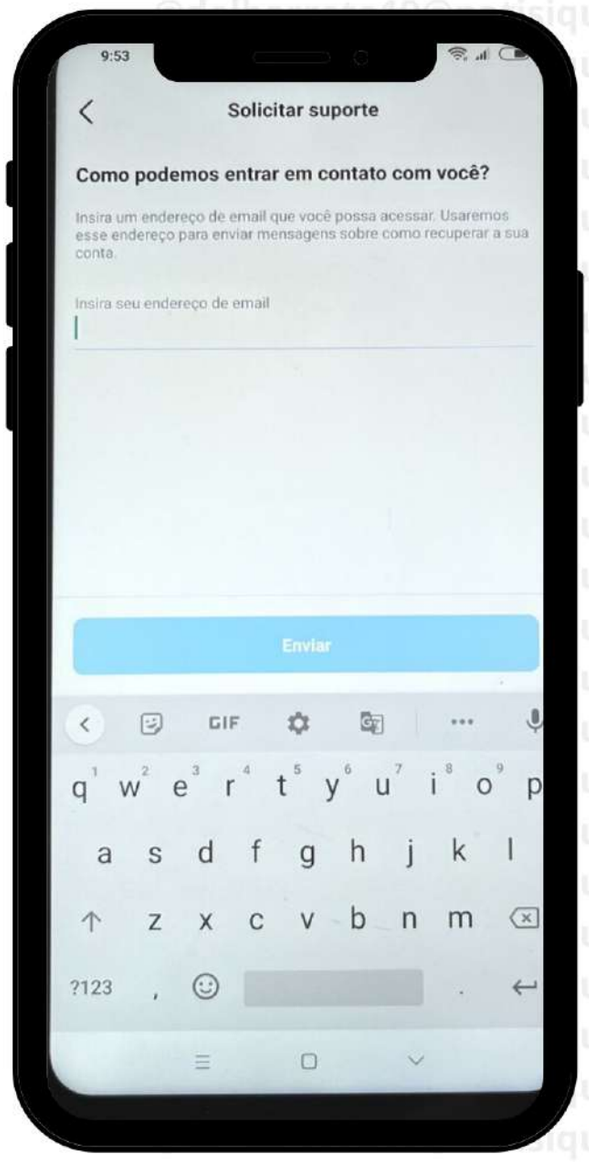
2- Coloque nome de usuário, email ou telefone e marque: 'Preciso de mais ajuda'. NÃO CLIQUE EM AVANÇAR.

3- Assinale: 'Não consigo acessar este email ou número de telefone.'

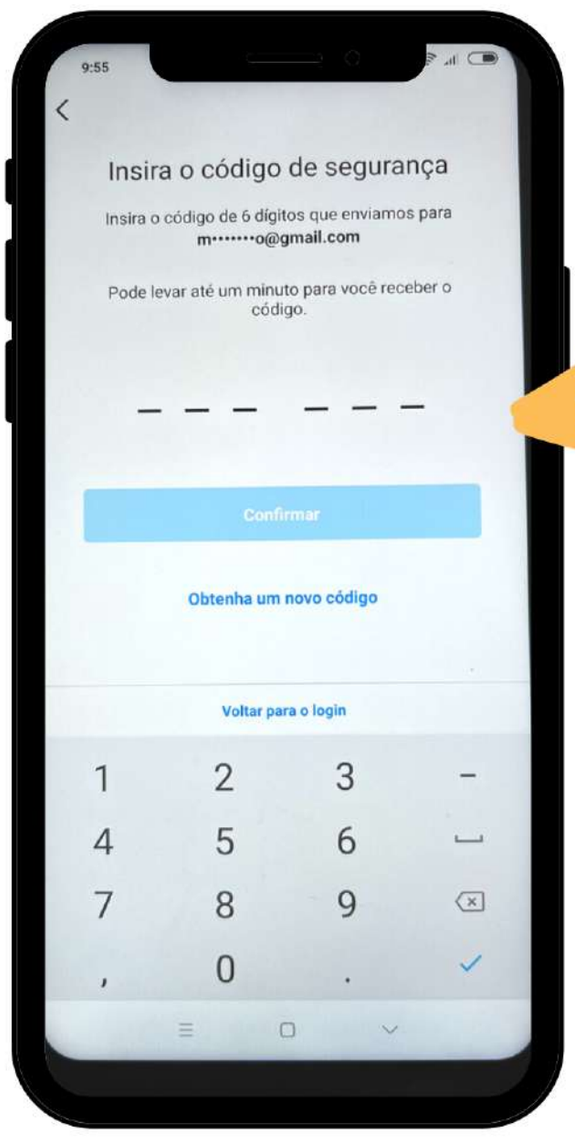


4- Marque: 'Minha conta foi invadida' e avançar.

5- Agora 'Sim, eu tenho uma foto minha na minha conta' e avançar.



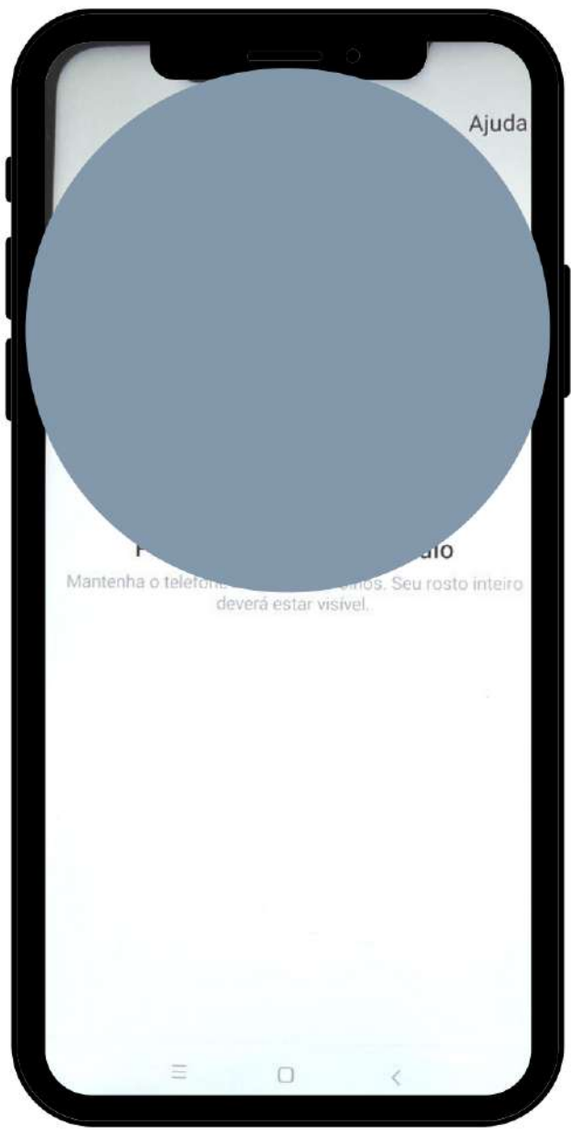
6- Informe um email para contato.
Se ocorreu um problema, crie outro.



7- Você receberá um código de confirmação. Insira e aperte em confirmar.

8- Aperte em avançar para iniciar a gravação de uma selfie de vídeo.

9- Siga as instruções para completar a selfie. Se ocorrer problema ao finalizar, faça de novo. Se iniciou com nome de usuário, tente agora com telefone ou email. Outra recomendação é instalar uma versão anterior do Instagram no smartphone e tentar novamente.



10- Não conseguiu recuperar mesmo assim? Faça uma notificação extrajudicial contra o Facebook ou ingresse na Justiça para obter uma ordem de recuperação.

RECUPERAÇÃO DE CONTA
NOTIFICAÇÃO EXTRAJUDICIAL

NOTIFICAÇÃO EXTRAJUDICIAL

_____(NOME E QUALIFICAÇÃO), _____(endereço e telefone de contato) vem, por meio desta, NOTIFICAR para proceder a recuperação de perfil hackeado na plataforma INSTAGRAM.

Sou proprietário (a) da conta _____ (nome de usuário), ___ seguidores, com telefone_____ (colocar +55 e DDD antes do número) e e-mail _____ vinculados.

No dia ___/___/___, por volta das __h, perdi o acesso à minha conta em razão do hackeamento (descrever o problema).

Informo, ainda, que a conta invadida está sendo utilizada para práticas delitivas, com prejuízos patrimoniais a terceiros. Acrescento que realizei tentativas de recuperação no suporte da página, todavia restaram infrutíferas, eis que o criminoso modificou a conta de email e o telefone vinculado. Com o intuito de solucionarmos a questão de forma amigável e extrajudicial, bem como mitigar os efeitos danosos desta prática delitiva e possibilitar ao usuário reativar seu perfil, solicito que a empresa encaminhe o link de recuperação da conta hackeada para o e-mail_____ (criar uma conta de email nova), no prazo de até 48 horas a contar do recebimento desta notificação.

Certo de que serei prontamente atendido, desde já agradeço sua compreensão.

Atenciosamente,

NOME E DOC DO NOTIFICANTE

Ao Facebook Serviços Online do Brasil Ltda
Rua Leopoldo Couto de Magalhães, 700, 6º andar
Itaim Bibi, São Paulo-SP

Não esqueça de demonstrar:

- **Ser proprietário da conta invadida;**
- **Nome de usuário, email e telefone vinculado com +55;**
- **Tentativa frustrada de recuperação pelo suporte;**
- **Prejuízos causados a terceiros;**
- **Email novo para recuperação;**
- **Endereço de entrega: Escritório de Advocacia Tozzini Freire Advogados, na Av. Paulista 2421, 8º andar, São Paulo, SP, CEP 01311-300.**

RECUPERAÇÃO DE CONTA INVADIDA
EMAIL INSTAGRAM

Para **security@mail.instagram.com**

Adicionar um assunto **Desativar Conta Invadida @nomedeusuario**

Nome completo:
Username:
Telefone vinculado: +55
Email Vinculado:

Prezado (a)
No dia ___ de _____ de 20__, minha conta foi invadida e está sendo utilizada para praticar crimes de estelionato contra meus seguidores. O criminoso assumiu minha identidade e, desde então, não obtive êxito no processo de recuperação pelo suporte.
As condutas por ele praticadas ferem os termos de uso do Instagram:

- **Você não pode se passar por outras pessoas ou fornecer informações imprecisas;**
- **Você não pode fazer algo ilícito, enganoso, fraudulento ou com finalidade ilegal;**

Assim sendo, gostaria que vocês tomassem as medidas necessárias para a recuperação da minha conta. Eventuais dúvidas, estarei à disposição no telefone e email para o processo de recuperação da minha identidade.
Certo de que serei prontamente atendido, desde já agradeço sua compreensão.

Agradecido,

Nome completo e username

Enviar | Descartar

RECUPERAÇÃO DE CONTA ORDEM JUDICIAL

Ordem judicial poderá determinar ao Facebook a recuperação da conta invadida. Na esfera cível, a determinação será encaminhada para o endereço da empresa em São Paulo. Já no âmbito criminal, a remessa será pela Plataforma Records.

