O GOLPE TÁ AÍ.

CAI QUEM NÃO SE INFORMA.

CARTILHA DE PREVENÇÃO CONTRA GOLPES.

POLÍCIA CIVIL DE SANTA CATARINA

O GOLPE TÁ AÍ.

CAI QUEM NÃO SE INFORMA.

CARTILHA DE PREVENÇÃO CONTRA GOLPES.

POLÍCIA CIVIL DE SANTA CATARINA

REALIZAÇÃO
Gerência de Planejamento e Avaliação - GEPLA

CONTEÚDO
Diretoria de Inteligência - DINT
Setor de Comunicação Visual - GEPLA/SECOV

DIAGRAMAÇÃO
Setor de Comunicação Visual - GEPLA/SECOV

Olá!

A PCSC apresenta esta cartilha que é um guia prático para ajudá-lo a manter-se protegido no vasto mundo on-line e off-line. Hoje em dia, a tecnologia nos conecta, nos informa e nos entretém de maneiras nunca antes imaginadas, mas, infelizmente, também expõe a possibilidade de sermos alvo de golpes e artimanhas virtuais. Este guia foi criado para capacitar você com o conhecimento necessário para identificar, prevenir e evitar quedas nas armadilhas que estão lá fora.

A cada avanço tecnológico, os golpistas encontram novas formas de explorar nossa confiança, curiosidade e, por vezes, até nossa ingenuidade. Acreditamos que a educação é a melhor defesa contra esses ataques. Portanto, convidamos você a explorar as páginas seguintes, onde abordaremos alguns dos golpes mais comuns e forneceremos orientações práticas para manter-se seguro em seu cotidiano, enquanto navega pela web, realiza transações online e interage nas redes sociais.

Lembre-se de que ao adquirir conhecimento sobre as táticas dos golpistas, você estará fortalecendo sua capacidade de discernir entre o genuíno e o enganoso. Com as informações certas e alguns passos simples, você estará pronto para enfrentar o mundo digital com mais confiança e cautela. Vamos começar a jornada rumo a uma experiência preventiva.

Boa leitura!

ORIENTAÇÕES GERAIS

Muitos bandidos, que são autores de estelionato, não se vestem mal, falam corretamente, tem o cabelo bem cortado e geralmente não usam armas. Podem estar atrás de uma tela de computador.

Sempre desconfie de situações em que a ESMOLA É DEMAIS.

Estamos em tempos difíceis financeiramente, ninguém está dando dinheiro facilmente.

Qualquer suspeita de que esteja sofrendo algum ataque de golpistas, procure uma delegacia de polícia, viatura policial ou ligue para: Polícia Militar/Polícia Civil".

É importante a vítima esclarecer todos os fatos na hora de fazer o Boletim de Ocorrência. Deve ser fornecidos todos os dados possíveis que envolvam o golpe, como o número que efetuou ligações, links enviados em SMS e dados de contas bancárias.

Em caso de ter sido efetuada alguma transferência solicitar ao banco os dados dos beneficiários, estabelecimentos em que foram efetuados pagamentos e os logs de acesso (IPs que acessaram a conta).

GLOSSÁRIO

Autenticação de dois fatores: Método de segurança que exige duas formas diferentes de comprovação de identidade antes de conceder acesso a uma conta ou sistema, aumentando a proteção ao exigir algo que o usuário sabe (senha) e algo que o usuário possui (como um código temporário enviado via SMS ou gerado por um aplicativo). Isso reduz os riscos associados a ataques cibernéticos.

Boletim de Ocorrência: É um documento oficial elaborado pelas autoridades policiais para registrar formalmente informações sobre um incidente, crime ou evento relevante, a fim de documentar os detalhes relevantes para fins legais e de investigação.

Criptomoeda: É uma forma de moeda digital baseada em criptografia que opera em uma rede descentralizada, como a blockchain. Ela permite transações seguras, anônimas e verificáveis pela tecnologia, eliminando a necessidade de intermediários, como bancos. Exemplos incluem Bitcoin, Ethereum e outras moedas virtuais.

Download: Ato de transferir dados, como arquivos, de um servidor ou origem online para um dispositivo local, como um computador ou dispositivo móvel, permitindo o acesso e uso offline.

E-mail: (eletronic mail) é um sistema de comunicação digital que permite o envio e recebimento de mensagens escritas, documentos e mídia entre pessoas por meio da internet.

Engenharia social: Técnica de manipulação usada para obter informações, acesso ou influência, explorando a confiança e interações humanas, geralmente com o objetivo de cometer fraudes, furto de dados ou ganhos ilícitos.

Extorsão: Crime no qual alguém obtém algo, como dinheiro, propriedade ou serviços, de outra pessoa por meio de ameaças, coerção ou intimidação.

Hackear: Refere-se ao ato de invadir ou comprometer sistemas de computador, redes ou contas digitais por indivíduos com conhecimento técnico avançado (hackers), muitas vezes com a intenção de obter acesso não autorizado, furtar informações ou causar danos.

Inteligência artificial: É a simulação de processos de raciocínio humano por meio de computadores, permitindo que máquinas realizem tarefas que normalmente exigiriam inteligência humana, como aprendizado, tomada de decisões e resolução de problemas.

Link: Conexão clicável que direciona de uma página da web para outra, permitindo a navegação entre diferentes recursos online, como sites, documentos ou mídia.

Log: É um registro detalhado de eventos, atividades ou informações que ocorrem em um sistema, aplicativo ou processo ao longo do tempo, frequentemente usado para monitoramento, análise e solução de problemas.

Nudes: Gíria que se refere a fotos ou vídeos de natureza sexualmente explícita, geralmente de natureza pessoal e íntima, compartilhados entre indivíduos. O termo é comumente usado no contexto das redes sociais e comunicações digitais.

Phishing: Forma de ataque cibernético em que os agressores se passam por entidades confiáveis por meio de mensagens falsas, como e-mails ou sites, para enganar as pessoas a revelarem informações pessoais, financeiras ou sensíveis. O objetivo é furtar dados ou induzir ações prejudiciais.

QR Code: (Quick Response Code) é um tipo de código de barras bidimensional que armazena informações, como URLs, textos ou outros dados, que podem ser lidos e interpretados rapidamente por dispositivos eletrônicos, como smartphones, usando a câmera para acessar o conteúdo associado.

Ransomware: Tipo de malware que infecta sistemas de computador e criptografa dados, bloqueando o acesso do usuário. Os cibercriminosos exigem um resgate em troca da chave de descriptografia, ameaçando tornar os dados inacessíveis ou publicá-los.

Redes sociais: São plataformas online que permitem que indivíduos e grupos interajam, compartilhem conteúdo e conectem-se digitalmente, facilitando a comunicação e o relacionamento entre pessoas de diferentes partes do mundo.

Selfie: Fotografia tirada por uma pessoa de si mesma, geralmente usando a câmera frontal de um dispositivo móvel, como um smartphone, para capturar a própria imagem.

Site: Conjunto de páginas da web relacionadas e acessíveis por meio da internet, que podem conter informações, mídia, serviços ou outros conteúdos interativos.

SMS: (Short Message Service) é um serviço de mensagens curtas que permite o envio e recebimento de mensagens de texto de tamanho limitado por meio de dispositivos móveis e comunicações celulares.

URL: (Uniform Resource Locator) é um endereço que identifica um recurso específico na internet, como uma página da web, permitindo que os navegadores localizem e acessem esse recurso.

Voucher: É um comprovante que confirma o direito a um serviço ou produto específico, muitas vezes usado como forma de pagamento ou para obter descontos.

ATENÇÃO!

GOLPES NAS PRÓXIMAS PÁGINAS

Nenhum golpista emitirá um alerta como esse antes de tentar te enganar.
Então é essencial conhecê-los para prevenir-se. Leia nas próximas páginas o conteúdo
que preparamos para você não se tornar uma vítima.