A determinação deverá conter:

- **A identificação do perfil invadido (nome de usuário, telefone e email vinculados);**
- **Email novo para recebimento do link de recuperação da conta;**
- **Determinação para o fornecimento dos registros de conexão da conta invadida com a inclusão de: email, telefone, IPs, data, hora, timezone e porta lógica de origem da conexão.**

FOI VÍTIMA DESTE GOLPE? VEJA O QUE FAZER

Registre boletim de ocorrência e informe:

- **Narração dos fatos com informações de data e hora que perdeu acesso à conta;**
- **Dados do usuário, telefone, quantidade de seguidores e conta de email vinculada. Caso o perfil seja modificado, deve-se informar;**
- **Perda de acesso à conta: SIMSWAP ou engenharia social;**
- **Modus operandi: venda de produtos ou serviços e chaves pix informadas;**
- **Dados de contas bancárias, vítimas e prejuízos sofridos;**
- **Telefone e emails que manteve contato com o criminoso.**

Informe à instituição financeira que a conta do infrator é utilizada para prática de fraudes:

- **Fundamentação Legal- Lei Complementar 105/2001, art. 1º, § 3º,inc. IV;**
- **Envie cópia do boletim de ocorrência.**

FOI VÍTIMA DESTE Ggolpe?
RESPONSABILIDADE CIVIL

FUNDAMENTAÇÃO LEGAL

Código de Defesa do Consumidor:

- **Art. 14. O fornecedor de serviços responde, independentemente da existência de culpa, pela reparação dos danos causados aos consumidores por defeitos relativos à prestação dos serviços, bem como por informações insuficientes ou inadequadas sobre sua fruição e riscos.**

LEGITIMIDADE PASSIVA

- **Operadoras de telefonia móvel - perda da conta por ataque simswap;**
- **Bancos Digitais - criação de conta em nome da vítima para recebimento de valores indevidos;**
- **Instagram - falha no suporte e demora no processo de recuperação da conta.**

FOI VÍTIMA DESTE GOLPE?
SOLICITAÇÃO DE DADOS/SIMSWAP

Nos casos de troca indevida do simcard, a vítima deve fazer a solicitação dos seguintes documentos junto à operadora de telefonia móvel:

- **Protocolo de mudança da linha telefônica, com a indicação do dia, hora, funcionário e loja;**
- **Documentos de identificação anexados;**
- **Quando realizada por telefone, solicitar a respectiva gravação;**

IMEI, protocolos de internet e modelo do aparelho utilizado;

- **Registros de conexão após a mudança, devendo incluir IPs, data, hora, timezone e portas lógicas de origem da conexão.**

FRAUDES CONTRA INSTITUIÇÕES FINANCEIRAS E CLIENTES

SIMSWAP

Objetivo:

Acessar indevidamente a conta bancária da vítima para desviar valores e realizar empréstimos.

MODUS OPERANDI

A engenharia social é realizada por SMS ou email;

Como estória-cobertura, utilizam mensagens com informações de milhas a vencer, bloqueio de conta, compra indevida ou suspensão de chave pix;

O usuário, ao clicar no link enviado, é redirecionado para um site falso e fornece as credenciais de acesso;

O fraudador realiza, então, um simswap, ou seja, mantém contato com a operadora de telefonia móvel do usuário e solicita a portabilidade ou mudança de pós para pré-pago;

O usuário perde acesso ao telefone;

O atacante instala o chip recuperado em outro smatphone

Como já possui a credencial de acesso, entra na conta do usuário e realiza uma tentativa de transação financeira;

Aparece, em seguida, uma mensagem sobre dispositivo novo e a aceitação do token de transação por SMS permitindo acesso irrestrito à conta bancária;

Todos os valores ali existentes são desviados, além da realização de empréstimos e adiantamento do 13º salário.

Principais Alvos: Cliente de instituições financeiras que permitem a liberação de token de transação por SMS.

PROTEÇÃO

Bloqueie junto à sua instituição financeira a liberação de token de transação via SMS. Opte, sempre, por autorização do dispositivo através de caixas de autoatendimento;

Desconsidere as mensagens enviadas por email ou SMS sobre: milhas a vencer, bloqueio de conta, descadastramento de chave pix;

Jamais clique em links e forneça suas credenciais de acesso do banco;

Se possível, vincule seus serviços com telefonia voip e não exponha informações pessoais nas redes sociais;

Fique atento com perda de sinal do smartphone;

Acompanhe, com frequência, sua movimentação bancária;

Utilize autenticação em dois fatores nos seus serviços

FOI VÍTIMA DESTE GgolpE? VEJA O QUE FAZER

Registre boletim de ocorrência e informe:

- **Dia e hora que ocorreu o fato com a descrição do problema;**
- **Modus operandi;**
- **Data do último acesso da conta bancária e linha telefônica;**
- **Número de telefone (vítima e infrator), conta bancária e valores subtraídos;**
- **Se possuir as contas dos beneficiários, informe.**
- **Pessoas envolvidas, testemunhas e declarantes;**
- **Comunique se recebeu SMS ou email sobre milhas a vencer, atualização cadastral, etc.**

Restituição dos Valores:

- **Procure sua agência bancária e faça uma solicitação de restituição dos valores subtraídos.**
- **Informe à instituição financeira que a conta do infrator é utilizada para prática de fraudes:**
- **Fundamentação Legal- Lei Complementar 105/2001, art. 1º, § 3º,inc. IV;**
- **Envie cópia do boletim de ocorrência.**

Responsabilidade Civil:

- **Ação Judicial contra a Operadora de Telefonia por falha na prestação do serviço no caso de SIMSWAP - Art. 14 do CDC.**

SMISHING

Objetivo:

Envio de phishing por SMS para convencer a vítima a repassar informações pessoais ou financeiras.

MODUS OPERANDI

Envio de phishing por SMS;

Utilizam engenharia social do medo:

- **Atualização de dados cadastrais da conta;**
- **Bloqueio de conta;**
- **Aplicativo suspenso;**
- **Compras indevidas no cartão de crédito;**
- **Pontos de milhagem a expirar.**

Ao clicar no link, o usuário é direcionado para uma página falsa com preenchimento de informações financeiras;

O criminoso utilizará estes dados para acessar as contas bancárias ou fazer compras indevidas na internet.

PROTEÇÃO

Nunca clique em links enviados por SMS;

Não forneça informações pessoais por telefone;

Atenção com erros de digitação e mensagens em caráter de urgência para cumprir uma tarefa (cadastrar conta, fornecer dados);

Bloqueie os números que enviaram conteúdo malicioso para você;

As instituições financeiras não mandam este tipo de solicitação por SMS.

FOI VÍTIMA DESTE GOLPE? VEJA O QUE FAZER

Registre boletim de ocorrência e informe:

- **Dia e hora que ocorreu o fato com a descrição do problema;**
- **Modus operandi;**
- **Telefone da vítima, número que enviou a mensagem e conteúdo;**
- **Valores subtraídos da conta bancária;**
- **Se possuir contas de favorecidos, comunique.**

Restituição dos Valores:

- **Procure sua agência bancária e faça uma solicitação de restituição dos valores subtraídos.**

VISHING

Objetivo:

Contato com a vítima através de chamadas telefônicas (voice + phishing) para convencer a repassar informações pessoais, financeiras, autorizar dispositivos ou fazer transferências para contas de terceiros.

MODUS OPERANDI

O criminoso utiliza serviços de telefonia fixa ou voip e simula o ambiente de auto-atendimento;

Como engenharia social empregam:

- **Suporte ou manutenção do serviço;**
- **Atualização cadastral;**
- **Atividade suspeita na conta do usuário;**

A vítima, acreditando estar falando com o banco, repassa informações pessoais, financeiras ou autoriza dispositivos;

De posse dessas informações, o infrator consegue acesso às contas da vítima, transfere valores e realiza empréstimos;

Em outros casos realiza compras fraudulentas em plataformas de comércio eletrônico.

PROTEÇÃO

Utilize serviços para bloqueio de chamadas indesejadas;

Opte sempre pelos canais oficiais para falar com seu banco;

Desconfie de chamadas inesperadas com ofertas atrativas;

As instituições financeiras não pedem informações pessoais por telefone. Se houver a solicitação durante a conversa, provavelmente trata-se de golpe.

FOI VÍTIMA DESTE GOLPE? VEJA O QUE FAZER

Registre boletim de ocorrência e informe:

- **Dia e hora que ocorreu o fato com a descrição do problema;**
- **Modus operandi;**
- **Telefone da vítima e número utilizado para contato;**
- **Valores subtraídos na conta bancária;**
- **Se possuir contas de favorecidos, informe.**

Restituição dos Valores:

- **Procure sua agência bancária e faça uma solicitação de restituição dos valores subtraídos.**

Informe à instituição financeira que a conta do infrator é utilizada para prática de fraudes:

- **Fundamentação Legal- Lei Complementar 105/2001, art. 1º, § 3º,inc. IV.**

PHARMING

Objetivo:

Direcionar os usuários para sites fraudulentos e capturar dados pessoais.

MODUS OPERANDI

Inicia com a alteração do arquivo host no computador da vítima ou exploração de vulnerabilidades no servidor DNS;

O servidor DNS é "envenenado" e o usuário, ao digitar um endereço de um site no navegador, é redirecionado para um domínio malicioso;

O infrator consegue, com esta prática, capturar credenciais de acesso, dados bancários e informações pessoalmente identificáveis.

PROTEÇÃO

Não abra email de fontes desconhecidas e jamais clique em links ou anexos recebidos.

Utilize provedores de serviços confiáveis;

Habilite a verificação em duas etapas nos seus serviços;

Configure seu roteador e modifique a senha default;

Atenção para sites sem certificado;

Antivírus e sistema operacional devem estar atualizados.

FOI VÍTIMA DESTE GOLPE? VEJA O QUE FAZER

Registre boletim de ocorrência e informe:

- **Dia e hora que ocorreu o fato com a descrição do problema;**
- **Modus operandi;**
- **Telefone da vítima, número que enviou a mensagem e conteúdo;**
- **Valores subtraídos na conta bancária;**
- **Procure o canal oficial da empresa com site phishing e denuncie.**

FRAUDE DO CARTÃO AUSENTE

Objetivo:

Criar cartões de crédito com validação do CVV a fim de realizar compras na internet ou vender dados em fóruns ou grupos de mensageria.

MODUS OPERANDI

O fraudador utiliza softwares para criar cartões de crédito aleatórios com números, bandeira e data de vencimento válida;

Para poder fazer compras no comércio ou negociar o cartão, há necessidade de obter o CVV (03 números que ficam na parte detrás do cartão);

A identificação de um CVV exige até 999 tentativas;

O criminoso procura sites testes: instituição beneficente ou religiosa para doação e estabelecimentos de hotelaria para reservas;

A fim de agilizar a tarefa, emprega scripts para adivinhar o CVV em menor tempo possível;

Os cartões validados são utilizados para compras em sites que exigem poucos dados (número, bandeira, vencimento e CVV) ou vendidos em fóruns de carders e grupos de mensageria;

Em tese, a vítima poderá ter seu cartão clonado sem nunca ter sido utilizado para compras na internet.

PROTEÇÃO

Acompanhe sua movimentação financeira, especialmente microfaturas;

Atuação das empresas de hotelaria ou instituição beneficente:

- **Implementar regras com bloqueio em mais de 03 tentativas de reserva ou doação com o mesmo cartão;**
- **Estabelecer um valor mínimo para a transação financeira;**
- **Implementar captcha para dificultar a ação de scripts automatizados;**

FOI VÍTIMA DESTE GOLPE? VEJA O QUE FAZER

Registre boletim de ocorrência e informe:

- **Dia e hora que ocorreu o fato com a descrição do problema;**
- **Modus operandi;**
- **Dados do cartão de crédito com a respectiva bandeira e valores subtraídos da conta bancária;**
- **Estabelecimentos beneficiados com os valores desviados;**
- **Pagamento de microfaturas nos meses anteriores.**

Procure a instituição financeira e faça uma solicitação de restituição dos valores subtraídos.

GOLPE DO EXTRAVIO DE CARTÃO

Objetivo:

Realizar compras indevidas na internet com cartão de terceiro.

MODUS OPERANDI

O cartão de crédito ou débito é furtado na entrega ou em caixas de correio;

O criminoso, utilizando uma call center fake, liga para a vítima e informa da subtração do cartão;

Para evitar fraudes e providenciar o bloqueio, o fraudador solicita algumas informações pessoais, inclusive a senha do cartão;

A partir de então, efetua saques e realiza compras indevidas na internet.

PROTEÇÃO

Nunca informe senhas de cartão ou qualquer outro serviço;

Desconfie de ligações indesejadas;

Utilize apenas os canais oficiais do banco para fazer solicitações;

Acompanhe, constantemente, os lançamentos na sua fatura;

Cadastre-se no Registrato para acompanhar empréstimos realizados em seu nome;

Nunca repasse informações pessoalmente identificáveis.

FOI VÍTIMA DESTE GOLPE? VEJA O QUE FAZER

Registre boletim de ocorrência e informe:

- **Descrição do fato;**
- **Prejuízos causados;**
- **Estabelecimentos e detalhamento das compras indevidas;**
- **Dados individualizadores do autor, se possuir.**

FALSO MOTOBOY

Objetivo:

Obter o cartão do banco da vítima para subtrair valores e/ou efetuar compras em sites de comércio eletrônico.

MODUS OPERANDI

Os idosos são as maiores vítimas deste tipo de crime;

O criminoso simula um atendimento com uma chamada de uma falsa central de segurança do banco;

Na ligação, ele informa sobre a clonagem do cartão com uma compra de valor considerável e do motoboy que enviará na residência para recolhimento e posterior bloqueio;

O golpista solicita a senha e pede para a vítima cortar o cartão ao meio, todavia, a trilha e o chip devem permanecer intactos;

O motoboy se dirige a residência para buscar o cartão;

Os golpistas utilizam o cartão para fazer compras em nome da vítima.

PROTEÇÃO

Desconfie de contatos por telefone, mesmo que sejam números semelhantes aos dos bancos. Criminosos usam técnicas spoofing para enganar você;

As instituições financeiras jamais te ligam para solicitar senhas e nunca mandam mensageiros para buscar cartões de crédito;

Não entregue seu cartão a terceiros e recuse visitas de motoboys para tal;

Sempre utilize os canais oficiais do banco para comunicação;

Identificou qualquer irregularidade, ligue imediatamente para a instituição financeira e efetue o bloqueio do cartão;

Sempre que possível, utilize cartões virtuais e com limites baixos para cadastro em delivery.

FOI VÍTIMA DESTE GOLPE? VEJA O QUE FAZER

Registre boletim de ocorrência e informe:

- **Dia e hora que ocorreu o fato com a descrição do problema;**
- **Modus operandi;**
- **Compra, valores, empresa, endereço de entrega e motoboy responsável (buscar essas informações no aplicativo);**
- **Compras indevidas, valores e estabelecimentos beneficiados.**

Procure a instituição financeira e solicite a restituição dos valores subtraídos.

Ggolpe do delivery

Objetivo:

Cobrar faturas elevadas no momento da entrega.

MODUS OPERANDI

A fraude é praticada com a participação de entregadores cadastrados em serviços de delivery;

Possui três modalidades:

- **Pagamento da fatura - o entregador informa que o visor da maquininha está danificado e cobra um valor elevado sem que o usuário perceba;**

- **Ligação do estabelecimento - valor a menos na hora da fatura e o comprador necessita pagar adicional na hora da entrega;**

- **Problemas com o pagamento - valor não foi creditado e pede para fazê-lo quando o entregador chegar.**

A vítima só irá perceber o golpe no fechamento da fatura do cartão de crédito.

PROTEÇÃO

Opte sempre pelo pagamento dentro do aplicativo.
Se for pagar na entrega, prefira dinheiro;

Pagamento com cartão, jamais entregue a terceiros, utilize a função crédito e cubra as informações do CVV;

Desconfie de celulares com visor quebrado ou cobertos com adesivos;

Fique atento ao uso do celular do entregador no momento do pagamento;

Mantenha contato com sua instituição financeira e efetue o bloqueio do cartão de crédito;

Foi vítima, procure o aplicativo para relatar o problema e registre ocorrência policial.

FOI VÍTIMA DESTE GOLPE? VEJA O QUE FAZER

Registre boletim de ocorrência e informe:

- **Dia e hora que ocorreu o fato com a descrição do problema;**
- **Modus operandi;**
- **Compra, valores, empresa, endereço de entrega e motoboy responsável (buscar essas informações no aplicativo);**
- **Se foi feito algum contato por telefone, informe o número;**
- **Compras indevidas, valores e estabelecimentos beneficiados.**

Procure a instituição financeira e solicite a restituição dos valores subtraídos.

GgolpE do delivery 2

Objetivo:

Obter os dados do cartão da vítima para fazer compras abusivas na internet.

MODUS OPERANDI

A fraude é praticada com a participação de entregadores cadastrados em serviços de delivery;

O entregador alega que precisa obter um melhor sinal da maquininha e consegue, sem que a vítima perceba, filmar os dados de cartão de crédito;

No momento do pagamento, ele se oferece para iluminar a máquina com seu smartphone e termina por capturar a senha digitada;

O golpista utiliza os dados do cartão para fazer compras na internet.

PROTEÇÃO

Opte sempre pelo pagamento dentro do aplicativo.
Se for pagar na entrega, prefira dinheiro;

Pagamento com cartão, jamais entregue a terceiros, utilize a função crédito e cubra as informações do CVV;

Fique atento ao uso do celular do entregador no momento do pagamento;

Mantenha contato com sua instituição financeira e efetue o bloqueio do cartão de crédito;

Foi vítima, procure o aplicativo para relatar o problema e registre ocorrência policial.

FOI VÍTIMA DESTE GOLPE? VEJA O QUE FAZER

Registre boletim de ocorrência e informe:

- **Dia e hora que ocorreu o fato com a descrição do problema;**
- **Modus operandi;**
- **Compra, valores, empresa, endereço de entrega e motoboy responsável (buscar essas informações no aplicativo);**
- **Se foi feito algum contato por telefone, informe o número;**
- **Compras indevidas, valores e estabelecimentos beneficiados.**

Procure a instituição financeira e solicite a restituição dos valores subtraídos.

GOLPE DA SELFIE

Objetivo:

Fazer reconhecimento facial da vítima para financiamento de veículo.

MODUS OPERANDI

Os dados da vítima são obtidos através de data brokers ilegais em sites e fóruns da internet;

O golpista acessa o aplicativo da instituição financeira e preenche os dados para financiar um veículo;

Simula uma ligação de um call center e diz que a vítima foi contemplada com um brinde a ser entregue por um motoboy;

Ao chegar na casa da vítima, o fraudador acessa o aplicativo do banco e deixa no ponto de realizar a selfie para finalizar o financiamento;

Para não gerar desconfiança, esconde a tela do smartphone e pede que a vítima deixe-se fotografar para confirmar o recebimento do brinde.

PROTEÇÃO

Desconfie de brindes e ofertas enviados para sua residência de maneira não solicitada. Recuse-os;

Não permita tirar fotografias suas para confirmação de entrega;

Jamais compartilhe com terceiros fotografia de documentos de identificação e comprovantes de endereço;

Habilite o serviço Registrato do Banco Central para acompanhar eventuais empréstimos realizados em seu nome;

Foi vítima? Registre ocorrência policial e procure a instituição financeira para contestar o financiamento.

FOI VÍTIMA DESTE GOLPE? VEJA O QUE FAZER

Registre boletim de ocorrência e informe:

- **Dia e hora que ocorreu o fato com a descrição do problema;**
- **Modus operandi;**
- **Detalhes da entrega do brinde pelo mensageiro (selfie, documentos pessoais repassados);**
- **Contatos realizados por telefone ou email;**
- **Empréstimos realizados com as respectivas instituições de crédito;**

Procure a instituição financeira e informe sobre a fraude.

CARTA DE CRÉDITO FALSA

Objetivo:

Receber valores indevidos através de engenharia social de carta de crédito de veículo.

MODUS OPERANDI

O fraudador oferece cartas de crédito para aquisição de veículos em sites e redes sociais com liberação entre 40 a 60 dias;

Para fortalecer a narrativa, utiliza call centers falsas de instituições financeiras;

São exigidos valores iniciais para a liberação da carta e, por vezes, os criminosos orientam a vítima a se dirigir à concessionária para reservar o veículo;

Vencido o prazo, o criminoso bloqueia a vítima para contato.

PROTEÇÃO

Desconfie de ofertas de cartas de crédito disponibilizadas em redes sociais ou através dos mecanismos de busca;

Opte por fazer negócios com administradoras conhecidas;

Nunca deposite valores antecipados para assegurar a aquisição.
Cuidado com engenharia social;

Preços muito atrativos: corra, é golpe!

Utilize sempre os canais oficiais para entrar em contato com as administradoras;

Procure informações sobre a empresa em mecanismos de busca.

FOI VÍTIMA DESTE GOLPE? VEJA O QUE FAZER

Registre boletim de ocorrência e informe:

- **Dia e hora que ocorreu o fato com a descrição do problema;**
- **Modus operandi;**
- **Redes sociais, mecanismos de busca ou sites do empréstimo fraudulento (detalhar os perfis e/ou URLs do conteúdo);**
- **Contas bancárias ou chaves pix informadas para depósito;**
- **Emails, telefones e redes sociais do fraudador, quando possível.**

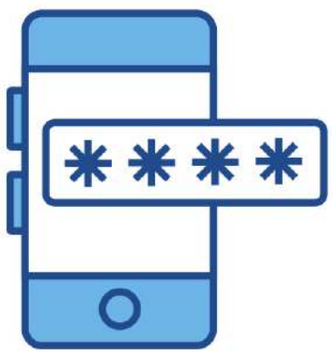
ROUBO/FURTO DE SMARTPHONE E ACESSO ÀS CONTAS BANCÁRIAS

Objetivo:

Subtrair valores de conta da vítima de smartphone roubado ou furtado.

MODUS OPERANDI

O golpe se inicia com a subtração do smartphone, especialmente quando ela está com o aparelho destravado;



Posteriormente o criminoso acessa o bloco de notas no aparelho e busca senhas salvas de bancos ou verifica se na caixa de email há alguma anotação relacionada;

Com estes dados, entra no aplicativo do banco e transfere valores para contas de terceiros;

Em alguns casos, eles criam contas fakes da vítima em bancos digitais para transferência de valores entre instituições financeiras.

PROTEÇÃO

Altere o código pin do simcard

Habilite o bloqueio de tela no dispositivo e coloque o menor tempo permitido;

Nunca salve senhas de bancos no bloco de notas do seu smartphone;

Para cada serviço você deve possuir uma senha distinta;

Não deixe aplicativos de banco abertos após a utilização;

O smartphone foi subtraído? Entre em contato com seu banco e bloqueie o app e toda e qualquer transação online;

Avise sua operadora e cancele o simcard subtraído;

Não guarde informações pessoalmente identificáveis ou credenciais de acesso no seu dispositivo.

FOI VÍTIMA DESTE GOLPE? VEJA O QUE FAZER

Registre boletim de ocorrência e informe:

- **Dia e hora que ocorreu o fato com a descrição do problema;**
- **Modus operandi;**
- **Detalhes sobre a subtração do smartphone;**
- **Bloqueio do aparelho com senhas?**
- **Havia código pin no simcard?**
- **Guarda de senha no bloco de notas;**
- **Conta bancária, valores subtraídos e dados dos beneficiados com as transferências;**
- **Compras realizadas;**
- **Emails, telefones e redes sociais do fraudador, quando possível.**

Procure a instituição financeira e solicite a restituição dos valores subtraídos.

APLICATIVOS FALSOS DE INSTITUIÇÕES FINANCEIRAS

Objetivo:

Obter as credenciais de acesso de contas bancárias de terceiros.

MODUS OPERANDI

O fraudador disponibiliza apps falsos da instituição financeira em lojas oficiais;

Posteriormente, publica o link para download em redes sociais ou envia por email. Alega, para tanto, que há problemas de segurança com o aplicativo instalado e pede para baixar a nova versão;

Após obter login e senha, a depender da instituição financeira, o criminoso terá acesso à conta bancária.

PROTEÇÃO

Baixe os aplicativos necessários e faça o download em lojas oficiais;

Jamais faça download por meio de links de email, redes sociais ou encontrados no Google;

Mesmo que o app tenha sido baixado em loja oficial, verifique:

- **Informações do desenvolvedor;**
- **Quantidade de downloads;**
- **Avaliações do app;**
- **Eventuais erros encontrados;**
- **Google.**

Encontrou um app falso? Denuncie na loja oficial;

Mantenha o app sempre atualizado e fique atento com permissões desnecessárias.

FOI VÍTIMA DESTE GOLPE? VEJA O QUE FAZER

Registre boletim de ocorrência e informe:

- **Dia e hora que ocorreu o fato com a descrição do problema;**
- **Modus operandi;**
- **Como fez o download do aplicativo: email, links em mensageria, indicação em rede social;**
- **Individualização do app (URL, desenvolvedor, quantidade de downloads)**
- **Prejuízos financeiros decorrentes e conta acessada**

Denuncie na loja oficial o app utilizado na prática do crime por violação aos termos de uso ou diretrizes da comunidade.

PIX

FALSO FUNCIONÁRIO DE BANCO E CADASTRO PIX

Objetivo:

Obter dados pessoais e financeiros do correntista.

MODUS OPERANDI

Com o pretexto de cadastrar chave pix, o fraudador manda email ou telefona para o cliente de uma instituição financeira;

Menciona sobre a obrigatoriedade de cadastrar a chave pix, solicita informações pessoais ou envia links maliciosos para preenchimento das credenciais de acesso.