A informação é uma ótima forma de ficar protegido.

1

PERFIL FALSO NO WHATSAPP

Os criminosos vinculam uma imagem de perfil da vítima, geralmente retirada do seu próprio perfil de WhatsApp ou redes sociais, a um número de telefone que não pertence a ela.

Com uma conta falsa, eles se passam pela vítima e solicitam dinheiro para amigos, familiares e conhecidos.

ⓘ COMO PREVENIR?

Ajuste a visualização da imagem da conta do WhatsApp apenas para contatos autorizados;

Fique atento a mensagens de conhecidos ou familiares solicitando depósito e/ou transferências bancárias (ainda mais se for em nome de terceiros);

Desconfie de contas com fotos de conhecidos, mas com números diferentes.

⌖ O QUE FAZER?

Registrar um Boletim de Ocorrência e denunciar ao WhatsApp através do e-mail: support@whatsapp.com. Também é possível denunciar clicando no número do golpe, clicar no campo "Dados do contato" e clicar em "denunciar".

Avisar familiares e conhecidos, no caso de detectar que estão utilizando seu nome para aplicar o golpe.

Este golpe não se trata de clonagem de WhatsApp; a vítima não deixa de ter acesso ao seu aplicativo; os criminosos utilizam um número diferente, com a foto da vítima, para se passar por ela.

2

VOUCHER/ CUPOM DE DESCONTO EM RESTAURANTE

Os criminosos entram em contato via rede social utilizando um perfil falso de um estabelecimento comercial.

Afirmam que a vítima foi selecionada para participar de um sorteio e solicitam o número de WhatsApp.

Com o número, eles tentam habilitar o aplicativo em outro aparelho, por isso solicitam que a vítima encaminhe o código de seis dígitos para validar a participação na promoção.

O código recebido é de autenticação do WhatsApp da vítima, que terá o aplicativo clonado, caso passe o código recebido ao criminoso.

ⓘ COMO PREVENIR?

Nunca informe códigos recebidos por mensagem para ninguém e habilite a autenticação de dois fatores em sua conta;

Se receber mensagens sobre promoções, sempre ligue e confirme através de canais de comunicação oficiais do estabelecimento.

⌖ O QUE FAZER?

Registrar um Boletim de Ocorrência e denunciar ao WhatsApp através do e-mail: support@whatsapp.com. Também é possível denunciar clicando no número do golpe, clicar no campo "Dados do contato" e clicar em "denunciar".

Após o envio do e-mail, realize o procedimento para recuperação da conta sucessivas vezes, para bloquear a conta e o criminoso não conseguir mais utilizá-la.

POLÍCIA CIVIL DE SANTA CATARINA

3

PLATAFORMAS DE COMPRA/ VENDA ON-LINE

A vítima faz um anúncio em plataformas de compra/venda online e deixa o número de contato acessível ao público;

Os criminosos, em posse do número, passam-se pelo suporte da plataforma e pedem para que a vítima passe um código de validação recebido por mensagem;

O código recebido é de autenticação do WhatsApp da vítima, que terá o aplicativo clonado, caso passe o código recebido ao criminoso.

ⓘ COMO PREVENIR?

Nunca informe códigos recebidos por mensagem para ninguém e habilite a autenticação de dois fatores em sua conta.

Na dúvida, entre em contato através dos canais oficiais da plataforma.

⌖ O QUE FAZER?

Registrar um Boletim de Ocorrência e denunciar ao WhatsApp através do e-mail: support@whatsapp.com, também é possível denunciar clicando no número do golpe, clicar no campo "Dados do contato" e clicar em "denunciar".

Após o envio do e-mail, realize o procedimento para recuperação da conta sucessivas vezes, para bloquear a conta e o criminoso não conseguir mais utilizá-la.

4

FALSOS LINKS

Através de mensagens, os criminosos dizem que a vítima se enquadrou para o recebimento de alguma promoção, sorteio, auxílio emergencial, ou encaminham algum alerta dizendo que ocorreu uma operação indevida em sua conta.