PROBLEMAS COM O PIX

Objetivo:

Obter dados pessoais e financeiros do correntista.

MODUS OPERANDI

O golpista envia mensagens por email, SMS ou WhatsApp sobre problemas técnicos com o PIX;

Alega que o cliente pode tirar proveito deste defeito e receber o valor em dobro se fizer uma transferência para uma chave pix informada;

Na expectativa de receber esta quantia, a vítima rapidamente faz a transferência.

CENTRAL DE ATENDIMENTO FALSA EM APLICATIVO DE MENSAGERIA

Objetivo:

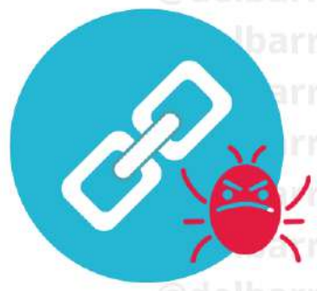
Obter dados pessoais e financeiros do correntista.

MODUS OPERANDI

Golpista cria perfis fakes no WhatsApp ou Telegram;

Envia mensagens avisando que o precisa atualizar dados relacionados as chaves PIX;

Manda links maliciosos para capturar dados financeiros do correntista.



PROTEÇÃO

O pix é seguro, mas esteja atento em abordagens com engenharia social;

Limite o valor diário de transações pix;

Engenharia social do medo: desconsidere as mensagens de descadastramento de chave pix, problemas técnicos, recompensas, ofertas tentadoras;

Faça o cadastro da chave apenas pelo aplicativo do banco;

Nunca forneça informações pessoais por telefone ou preencha formulários enviados por link;

Atenção com QR code falso e evite fazer transações com wi-fi pública.

FOI VÍTIMA DESTE GOLPE? VEJA O QUE FAZER

Registre boletim de ocorrência e informe:

- **Dia e hora que ocorreu o fato com a descrição do problema;**
- **Modus operandi;**
- **Chaves pix da vítima e infrator; Individualização do app (URL, desenvolvedor, quantidade de downloads)**
- **Valores transferidos e dados dos favorecidos;**
- **Compras realizadas em plataformas de comércio eletrônico;**
- **Abertura de contas em bancos digitais;**
- **SMS, emails ou contatos por redes sociais e mensageria**

PIX

MECANISMO ESPECIAL DE DEVOLUÇÃO

É a possibilidade de devolução de valores transferidos por pix nos casos de fraude ou falha operacional do sistema.

Como funciona:

• O usuário informa ocorrência de fraude;
• A agência dele entra em contato com a unidade recebedora e solicita o bloqueio dos valores;
• O usuário recebedor é notificado do bloqueio e do débito em conta;
• A transação constará no extrato de movimentações e, caso a fraude seja confirmada, os valores serão devolvidos.

Previsão:

• Resolução nº 103/2021 do Banco Central do Brasil.

FRAUDES POR EMAIL

SPRAY AND PRAY

Objetivo:

Extorsão por email com pagamento em pix ou criptoativos.

MODUS OPERANDI

Milhares de emails são enviados para usuários com informação de comprometimento da conta e, para que o conteúdo não seja espalhado, há exigência de pagamento indevido;

Normalmente, o infrator fala que possui o histórico de navegação do usuário, inclusive com conteúdo íntimo;

A vítima acredita que seu dispositivo foi invadido, daí o nome do golpe spray and pray (espalhe e reze);

O criminoso afirma ter acesso ao dispositivo do usuário (emails, webcam, sites acessados, conteúdo íntimo);

Em regra, as mensagens são redigidas em inglês e o pagamento é feito em criptoativos.

PROTEÇÃO

Desconsidere as mensagens recebidas por email com prática de extorsão;

Não pague os valores exigidos;

Nunca interaja com o criminoso e jamais repasse seu número de telefone;

Antivírus e sistema operacional atualizados;

Desative a webcam quando não estiver em uso;

Proteja seu email e contas de redes sociais com autenticação em dois fatores por aplicativos;

Avise aos seus familiares da extorsão e registre ocorrência policial.

FOI VÍTIMA DESTE GOLPE? VEJA O QUE FAZER

Registre boletim de ocorrência e informe:

- **Dia e hora que ocorreu o fato com a descrição do problema;**
- **Endereços de email, perfis e números de telefone utilizados para a prática de extorsão;**
- **Dados individualizadores do autor;**
- **Contas bancárias, carteiras e chaves pix informadas.**

Informe à instituição financeira que a conta do infrator é utilizada para prática de fraudes:

- **Fundamentação Legal- Lei Complementar 105/2001, art. 1º, § 3º,inc. IV;**
- **Envie cópia do boletim de ocorrência.**

BEC - BUSINESS EMAIL COMPROMISE

Objetivo:

Receber vantagem indevida através do envio de emails aparentemente legítimos.

MODUS OPERANDI

O fraudador obtém informações sobre a rotina de uma pessoa ou empresa em redes sociais;

Em seguida, cria contas de email aparentemente legítimas e envia para a vítima orientando a fazer um pagamento;

A fraude não é descoberta de imediato e acarreta prejuízos milionários a pessoas físicas e jurídicas.

PROTEÇÃO

Não exponha informações pessoais ou da empresa em redes sociais. Gerencie sua privacidade;

Configure o servidor de email para bloquear spam e evitar spoofing;

Faça a dupla verificação para toda e qualquer ordem de pagamento;

Atenção para engenharia social do medo: email aparentemente enviado por alguém da diretoria para convencer o funcionário a fazer pagamento;

Examine subtração ou adição no endereço de email e eventuais erros de digitação;

Educação digital e conscientização são de suma importância para prevenção deste tipo de ataque.

FOI VÍTIMA DESTE GOLPE? VEJA O QUE FAZER

Registre boletim de ocorrência e informe:

- **Descrição do fato;**
- **Prejuízos causados;**
- **Dados individualizadores autor;**
  *** Email enviados e recebidos;**
  *** Perfis em rede sociais;**
  *** Telefone;**
  *** Mensageria.**
- **Contas bancárias, carteiras e chaves pix informadas.**

Informe à instituição financeira que a conta do infrator é utilizada para prática de fraudes:

- **Fundamentação Legal- Lei Complementar 105/2001, art. 1º, § 3º,inc. IV;**
- **Envie cópia do boletim de ocorrência.**

WHALE PHISHING

Objetivo:

Receber valores ou obter informações sigilosas da empresa através de ataques de engenharia social

MODUS OPERANDI

A abordagem inicia-se com a coleta de informações dos funcionários em redes sociais de perfis profissionais;

De posse dos dados, rotina e da função de cada um na empresa, o criminoso, com técnicas de engenharia social, cria emails personalizados do CEO ou de executivos de alto escalão;

Posteriormente, envia mensagens para os funcionários do financeiro ou aqueles que possuem informações sigilosas ou estratégicas da empresa;

Algumas mensagens são convincentes e solicitam transferências de valores ou encaminhamento da cópia de projeto da empresa em andamento;

Por vezes, o ataque só é identificado dias após.

PROTEÇÃO

Tenha um duplo fator de confirmação para pagamentos ou compartilhamento de informações sigilosas da empresa;

Verifique o email recebido. O infrator cria contas semelhantes com adição ou subtração de letras do email do CEO ou de executivos da empresa;

Atente para erros de digitação no corpo do texto;

Oriente os funcionários a não expor informações pessoalmente identificáveis em redes sociais;

Configure o servidor de email para bloquear spam e evitar spoofing;

Educação digital e conscientização são de suma importância para prevenção deste tipo de ataque.

FOI VÍTIMA DESTE GOLPE? VEJA O QUE FAZER

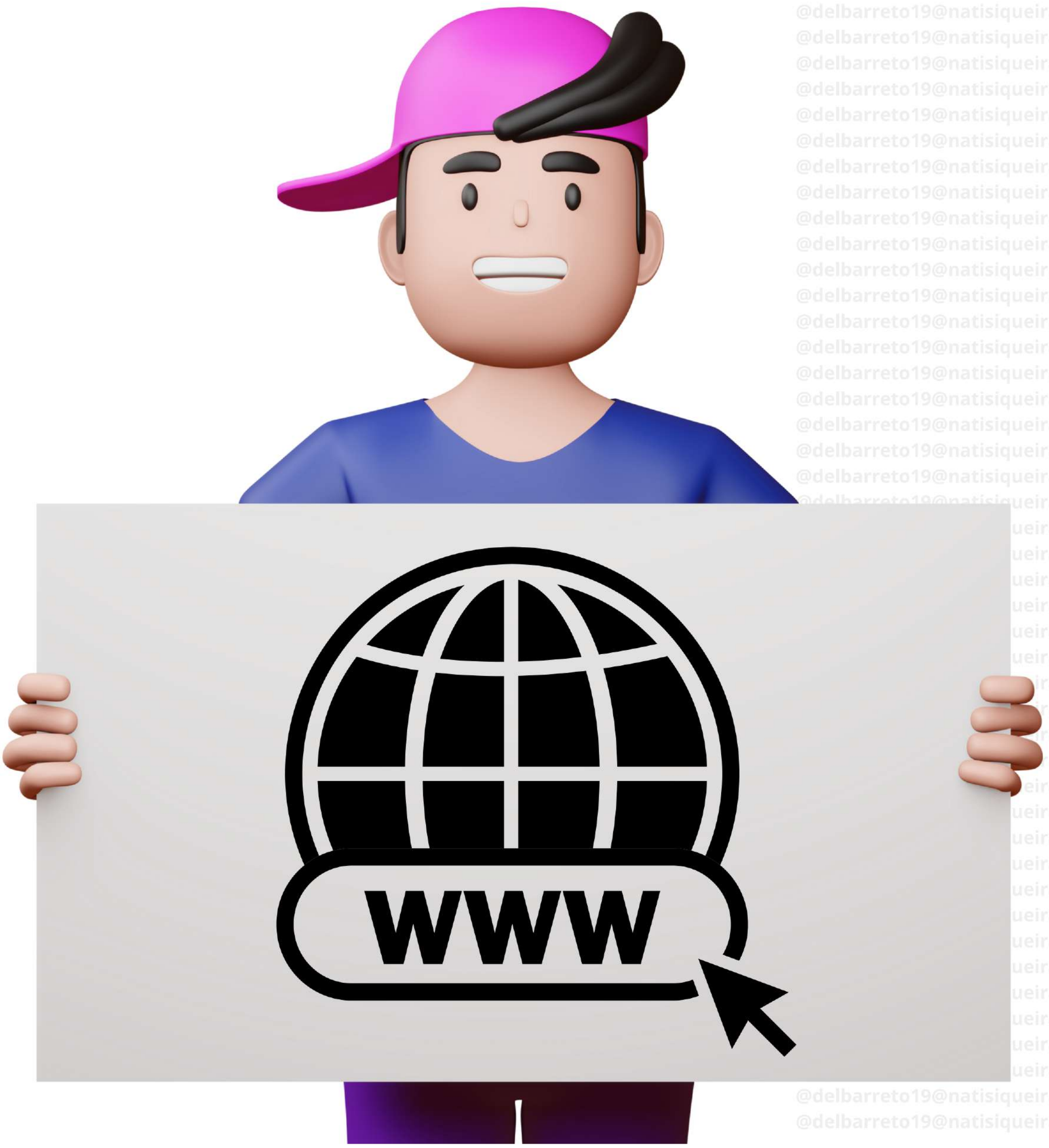
Registre boletim de ocorrência e informe:

- **Descrição do fato;**
- **Prejuízos causados;**
- **Dados individualizadores autor;**
  *** Email enviados e recebidos;**
  *** Perfis em rede sociais;**
  *** Telefone;**
  *** Mensageria.**
- **Contas bancárias, carteiras e chaves pix informadas.**

Informe à instituição financeira que a conta do infrator é utilizada para prática de fraudes:

- **Fundamentação Legal- Lei Complementar 105/2001, art. 1º, § 3º,inc. IV;**
- **Envie cópia do boletim de ocorrência.**

COMPRAS NA INTERNET



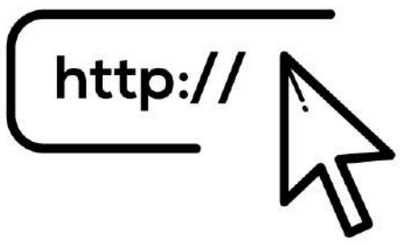
LEILÃO FALSO DE VEÍCULOS

Objetivo:

Obter vantagem ilícita através de sites falsos de leilão de veículos na internet.