Um link malicioso, então, é enviado para a vítima, sugerindo que ela acesse-o a fim de receber algum prêmio, benefício, ou até mesmo para evitar que sua conta seja bloqueada.

Ao acionar o link, a vítima é redirecionada para sites falsos de cadastros, ou baixa automaticamente aplicativos maliciosos no telefone, todos com objetivo de obter informações pessoais dela.

Fique atento nas suas buscas: Criminosos costumam pagar para seus falsos sites aparecerem nos primeiros resultados de uma busca, fazendo pequenas alterações no endereço (URL), mudando apenas uma letra, ou alterando o domínio (de *exemplo.com* para *exemp1o.com* > Veja que nesse exemplo de links foi alterado a letra “L” pelo número “1”).

ⓘ COMO PREVENIR?

Sempre desconfie de links encaminhados via WhatsApp ou SMS, e na dúvida, entre em contato direto com os canais oficiais de comunicação.

No caso de acionar o link ou realizar o cadastro em algum site, informe seu banco e leve seu telefone em alguma assistência para verificar a existência de aplicativos maliciosos.

Ao efetuar pesquisas em sites de buscas, observar se nos resultados a "escrita" está correta e corresponde ao esperado.

5

FALSO INTERMEDIADOR DE VENDAS

O criminoso consegue o telefone da vítima em sites de vendas on-line;

Ele copia o anúncio feito pela vítima e cria um novo anúncio falso, entretanto, com o valor mais baixo.

O golpista diz que comprará o bem anunciado e que pagará uma dívida que possui com algum cliente, sócio, amigo ou irmão, e, portanto, pede silêncio no momento de apresentar o objeto para a segunda vítima, prometendo algum lucro financeiro nesta negociação silenciosa.

A vítima interessada em comprar também é orientada a se manter em silêncio e por isso ganhará um desconto.

Com o enredo pronto, o criminoso fornece contas de terceiros para receber o pagamento.

Após recebido valor, o criminoso combina de assinar o recibo em cartório com ambas as vítimas, as quais descobrem que caíram em um golpe.

ⓘ COMO PREVENIR?

Mantenha sempre um diálogo aberto com o vendedor/comprador.

Faça questão de ver o bem pessoalmente marcando o encontro em um local público e movimentado e, se possível, vá acompanhado.

Busque outras formas de confirmar que realmente a pessoa que esta vendendo é a mesma que esta sendo feita a negociação.

Confirme se a conta informada pertence ao vendedor, ou algum familiar próximo (filho, esposa, pai, mãe, etc.).

Quando disponível, utilize os meios de pagamentos oferecidos pelas plataformas de venda.

Desconfie de bens com valores muito abaixo de suas tabelas. Geralmente, nesses casos, é golpe!

6

FALSO EMPRÉSTIMO

Os criminosos fazem anúncios em redes sociais se passando por instituições financeiras de crédito rápido com ofertas tentadoras.

Após contato da vítima, os criminosos solicitam o pagamento de uma taxa para a liberação do empréstimo.

São solicitados diversos pagamentos, até que vítima perceba que se trata de um golpe e pare de pagar.

ⓘ COMO PREVENIR?

Instituições financeiras nunca solicitam pagamentos prévios para a liberação de valores.

Sempre desconfie de ofertas imperdíveis, e na dúvida, procure os canais oficiais de comunicação da instituição.

GOLPE DO AMOR

Os golpistas buscam dados de suas vítimas em aplicativos de relacionamento e namoro.

O primeiro contato é feito pelo site de relacionamento e depois pelo WhatsApp.

Após iniciar conversas amorosas com fotos de uma pessoa fictícia, surgem as falsas declarações de amor e conversas sobre o desejo de se mudar para o Brasil e assim poder viver perto da vítima.