MODUS OPERANDI

O criminoso contrata um serviço para registrar e hospedar sites falsos de leilão de veículos;



Os sites utilizam nomes de domínio semelhantes aos originais e empregam imagens de veículos obtidas na internet;

Os preços para arrematar são bem baixos para atrair potenciais consumidores;

O usuário faz uma oferta online e rapidamente é informado da contemplação;

Recebe, por conseguinte, um contrato em papel timbrado para preenchimento, com a cópia dos documentos de identificação;

Para finalizar o golpe, o criminoso exige depósito prévio do lance em conta de pessoa física;

Após isso, os contatos são encerrados e o veículo nunca será entregue.

PROTEÇÃO

Desconfie de veículos com preços irresistíveis;

Use o Google para buscar imagens semelhantes do veículo ofertado;

Verifique as informações de registro e hospedagem do site. Se for novo, caia fora;

Não envie nenhum valor até que um contato seu verifique o veículo de forma presencial;

Procure em sites de fraudes informações sobre o domínio que oferta o veículo;

Procure em sites de mapas as informações sobre o endereço onde o "leiloeiro" informa sobre o depósito do veículo;

Não deposite em conta de pessoa física e, mesmo que seja jurídica, mantenha cautela.

FOI VÍTIMA DESTE GOLPE? VEJA O QUE FAZER

Registre boletim de ocorrência e informe:

- **Descrição do fato;**
- **Prejuízos causados;**
- **Site utilizado com a url e outros dados identificadores;**
- **Se possuir informações de registro e hospedagem do domínio, acrescente;**
- **Contas bancárias ou chaves pix informadas;**
- **Telefone de contato, email, redes sociais e mensageria do infrator**
- **Endereços encontrados.**

Informe à instituição financeira que a conta do infrator é utilizada para prática de fraudes:

- **Fundamentação Legal- Lei Complementar 105/2001, art. 1º, § 3º,inc. IV;**
- **Envie cópia do boletim de ocorrência.**

Denuncie o site falso de leilão para posterior remoção.

GOLPE DO INTERMEDIÁRIO NA VENDA DE VEÍCULO EM PLATAFORMAS DE COMÉRCIO ELETRÔNICO

Objetivo:

Enganar vendedor e comprador na venda de veículo em plataformas de comércio eletrônico.

MODUS OPERANDI

O estelionatário encontra uma oferta de venda de anúncio de um veículo em plataforma de comércio eletrônico;

Detalhe do golpe: o fraudador nunca aparece fisicamente durante a negociação;

Passo seguinte entra em contato com o vendedor do veículo e demonstra interesse na compra, todavia, alega que a negociação será para quitar dívidas com terceiros;

O fraudador pede sigilo absoluto na transação e solicita que a comprador dirija-se ao endereço do vendedor para ver o veículo;

Apresenta o vendedor como um parente e o comprador como aquele que vai quitar uma dívida, orientando-os a não falar sobre valores da transação;

O comprador faz um depósito para o fraudador, acreditando estar negociando com o proprietário. Neste ínterim, um comprovante falso é enviado ao vendedor;

O golpe só é descoberto quando os valores não são creditados;

O terceiro se recusa a fazer a transferência.

PROTEÇÃO

Evite negociar com intermediário. A transação deve ser realizada sempre entre vendedor e comprador;

Negocie apenas dentro da plataforma de comércio eletrônico e evite aplicativos de mensageria;

A transferência de valores só deve ser feita para o vendedor, nunca para terceiros;

Verifique com seu banco se os valores foram creditados antes de efetuar a transferência do veículo;

Desconfie de ofertas tentadoras.

FOI VÍTIMA DESTE GOLPE? VEJA O QUE FAZER

Registre boletim de ocorrência e informe:

- **Descrição do fato;**
- **Prejuízos causados;**
- **Conta bancária informada para depósito ou chaves pix;**
- **Contatos com o infrator (telefone, mensageria, email);**
- **Perfis na plataforma de comércio eletrônico (vítima e infrator);**
- **Telefone de contato, email, redes sociais e mensageria do infrator**

Informe à instituição financeira que a conta do infrator é utilizada para prática de fraudes:

- **Fundamentação Legal- Lei Complementar 105/2001, art. 1º, § 3º,inc. IV;**
- **Envie cópia do boletim de ocorrência.**

Denuncie na plataforma o perfil utilizado na prática do crime por violação aos termos de uso ou diretrizes da comunidade.

SITES FALSOS DE VENDA DE PRODUTOS ELETRÔNICOS

Objetivo:

Simular venda de produtos inexistentes a fim de obter vantagem ilícita com pagamento de pix.

MODUS OPERANDI

O fraudador hospeda um site falso com nome de lojas conhecidas de eletrônicos;

Por vezes, inclui informações de CNPJ e endereço da empresa verdadeira para dar uma maior credibilidade ao comprador;

Disponibiliza produtos com preços atrativos e super descontos com pagamento por pix;

O fraudador utiliza aplicativos de mensageria para intermediar a compra. Algumas vezes emprega bots para automatizar as respostas;

Após o pagamento, o fraudador encerra os contatos.

PROTEÇÃO

Faça compras em sites de estabelecimentos conhecidos;

Desconfie de preços baixos e sites recentemente criados;

Verifique se o site é seguro e procure por informações em plataformas de reclamação de consumidores e no Google;

Pague com cartão de crédito virtualizado e preferencialmente parcelado;

Evite transferências bancárias para contas de pessoa física;

Examine a reputação da empresa e procure o canal oficial para contato.

FOI VÍTIMA DESTE GOLPE? VEJA O QUE FAZER

Registre boletim de ocorrência e informe:

- **Descrição do fato;**
- **Prejuízos causados;**
- **Site utilizado com a url e outros dados identificadores;**
- **Se possuir informações de registro e hospedagem do domínio, acrescente;**
- **Contas bancárias ou chaves pix informadas;**
- **Telefone de contato, email, redes sociais e mensageria do infrator**

Informe à instituição financeira que a conta do infrator é utilizada para prática de fraudes:

- **Fundamentação Legal- Lei Complementar 105/2001, art. 1º, § 3º,inc. IV;**
- **Envie cópia do boletim de ocorrência.**

Denuncie o site falso na internet.

SITES FALSOS DE RESERVA DE ESTABELECIMENTOS DE HOTELARIA

Objetivo:

Obter depósito indevidos por reservas falsas em estabelecimentos de hotelaria

MODUS OPERANDI

Ocorre o registro e a hospedagem do site com o nome semelhante ao estabelecimento de hotelaria (typosquatting);

O criminoso, por vezes, faz um clone da página verdadeira para dar maior credibilidade;

Quando o usuário acessa a página e demonstra interesse na reserva, recebe excelentes descontos;

Após isto, é redirecionado para o WhatsApp e o infrator solicita o pagamento em conta de pessoa física;

Muitas vezes a vítima só toma conhecimento do golpe quando chega no estabelecimento para se hospedar.

PROTEÇÃO

Faça reservas apenas nos canais oficiais do estabelecimento;

Execute um whois no site para obter dados de registro, hospedagem, período e pessoa responsável;

Verifique no Google se há reclamações sobre o site do hotel;

Nunca mande depósitos para pessoa física;

As reservas devem ser realizadas apenas com cartões de crédito. Em caso de fraude você poderá fazer o estorno;

FOI VÍTIMA DESTE GOLPE? VEJA O QUE FAZER

Registre boletim de ocorrência e informe:

- **Descrição do fato;**
- **Prejuízos causados;**
- **Site utilizado com a url e outros dados identificadores;**
- **Se possuir informações de registro e hospedagem do domínio, acrescente;**
- **Contas bancárias ou chaves pix informadas**
- **Telefone de contato, email, redes sociais e mensageria do infrator.**

Informe à instituição financeira que a conta do infrator é utilizada para prática de fraudes:

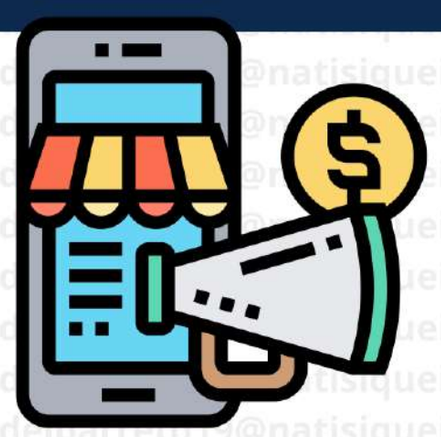
- **Fundamentação Legal- Lei Complementar 105/2001, art. 1º, § 3º,inc. IV;**
- **Envie cópia do boletim de ocorrência;**

Denuncie na rede social o perfil utilizado na prática do crime por violação aos termos de uso ou diretrizes da comunidade.

GOLPE PARA RECEBIMENTO DE PRODUTO - ENGENHARIA SOCIAL NO MERCADO LIVRE E OLX

Objetivo:

Enganar a vítima com informações falsas de pagamento para recebimento do produto.



MODUS OPERANDI

O criminoso entra em contato com o vendedor do produto na plataforma de comércio eletrônico;

Envia uma mensagem no WhatsApp e pede que a negociação seja realizada através do Mercado Livre;

Alega, para tanto, que esta forma de negociação assegura confiança e confidencialidade da transação;

O vendedor recebe um email fraudulento de confirmação do pagamento;

O fraudador solicita que a mercadoria seja entregue a um motoboy ou enviada pelos correios;

O golpe, por vezes, só é descoberto dias após a entrega da mercadoria.

PROTEÇÃO

Realize a negociação apenas pela plataforma de comércio eletrônico. Nunca faça através de aplicativo de mensageria;

Antes de remeter qualquer produto, verifique o status na plataforma;

Examine se o email enviado provém de fonte confiável;

Só forneça os dados de contato após a confirmação da compra;

Denuncie esses perfis fraudulentos no Mercado Livre e OLX.

FOI VÍTIMA DESTE GOLPE? VEJA O QUE FAZER

Registre boletim de ocorrência e informe:

- **Descrição do fato;**
- **Prejuízos causados;**
- **Informações do fraudador:**

  *** Perfil na plataforma de comércio eletrônico;**

  *** Email, telefone e WhatsApp;**

  *** Contas bancárias ou chaves pix informadas.**

Informe à instituição financeira que a conta do infrator é utilizada para prática de fraudes:

- **Fundamentação Legal- Lei Complementar 105/2001, art. 1º, § 3º,inc. IV;**
- **Envie cópia do boletim de ocorrência.**

BOLETOS

COBRANÇA INDEVIDA DE CONTAS DE TELEFONE E INTERNET

Objetivo:

Enganar a vítima para que ela pague uma conta em nome de terceiro.

MODUS OPERANDI

O usuário recebe cobranças por email de faturas vencidas com ameaças de suspensão do plano (engenharia social do medo);

Para dar credibilidade, o infrator envia boletos personalizados da empresa, todavia, o código de barras é diferente;

Ao fazer o pagamento, a vítima quitou, de fato, um boleto em nome de terceiro.

PAGAMENTOS DE BOLETOS POR CONSULTA EM MECANISMOS DE BUSCA E REDIRECIONAMENTO PARA PÁGINA FALSA

Objetivo:

Receber o pagamento de valores indevidos com o impulsionamento de sites falsos em mecanismos de busca.

MODUS OPERANDI

O fraudador hospeda um site falso de pagamento de plano de saúde, conta de telefone ou financiamento de um veículo;

Faz o impulsionamento do site em mecanismos de busca a fim de que ele fique bem rankeado, ou seja, toda vez que alguém procurar sobre aquele assunto, o site falso será mostrado como uma das primeiras opções. Impulsiona, ainda, por palavras-chave: quitar dívida, pagar boleto;

O usuário utiliza mecanismos de busca para localizar o site de pagamento e é redirecionado para um atendimento no WhatsApp web;

O golpista solicita informações sobre débitos pendentes e oferta um excelente desconto para quitação;

Os boletos são emitidos com o logo da empresa, todavia, o código de barras direciona o pagamento para usuário distinto.