Na sequência, pedem o endereço residencial da vítima e depois afirmam que estão enviando uma caixa (muitas vezes mandam fotos) com jóias, numerários e outros itens. Dias após o suposto envio, um contato falso da Receita Federal (ou o próprio golpista) diz que a encomenda foi retida e para retirá-la, a vítima precisa fazer um depósito de um valor, que geralmente varia de R$ 2.500 a R$ 4.000.

Em alguns casos, o golpista afirma que tem um intermediário no envio da tal caixa e pede que todo o depósito ou parte dele seja feito no nome dessa pessoa.

Fazem ameaças à vítima e seus familiares caso não efetue o depósito.

COMO PREVENIR?

Nunca compartilhe fotos e vídeos íntimas através de mensagens.

O QUE FAZER?

Se for vítima de extorsão, procure a Delegacia de Polícia mais próxima.

Não deposite o valor solicitado.

FALSO SEQUESTRO

Os criminosos ligam para a vítima se passando por algum familiar. Com voz de choro, o suposto familiar diz que foi sequestrado e que os criminosos vão tirar a sua vida. A vítima, assustada, acaba informando o nome de familiares aos criminosos, informação utilizada por eles para dar mais autenticidade ao golpe.

Os criminosos solicitam o depósito de valores em algumas contas ou pedem que coloquem créditos em alguns números telefônicos.

Em algumas modalidades, os criminosos determinam que a vítima saia de casa, vá até um local reservado, que não alerte ninguém e que não entre em contato com seus familiares. Solicitam, então, o telefone de outra pessoa da família, para que esta consiga o dinheiro solicitado.

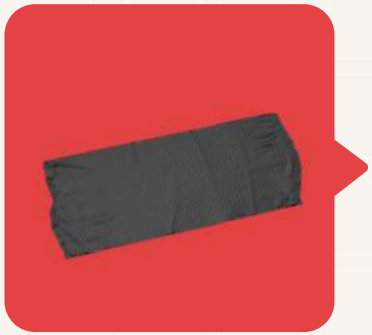
Em posse do telefone de outro familiar, o criminoso entra em contato, dizendo que sequestrou a vítima, esta, incomunicável e fora de casa, não consegue entrar em contato, deixando a impressão que realmente foi sequestrada.

O QUE FAZER?

No caso de receber alguma ligação deste tipo, desligue e tente entrar em contato com o familiar que supostamente foi sequestrado.

Na dúvida, solicite ajuda a alguém próximo para entrar em contato com o familiar; o nervosismo pode induzir a vítima a erro, alguém que não esteja sofrendo o golpe pode ajudar a localizá-lo e perceber que se trata de um golpe.

Caso não consiga entrar em contato com o familiar, procure em locais próximos, como shoppings, praças, bares e até mesmo hotéis, às vezes o familiar supostamente sequestrado também esta sendo induzido a erro.



GOLPE DO “NUDES” OU EXTORSÃO PELAS REDES SOCIAIS

Os golpistas estudam o perfil de suas vítimas através das redes sociais.

Geralmente as vítimas em potencial são homens (podendo também ser mulheres) de meia idade ou mais, casados e com círculo familiar, amigos ou profissional visível nas redes sociais.

O golpista utiliza um perfil falso, muitas vezes com a fotografia de uma jovem bonita e atraente. O contato inicial quase sempre ocorre através do Facebook onde eles começam uma amizade.

Logo a conversa privada passa para o WhatsApp onde a “moça” encaminha fotos íntimas suas e pede para que a vítima faça o mesmo. A partir dai, outro golpista entra em cena: o suposto pai ou padrasto da jovem, alegando que ela é “menor de idade” e que a vítima estaria praticando pedofilia através da internet. A partir daí, inicia-se a extorsão.

Para que o caso não seja levado à polícia, ou para que as fotos íntimas e as conversas privadas não sejam compartilhadas com a esposa, parentes ou amigos da vítima, o golpista exige que seja paga certa quantia em dinheiro por meio de depósito bancário.

Algumas vezes os golpistas também se fazem passar por supostos advogados, policiais civis ou delegados, alegando que as fotos já fazem parte de uma investigação policial e solicitam depósitos em dinheiro para que o “inquérito” seja arquivado. A vítima, temendo ser presa ou à exposição social, cede à extorsão e acaba fazendo o depósito dos valores solicitados pelos golpistas.

ⓘ COMO PREVENIR?

Nunca compartilhe fotos íntimas pela internet. Depois de compartilhada, a foto ou o vídeo podem circular entre milhares de pessoas.

Desconfie sempre de solicitações de amizade, através das redes sociais, de pessoas que você não conhece.

⌖ O QUE FAZER?

Caso você tenha sido vítima de algum destes golpes, procure imediatamente a Polícia Civil. Você também pode registrar o boletim de ocorrência através da Delegacia de Polícia Virtual de Santa Catarina, acessível em: delegaciavirtual.sc.gov.br

CLONAGEM DO WHATSAPP

Os criminosos possuem diversas formas de obter o número de telefone das vítimas, mas o mais usual é que seja retirado de anúncios em plataformas de sites de compras ou anúncios públicos em redes sociais.

O golpista se passa por funcionário da plataforma de anúncio e, sob o pretexto de corrigir uma duplicidade no anúncio com valores diferentes, ou mesmo ativar o anúncio, solicita à vítima que informe seus dados pessoais (nome, RG, CPF, endereço) e um código de 6 dígitos que receberá no telefone.

Esse código, na verdade, é uma verificação do WhatsApp, ou seja, a partir do fornecimento dessa chave o golpista desviará o WhatsApp da vítima para o aplicativo dele. Nesse caso a vítima perde o acesso ao aplicativo de mensagens.

A partir disso o criminoso se passa pela vítima e, alegando algum problema na conta ou com cartão de crédito bloqueado solicita dinheiro emprestado se comprometendo a pagar no dia seguinte. O parente ou amigo da vítima, acreditando estar falando com a pessoa de sua confiança, acaba transferindo o dinheiro para a conta bancária informada, e assim se torna também vítima do golpe.

ⓘ COMO PREVENIR?

Habilite a “confirmação em duas etapas” no aplicativo WhatsApp. Para isso, dentro do seu aplicativo clique em “configurações/ajustes” e depois clique em “conta”, escolha a opção “confirmação em duas etapas” e habilite a senha de 6 dígitos numéricos. Isso impede que golpistas façam a clonagem do WhatsApp. ***Esse código numérico é uma senha, portanto não envie para ninguém.***

Nunca informe códigos recebidos por mensagem para ninguém.

Caso você receba uma mensagem de algum amigo ou parente solicitando empréstimo em dinheiro, ou depósito de algum valor em uma determinada conta, verifique com cautela a veracidade desta solicitação. E, caso seja verdade, antes de qualquer confirmação de depósito, verifique o destinatário (nome, CPF, agência bancária).

⌖ O QUE FAZER?

Caso tenha enviado o código recebido por torpedo SMS e caído no golpe, encaminhe um e-mail para: support@whatsapp.com pedindo a desativação temporária de sua conta do WhatsApp.

Posteriormente, após receber o e-mail do WhatsApp no prazo de 30 dias, configure-o novamente com o seu número de celular.

BILHETE PREMIADO

A vítima, geralmente pessoa idosa, é abordada por uma pessoa com aparência humilde, que pede algumas informações, dizendo ter um bilhete de loteria premiado.

O criminoso, supostamente ganhador da loteria, alega ter medo de ser enganado na hora de resgatar o prêmio ou que tem ações na justiça que o impediriam de receber o prêmio.

Em seguida entra em cena um segundo golpista, um sujeito bem arrumado, que diz ter ouvido a conversa. A partir daí inicia-se a encenação, onde o segundo golpista simula falar com alguém da Caixa Econômica Federal para confirmar a legitimidade do prêmio.

Então, ele sugere que a vítima fique com o bilhete premiado, mas, em contrapartida, repasse algum dinheiro para o suposto ganhador. Geralmente eles acompanham a vítima até uma agência bancária para fazer o saque do dinheiro, ou a transferência como garantia de que o humilde suposto ganhador não seja enganado, e então entregam o bilhete premiado à vitima.