BOLWARE

Objetivo:

Instalar malware no dispositivo informático da vítima para alteração do código de barras do boleto com redirecionamento para beneficiário distinto.

MODUS OPERANDI

Criminoso instala software malicioso no computador da vítima;

Após o usuário gerar um boleto, ocorre a alteração da linha digitável;

O pagamento é direcionado para um terceiro e não para o usuário;

O golpista solicita informações sobre débitos pendentes e oferta um excelente desconto para quitação;

A vítima só toma conhecimento do golpe quando ocorre a cobrança do débito ou a negativação em serviços de proteção do consumidor;

PROTEÇÃO

Antes de finalizar o pagamento, o usuário deve observar todas as informações contidas no boleto, dentre as quais:

- **A linha digitável deve conter agência, código cedente e número, independentemente do banco emissor;**
- **O número do banco e os 03 primeiros caracteres da linha digitável devem ser iguais;**
- **Verifique, antes de confirmar o pagamento, se o beneficiário e os valores são os mesmos do boleto;**

Desconfie quando você recebe boletos não solicitados;

Fique atento com mensagens por email que contenham engenharia social do medo: "pague o quanto antes sob pena de suspensão do serviço";

Dê preferência ao pagamento com leitura automática do código de barras;

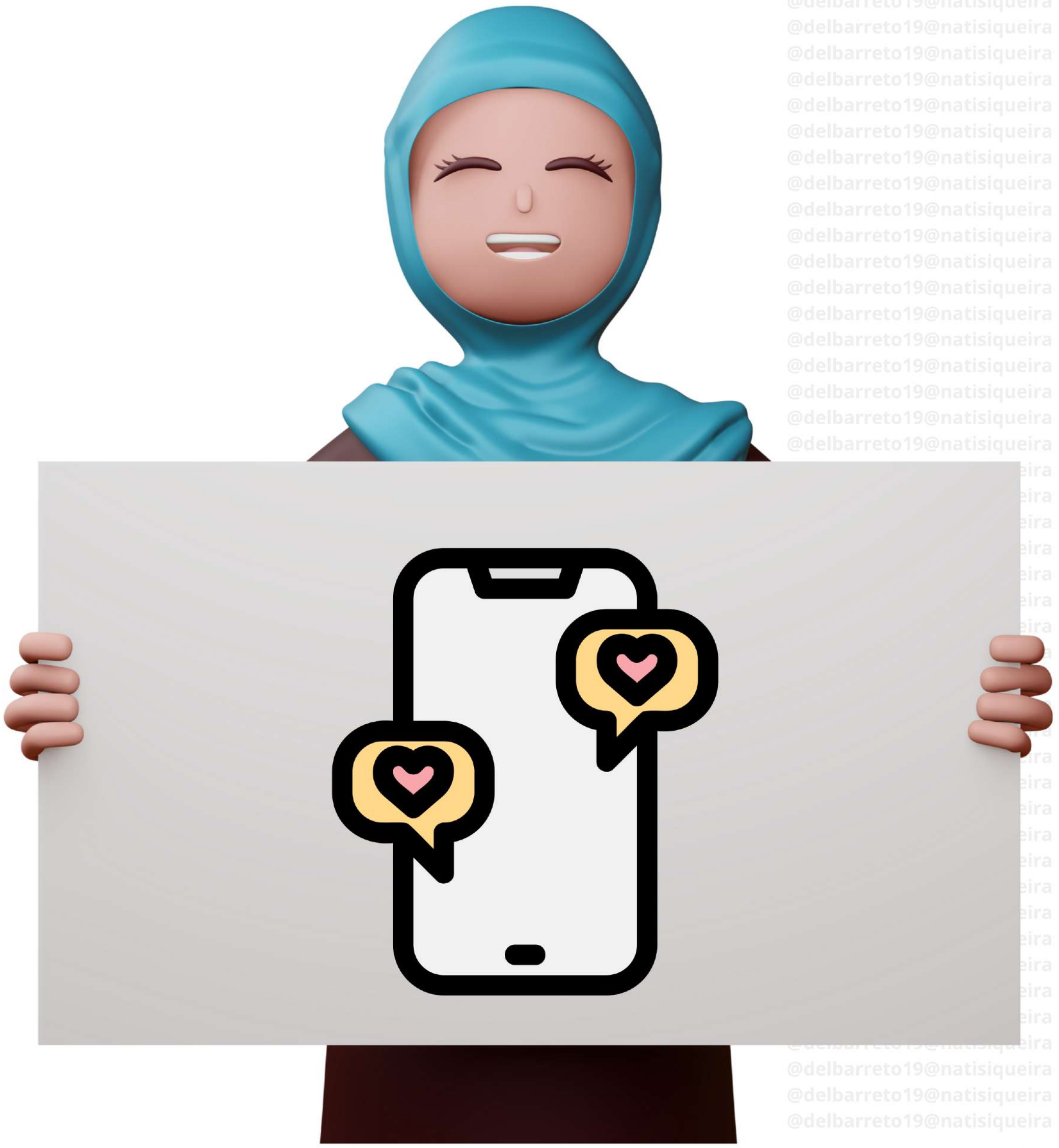
Mantenha o sistema operacional atualizado e utilize antivírus pago.

FOI VÍTIMA DESTE GOLPE? VEJA O QUE FAZER

Registre boletim de ocorrência e informe:

- **Descrição do fato;**
- **Prejuízos causados;**
- **Informações do beneficiário e da instituição;**
- **Modus Operandi do Boleto Falso;**
  - *** Email;**
  - *** Mensageria;**
  - *** Bolware;**
- **Outras informações relacionadas.**

AMOR, INTERNET E GOLPES RELACIONADOS



SEXTORSÃO

Objetivo:

Convencer usuários a compartilhar conteúdo íntimo e exigir o pagamento de valores por pix ou criptoativos.

MODUS OPERANDI

Em regra, as principais vítimas são homens e a abordagem inicial é realizada através de redes sociais ou aplicativos de mensageria;

Os criminosos criam perfis de garotas novas e atraentes em busca de interessados. Após o primeiro contato, a conversa evolui rapidamente para o exibicionismo em webcams.

Em algumas situações, o infrator utiliza softwares simuladores de streaming de vídeo para dar maior credibilidade;

De posse do conteúdo íntimo, a extorsão é iniciada com a exigência do pagamento em pix ou criptoativos. O criminoso ameaça divulgar as imagens e vídeos íntimos caso não haja o pagamento dos valores;

Para as mulheres, a engenharia social é de trabalho, empresários de modelos ou personalidades;

Organizações criminosas do continente africano se especializaram nesta modalidade delitiva.

PROTEÇÃO

Nunca compartilhe conteúdo íntimo;

Desconfie sempre de bate-papos que direcionam rapidamente para intimidades;

Amigos reais são diferentes dos virtuais. Antes de adicionar alguém, verifique antes;

Evite fazer streaming ou compartilhar conteúdo com desconhecidos;

Utilize adesivos para acobertar webcams;

Oculte informações pessoalmente identificáveis;

Foi vítima? Procure a polícia.

FOI VÍTIMA DESTE GOLPE? VEJA O QUE FAZER

Registre boletim de ocorrência e informe:

- **Descrição do fato;**
- **Prejuízos causados;**
- **Dados individualizadores autor;**
  *** Rede Social;**
  *** Email;**
  *** Telefone;**
  *** Mensageria.**
- **Contas bancárias, carteiras e chaves pix informadas.**

Informe à instituição financeira que a conta do infrator é utilizada para prática de fraudes:

- **Fundamentação Legal- Lei Complementar 105/2001, art. 1º, § 3º,inc. IV;**
- **Envie cópia do boletim de ocorrência.**

Denuncie na rede social o perfil utilizado na prática do crime por violação aos termos de uso ou diretrizes da comunidade.

LOVE SCAMMERS

Objetivo:

Iniciar romances com mulheres em sites de relacionamento com o intuito de obter vantagem indevida

MODUS OPERANDI

A vítima é abordada em sites de relacionamento ou redes sociais. Normalmente, mulheres divorciadas ou viúvas são os principais alvos;

Os criminosos criam perfis fakes e assumem a identidade de pessoas reais. Médicos, engenheiros, militares bem sucedidos no exterior são os favoritos;

Preferem, sempre, conversar por email e aplicativos de mensageria. Nunca fazem chamadas de vídeo e alegam, para isso, não ser permitido no local de trabalho ou telefone com defeito;

Enviam presentes para as vítimas para ganhar a confiança e solicitar pequenos empréstimos. Os valores são crescentes e sempre devolvidos;

Por fim, alegam problemas de saúde na família e pedem uma quantia elevada que nunca mais será devolvida. Excluem, então, os perfis e não mantêm mais contato com a vítima.

PROTEÇÃO

Nunca compartilhe conteúdo íntimo;

Oculte suas informações pessoalmente identificáveis nas redes sociais;

Não envie dinheiro quando solicitado por contato telefônico ou mensagem, por mais triste que seja a estória, desconfie;

Começou um relacionamento online? Pesquisa sobre o perfil, contatos e informações pessoais;

Procure no Google imagens semelhantes daquelas postadas pelo seu contato;

Quando o contato te direciona logo para WhatsApp, fique atento;

Fraudadores sempre alegam problemas na webcam ou smartphone quebrado. Procure fazer videochamadas para certificar a identidade do seu perfil;

Atenção por encontros cancelados por diversas vezes;

Avise aos seus familiares. Criminosos sempre solicitam que as vítimas não mencionem o relacionamento.

FOI VÍTIMA DESTE GOLPE? VEJA O QUE FAZER

Registre boletim de ocorrência e informe:

- **Descrição do fato;**
- **Prejuízos causados;**
- **Dados individualizadores autor;**
  - *** Rede Social;**
  - *** Sites de relacionamento**
  - *** Mensageria utilizada;**
  - *** URL, ID ou username;**
- **Contas bancárias, carteiras e chaves pix informadas.**

Informe à instituição financeira que a conta do infrator é utilizada para prática de fraudes:

- **Fundamentação Legal- Lei Complementar 105/2001, art. 1º, § 3º,inc. IV;**
- **Envie cópia do boletim de ocorrência.**

Denuncie na rede social o perfil utilizado na prática do crime por violação aos termos de uso ou diretrizes da comunidade.

GOLPE DA NOVINHA

Objetivo:

Extorquir homens com perfis de garotas jovens através de redes sociais.

MODUS OPERANDI

Criminosos criam perfis com garotas atraentes em redes sociais. Iniciam uma conversa com homens e demonstram interesse em relacionamento afetivo;

Após adquirir confiança, solicitam o WhatsApp e imagens sensuais de uma jovem são compartilhadas;

Quando o usuário repassa imagens íntimas, a extorsão inicia por um suposto familiar daquela garota do perfil;

Um teatro é montado para dar maior credibilidade e impor medo à vítima: parentes, advogado e até uma falsa delegacia;

Há ameaça de prisão e divulgação do conteúdo íntimo em redes sociais. Contas de laranja são utilizadas para o recebimento de valores.

PROTEÇÃO

Nunca compartilhe conteúdo íntimo;

Desconfie de perfis desconhecidos e com fotos atrativas adicionados e intimidades via direct;

Recebeu qualquer contato neste sentido, denuncie na plataforma e bloqueie da sua lista;

Ocorrida a extorsão, avise aos familiares e amigos próximos;

Foi vítima? Procure a polícia.

FOI VÍTIMA DESTE GOLPE? VEJA O QUE FAZER

Registre boletim de ocorrência e informe:

- **Descrição do fato;**
- **Prejuízos causados;**
- **Dados individualizadores autor;**
- **Contas bancárias, carteiras e chaves pix informadas;**
- **Redes sociais, mensageria, email e telefones.**

Informe à instituição financeira que a conta do infrator é utilizada para prática de fraudes:

- **Fundamentação Legal- Lei Complementar 105/2001, art. 1º, § 3º,inc. IV;**
- **Envie cópia do boletim de ocorrência.**

Denuncie na rede social o perfil utilizado na prática do crime por violação aos termos de uso ou diretrizes da comunidade.

GOLPE DO PEDÓFILO

Objetivo:

Praticar extorsão sob a acusação de crime de abuso e exploração sexual infantil com o intuito de obter vantagem ilícita.

MODUS OPERANDI

Inicialmente ocorre a criação de perfis falsos de policiais no WhatsApp para interação com homens;

Há o envio de mensagens avisando sobre uma investigação de "pedofilia" e mandado de prisão em aberto;

O falso policial solicita valores para não dar cumprimento da ordem judicial. Avisa que estava monitorando os acessos da vítima na internet. Por vezes, faz chamadas de vídeos em delegacias fakes;

Contas bancárias de terceiros são utilizadas para o recebimento de valores. Homens são as principais vítimas desta modalidade criminosa.

PROTEÇÃO

Desconsidere as mensagens que exijam valores para não divulgar conteúdo;

Bloqueie no WhatsApp e nas redes sociais qualquer tipo de contato por número ou perfil;

Está sendo extorquido? Avise aos amigos e familiares;

Denuncie no WhatsApp e nas redes sociais os perfis dos criminosos;

Foi vítima? Procure a polícia.

FOI VÍTIMA DESTE GOLPE? VEJA O QUE FAZER

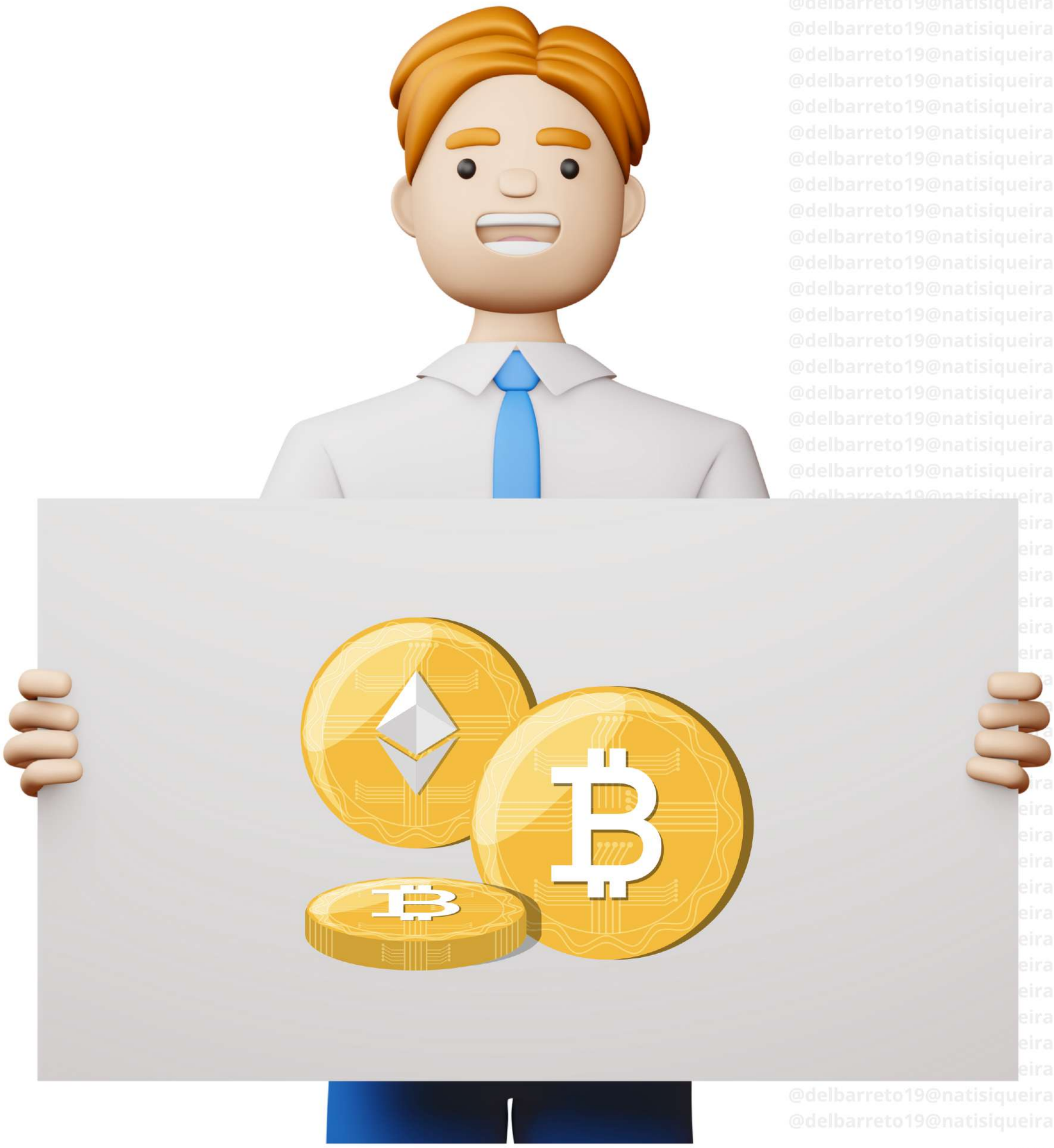
Registre boletim de ocorrência e informe:

- **Descrição do fato;**
- **Prejuízos causados;**
- **Dados individualizadores autor;**
- **Contas bancárias, carteiras e chaves pix informadas;**
- **Redes sociais, mensageria, email e telefones.**

Informe à instituição financeira que a conta do infrator é utilizada para prática de fraudes:

- **Fundamentação Legal- Lei Complementar 105/2001, art. 1º, § 3º,inc. IV;**
- **Envie cópia do boletim de ocorrência.**

CRIPTOMOEDAS



PIRÂMIDE

Objetivo:

Obter quantias consideráveis de investidores sob o argumento de altas taxas de retorno financeiro.

MODUS OPERANDI

O intermediário procura investidores interessados no mercado de criptomoedas e promete altas taxas de retorno e não detalha os riscos de investimentos;

Com os primeiros pagamentos, o investidor termina por fazer mais aportes e convocar familiares e amigos a participar do negócio;

Os fraudadores chegam a investir milhares de reais em propaganda para chamar outros interessados;

Em determinado momento, a estrutura montada não consegue mais pagar os valores prometidos, deixando milhares de pessoas no prejuízo.

PROTEÇÃO

Ofertas tentadoras e garantia certa de lucros rapidamente: é golpe;

Atenção para recrutamento de terceiros com promessa de mais lucros e condição de rentabilidade;

Os investimentos não são claros, apenas existe a promessa de lucro, tendência de fraude.

FOI VÍTIMA DESTE GgolpE? VEJA O QUE FAZER

Registre boletim de ocorrência e informe:

- **Descrição do problema, com valores aportados e prejuízos;**
- **Pessoas envolvidas;**
- **Contas bancárias, chaves pix, telefone, email, redes sociais e outros contatos com intermediário;**
- **Preserve as conversas em mensageria e email, posteriormente podem ser solicitadas.**

PERFIS FALSOS EM REDES SOCIAIS E INVESTIDORES DESATENTOS

Objetivo:

Criação de perfis falsos com intuito de atrair investidores a transferir valores indevidamente.

MODUS OPERANDI

O fraudador cria perfis falsos de exchanges, empresas ou investidores conhecidos em redes sociais;

Utiliza as imagens do perfil verdadeiro no feed e oferece excelente retorno para o investimento;

Após adquirir confiança, o criminoso informa um endereço diverso para o recebimento de criptomoedas ou conta para transferência pix;

O golpe encerra quando a vítima faz a transferência.

PROTEÇÃO

Desconfie de retornos rápidos e ofertas tentadoras;

Observe o engajamento daquele perfil nas redes sociais;

Cuidado com engenharia social para comprar a moeda ou token de forma imediata;

Verifique a reputação do vendedor e procure outras informações em mecanismos de busca;

É muito bom para ser verdade? Caia fora.

FOI VÍTIMA DESTE GOLPE? VEJA O QUE FAZER

Registre boletim de ocorrência e informe:

- **Rede social com individualizador (email, telefone, ID ou username);**
- **Contas e chaves pix de depósito;**
- **Redes socias e números de telefone;**
- **Modus operandi;**

Denuncie na rede social o perfil utilizado na prática do crime por violação aos termos de uso ou diretrizes da comunidade.

SITES FALSO OU SCAM PARA A VÍTIMA CONECTAR A WALLET

Objetivo:

Subtrair valores de investidores em criptoativos.

MODUS OPERANDI

O fraudador hospeda sites maliciosos com aparência de legítimos para enganar os investidores;

Impulsiona o serviço para que ele apareça no topo dos resultados de mecanismos de busca;

Quando a vítima utiliza um buscador, é direcionada para o site falso e, ao colocar os dados da carteira, terá seus valores subtraídos.

PROTEÇÃO

Verifique se a URL é legítima ou há erros de digitação;

Consulte um serviço de whois e obtenha informações de registro, hospedagem e data de criação do site;

Observe o endereço de toda e qualquer transferência que você vai realizar;

Examine a reputação do site e reclamações existentes em mecanismos de busca;

Proteja sua carteira.

FOI VÍTIMA DESTE GOLPE? VEJA O QUE FAZER

Registre boletim de ocorrência e informe:

- **O domínio falso com a respectiva URL;**
- **Prejuízos ocorridos;**
- **Se houver transferência, informar os endereços (chaves, pix, carteiras, etc.)**
- **Endereços de email, telefone de contato, redes sociais e todas as informações que possuir do autor;**

Procure o canal de denúncia para reportar o site falso.

APLICATIVOS FALSOS

Objetivo:

Criação de aplicativos falsos para o recebimento de criptoativos.

Aplicativos falsos de exchanges conhecidas são desenvolvidos e disponibilizados através de lojas oficiais;

Para atrair usuários, criminosos criam perfis em redes sociais e colocam o link para baixar o app;

Pensando se tratar de app oficial, o usuário faz o download e cadastra na plataforma;

Os endereços informados para a transferência de criptoativos pertencem aos invasores;

Quando o volume investido é considerável, ocorre o saque e o investidor fica com o prejuízo.

PROTEÇÃO

Baixe os aplicativos necessários e apenas de lojas oficiais;

Jamais faça download por meio de links de email, redes sociais ou encontrados no Google;

Mesmo que o app tenha sido baixado em loja oficial, verifique:

- **Informações do desenvolvedor;**
- **Quantidade de downloads;**
- **Observar a data das avaliações e o tempo que o app está disponível;**
- **Eventuais erros encontrados;**
- **Google.**

Mantenha o app sempre atualizado e fique atento às permissões desnecessárias.

FOI VÍTIMA DESTE GOLPE? VEJA O QUE FAZER

Registre boletim de ocorrência e informe:

- **Dia e hora que ocorreu o fato com a descrição do problema;**
- **Modus operandi;**
- **Como fez o download do aplicativo: email, links em mensageria, indicação em rede social;**
- **Individualização do app (URL, desenvolvedor, quantidade de downloads)**
- **Prejuízos financeiros;**

Denuncie na loja oficial o app falso empregado na prática do crime por violação aos termos de uso ou diretrizes da comunidade.

LANÇAMENTO DE CRIPTOATIVOS INOVADORES

Objetivo:

Lançamento de um crypto ativo inovador para atrair investidores e obter vantagem indevida.

MODUS OPERANDI

Os fraudadores fazem uma oferta inicial da moeda(ICO) com promessas de lucros exorbitantes;

Após a captação de somas consideráveis, os desenvolvedores retiram os valores e deixam os investidores no prejuízo.