O QUE FAZER?

Caso se depare com alguém pedindo ajuda em situação semelhante, diga que não pode ajudar e procure uma Delegacia de Polícia mais próxima para informar o fato.

Saiba que não se ganha dinheiro fácil, principalmente em abordagens de rua por desconhecidos. Sempre desconfie!

PARENTE QUE TEVE O CARRO QUEBRADO

O golpista liga aleatoriamente para as vítimas, geralmente no período noturno.

Independentemente de quem atende o telefone, o golpista logo fala: “oi tio (a), ou oi primo (a), sabe quem está falando?”.

Caso a vítima diga um nome, achando ser algum sobrinho ou outro parente distante, já deu ao golpista o que ele queria.

Muitas vezes a vítima fala que não se recorda e então o golpista usa do artifício “nossa, não lembra mais de mim!”, dialogando com a vítima até que seja possível extrair dela um nome de um parente que mora distante.

Com isso, ele forja uma história de que estaria viajando ou chegando próximo à cidade onde a vítima reside, e relata que sofreu algum acidente ou que o carro dele quebrou. Então, o criminoso solicita que a vítima faça uma transferência em dinheiro para determinada conta bancária do mecânico, do guincho ou da borracharia onde o veículo está sendo consertado. Ele promete devolver o dinheiro no dia seguinte quando chegar à cidade da vítima.

COMO PREVENIR?

Não faça transferências ou entregue dinheiro para terceiros.

Desligue o telefone e faça contato com o familiar que você achava estar falando. Caso a pessoa esteja realmente em apuros, você ainda poderá ajudá-la.

DEPÓSITO COM ENVELOPE VAZIO

Geralmente a vítima fez algum tipo de anúncio para a venda de um determinado bem/objeto em sites de compras pela internet ou através de redes sociais.

Após a negociação, o golpista simula o depósito do valor acertado inserindo um envelope vazio no caixa eletrônico (ou na lotérica).

O golpista então encaminha uma fotografia do comprovante de depósito e a vítima confirma o recebimento em consulta à sua conta pelo aplicativo do banco. Como a verificação bancária do depósito demora algumas horas ou, às vezes, é feita apenas no próximo dia útil, o valor fica aparecendo como depositado até que se verifique que depósito não foi satisfeito. Assim, a vítima efetua a entrega do bem/objeto (normalmente o golpista manda um motorista de aplicativo para apanhar o objeto no mesmo dia do depósito).

ⓘ COMO PREVENIR?

Quando realizada uma negociação pela internet aguarde sempre a compensação do depósito bancário. Se possível, aguarde até o próximo dia útil para que haja a confirmação da entrada do dinheiro na conta. Isso vale para qualquer situação.

Verificar a data de criação do perfil do suposto comprador na plataforma de venda, em muitos casos a conta foi criada no mesmo dia ou no dia anterior ao contato com a vítima.

O GOLPE DO ENVELOPE VAZIO TAMBÉM É APLICADO DE OUTRAS FORMAS.

Geralmente, o golpista se passa por uma suposta autoridade pública ou servidor de algum órgão público. É um golpe bastante comum, por exemplo, na época das eleições. O golpista finge ser um servidor da justiça eleitoral ou promotor, requisitando os serviços de "motorista" de alguma instituição ou empresa, sob o pagamento de supostas diárias para a fiscalização de seções eleitorais nos municípios da região.

O depósito dos valores (diárias) é feito de forma antecipada diretamente na conta do "motorista", e o golpista envia a foto do comprovante. Logo em seguida, o golpista novamente entra em contato alegando que, por equívoco, efetuou o depósito de valor superior e necessita que seja imediatamente restituída a diferença por se tratar de verba pública.