PROTEÇÃO

Leia o contrato e pesquise sobre os desenvolvedores em fontes abertas;

Antes de comprar qualquer crypto ou token, procure bastante em sites especializados na matéria;

Tem alguma dúvida sobre a aquisição, busque informações com investidores experientes;

Cuidado com engenharia social e promessas de lucros exorbitantes em prazo curto;

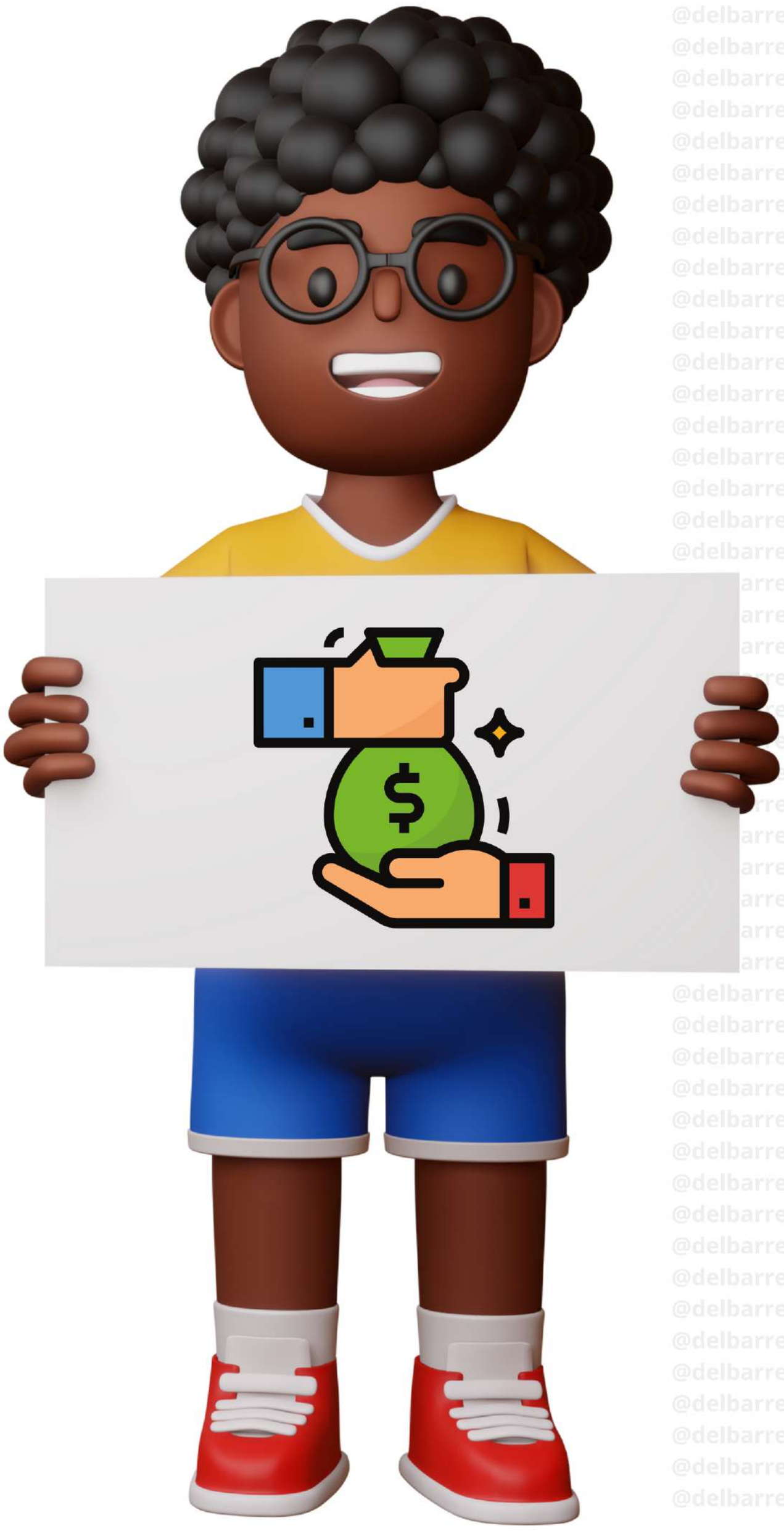
Mantenha sua carteira segura.

FOI VÍTIMA DESTE GOLPE? VEJA O QUE FAZER

Registre boletim de ocorrência e informe:

- **Descrição do fato;**
- **Prejuízos causados;**
- **Dados individualizadores do fato, projeto e autor;**
- **Redes sociais, mensageria, email e telefones.**

OUTROS GOLPES



FALSO EMPREGO EM PLATAFORMAS DE COMÉRCIO

Objetivo:

Obter vantagem ilícita com depósitos para garantir emprego ou pagamento de taxas de cursos inexistentes.

MODUS OPERANDI

Criminoso cria perfis falsos para anunciar vagas falsas de emprego nas plataformas de comércio eletrônico;

Chega até mesmo a pagar para anunciar em perfis com um bom engajamento;

Solicitam cópias de RG, CPF e comprovante de residência para realizar o cadastro;

O interessado é avisado que foi selecionado, todavia necessita adiantar valores como taxa ou pagar a inscrição em um curso como pré-requisito;

Após o recebimento dos valores, o estelionatário bloqueia a vítima e os contatos são suspensos.

PROTEÇÃO

Desconfie de anúncios de emprego em redes sociais ou sites desconhecidos. Procure as informações no canal oficial da empresa;

A oferta de emprego é genérica, caia fora;

Houve solicitação de valores antecipados para cadastro ou pagamento de curso como condição de assegurar a vaga? Não faça;

Busque pela oferta do emprego apenas nos canais oficiais do estabelecimento;

Nunca forneça informações pessoalmente identificáveis por email, telefone ou mensageria;

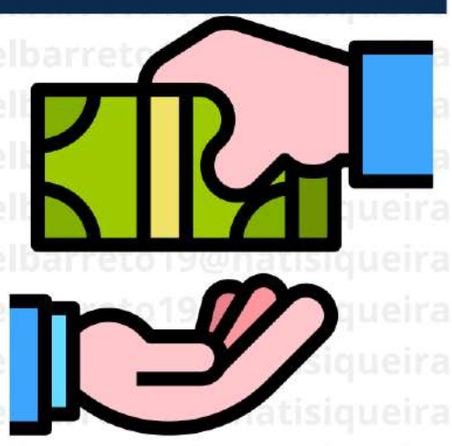
FOI VÍTIMA DESTE GOLPE? VEJA O QUE FAZER

Registre boletim de ocorrência e informe:

- **Descrição do fato;**
- **Prejuízos causados;**
- **Dados individualizadores do autor;**
- **Contas bancárias e chaves pix informadas;**
- **Redes sociais, mensageria, email e telefones**
- **Sites e redes sociais com os respectivos individualizadores (url, perfil, etc);**

Denuncie na plataforma o perfil utilizado na prática do crime por violação aos termos de uso ou diretrizes da comunidade.

GOLPE DO EMPRÉSTIMO



Objetivo:

Obter valores antecipados das vítimas para liberação dos valores desejados ou adquirir os dados pessoais para praticar outros golpes.

MODUS OPERANDI

O infrator oferta empréstimos sem consulta de crédito e em condições extremamente vantajosas através de redes sociais e publicidades em sites;

Após o convencimento do cliente, ocorre a solicitação de um adiantamento de valores para pagamento de taxas;

São solicitadas informações pessoais e financeiras do interessado;

Após o pagamento, o estelionatário disse que há necessidade de efetuar outro pagamento;

A vítima chega a enviar uma quantia considerável até ser bloqueada pelo criminoso.

PROTEÇÃO

Desconfie de ofertas atraentes de empréstimo sem consulta de crédito;

Procure estabelecimentos conhecidos e, preferencialmente, faça o empréstimo em lojas físicas;

Jamais deposite valores adiantados sob o pretexto de pagamento de taxas;

Não transfira ou receba valores de contas de pessoa física;

Não forneça informações pessoais ou financeiras. Seus documentos podem ser utilizados em outros golpes.

Procure informações da financeira em mecanismos de busca e sites de reclamação de serviços;

Está muito bom para ser verdade? Caia fora, é golpe.

FOI VÍTIMA DESTE GOLPE? VEJA O QUE FAZER

Registre boletim de ocorrência e informe:

- **Descrição do fato;**
- **Prejuízos causados;**
- **Dados individualizadores do autor;**
- **Contas bancárias e chaves pix informadas;**
- **Redes sociais, mensageria, email e telefones**
- **Sites e redes sociais com os respectivos individualizadores (url, perfil, etc);**

Denuncie na plataforma o perfil utilizado na prática do crime por violação aos termos de uso ou diretrizes da comunidade.

FALSA AGÊNCIA DE MODELO

1

Objetivo:

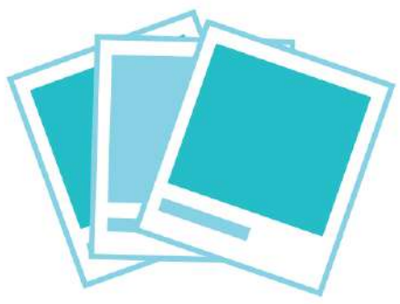
Obter vantagem indevida sob o pretexto de realizar ensaios fotográficos.

MODUS OPERANDI

Os fraudadores alugam salas comercias e colocam anúncios em redes sociais na busca de modelos;

Há promessas de empregos ou de contratos publicitários;

Solicitam o pagamento de valores para a realização de books e divulgação com empresas interessadas;



Após o recebimento desaparecem ou entregam fotos de péssima qualidade

PROTEÇÃO

Desconfie de ofertas de emprego sem detalhamento das atividades;

Busque no Google e nas redes sociais informações sobre a empresa;

Atenção para a exigência de valores antecipados como pré-requisito.

FOI VÍTIMA DESTE GOLPE? VEJA O QUE FAZER

Registre boletim de ocorrência e informe:

- **Descrição do fato;**
- **Prejuízos causados;**
- **Dados individualizadores do autor:**
  - *** Rede Social;**
  - *** Email;**
  - *** Telefone;**
  - *** Mensageria.**
- **Contas bancárias e chaves pix informadas;**
- **Escritórios utilizados com os respectivos endereços.**

FALSA AGÊNCIA DE MODELO

2

Objetivo:

Praticar golpes na internet com a obtenção de informações pessoais.

MODUS OPERANDI

Os golpistas criam perfis falsos de agentes de modelos em redes sociais;

Procuram perfis femininos e fazem comentários nas fotografias ou enviam mensagens por direct;

Convidam para trabalhar ou participar de uma seleção e remetem formulário para preenchimento de informações pessoais;

Os dados são utilizados para praticar golpes na internet.

GOLPE DA DOAÇÃO

Objetivo:

Obter vantagem indevida com o recebimento de valores de doação.

MODUS OPERANDI

O golpista, através de ligações telefônicas ou contas em redes sociais, solicita doações;

Para maior convencimento, utiliza nome de ONGs, fundações e creches, inclusive com páginas fakes no Instagram;

Os valores doados são depositados em "contas de laranjas" e sacados imediatamente.

PROTEÇÃO

Procure no Google e nas redes sociais informações sobre a instituição;

- **Páginas oficiais;**
- **Criação;**
- **Responsáveis;**
- **Engajamento nas mídias sociais.**

Quando for doar para instituições, nunca deposite em contas pessoa física;

Atenção contra engenharia social do medo.

FOI VÍTIMA DESTE GOLPE? VEJA O QUE FAZER

Registre boletim de ocorrência e informe:

- **Descrição do fato;**
- **Valores depositados;**
- **Modus operandi do fraudador;**
- **Site, email, telefone e redes sociais utilizadas no golpe.**

OFERTA DE EMPREGO
TRABALHE SEM SAIR DE CASA

Objetivo:

Obter vantagem indevida com o recebimento de transferências pix.

MODUS OPERANDI

O fraudador hospeda site e cria perfis em redes sociais de oferta de empregos;

As vagas oferecem salários tentadores e ainda a oportunidade de trabalhar em casa;

As mensagens são enviadas por SMS (número nacional e internacional) com link para WhatsApp;

Os fraudadores informam da contratação e necessidade de preenchimento doe cadastro com envio de documentos;

Algumas taxas são exigidas por pix. Posteriormente, exigem valores para que o 'contratado' possa liberar a comissão recebida.

PROTEÇÃO

Desconfie de ofertas tentadoras e mensagens inesperadas;

Procure informações sobre a empresa no Google e nos sites de reclamação de consumidores;

As oportunidades de emprego devem ser buscadas apenas nos canais oficiais da empresa;

Nunca mande valores antecipados para assegurar a contratação ou liberar uma comissão de venda.

FOI VÍTIMA DESTE GOLPE? VEJA O QUE FAZER

Registre boletim de ocorrência e informe:

- **Descrição do fato;**
- **Valores depositados;**
- **Modus operandi do fraudador;**
- **Site, email, telefone e redes sociais utilizadas no golpe;**
- **Contas bancárias ou chaves pix;**

ESSE CONTEÚDO TE AJUDOU?

SIGA-NOS NAS REDES SOCIAIS PARA SABER MAIS

@DELBARRETO19
@NATISIQUEIRA

DELEGADO BARRETO

ATÉ BREVE!