Ocorre que a vítima confirma o recebimento em consulta à sua conta pelo aplicativo do banco. Como a verificação bancária do depósito demora algumas horas ou, às vezes, é feita apenas no próximo dia útil, o valor fica aparecendo como depositado até que se verifique que o depósito não foi satisfeito. Assim, a vítima acreditando se tratar de uma situação real, efetua a transferência do valor recebido a mais.

FALSA LIGAÇÃO DO BANCO

O golpista liga para a vítima como se fosse o banco no qual ela possui conta, fala que precisa liberar algumas chaves de acesso e passa um endereço de site supostamente do banco, para ela acessar.

Esse site é falso e redireciona a vítima para uma página semelhante à página oficial, mas que pertence ao golpista, o qual vai roubar todas as credenciais da vítima, como número da conta e senhas.

Após a vítima digitar os seus dados na página falsa e em posse dessas informações, o golpista transfere todo o dinheiro da conta da vítima para sua conta.

ⓘ COMO PREVENIR?

Nunca forneça dados pessoais ou realize atendimentos bancários de ligações recebidas no telefone. Caso seja urgente, ligue para o número do banco ou vá pessoalmente à agência.

Sabe-se que os bancos realmente ligam para seus clientes para confirmar transações suspeitas, contudo, nunca solicitam senhas, tokens, ou dados pessoais dos clientes. Deste modo, jamais fornecer informações bancárias ou pessoais para pessoas desconhecidas, e especialmente, nunca realizar transferências PIX ou qualquer outro tipo de pagamento para atendentes que se apresentam nos moldes citados.

É necessário, sempre que receber alguma ligação suspeita, desligar na hora e entrar em contato com a instituição pelos canais oficiais que ela possui, ou até mesmo através de aplicativos móveis. Jamais clicar em links recebidos via SMS ou WhatsApp, nem mesmo retornar ligação aos números indicados por esses meios.

RECUPERAÇÃO DO VEÍCULO FURTADO/ ROUBADO

A vítima tem o seu veículo (pode ser também um caminhão, trator ou outro bem) furtado ou roubado.

Com a expectativa de reaver o bem, ela faz anúncios públicos nas redes sociais ou em portais de notícias na internet, repassando informações detalhadas sobre o veículo que lhe foi subtraído.

Nesse momento entra em cena o golpista, que faz contato com a vítima solicitando o pagamento de uma determinada quantia em dinheiro através de depósito ou transferência bancária, para então devolver o bem ou fornecer informações sobre o seu paradeiro.

Depois que o pagamento é efetuado a vítima perde o contato com o golpista e se torna vítima pela segunda vez.

ⓘ COMO PREVENIR?

Independente da circunstância, evite pagar o resgate para reaver o seu bem.

FALSO BOLETO

O criminoso possui, mediante algum golpe aplicado anteriormente, informações sobre dados pessoais da vítima, de maneira que o recebimento do boleto torna-se muito convincente.

Este recebimento acontece ou via e-mail, páginas falsas que oferecem o download da fatura forjada, ou até mesmo via WhatsApp. O pagamento do boleto falso é feito para uma conta bancária vinculada ao golpista.

Como resultado, o credor do boleto original continua a efetuar cobranças, ou em casos de boletos provenientes de compras efetuadas, o produto não é enviado.

COMO PREVENIR?

Importante, nesses casos, sempre checar as informações existentes no boleto, especialmente, os dados do beneficiário e do pagador, CPF e/ou CNPJ, valor, data de vencimento e de emissão. Vale, ainda, verificar os três primeiros dígitos do código de barras do boleto, uma vez que eles correspondem ao banco emitente.

Outro tipo de golpe envolvendo Falso Boleto, ocorre com a vítima recebendo via Correios uma multa do Detran. Neste golpe os criminosos se posicionam em "passarelas" sobre vias rápidas e fotografam os veículos, pesquisam determinada placa em em bases abertas na Internet e com os dados do proprietário, emitem para seu endereço uma falsa multa.

LIGAÇÃO PARA ESTABELECIMENTOS

Nesta prática o golpista coleta dados de empresas reais, como telefone, endereço, fachada.

Esses dados são verificados, na grande maioria das vezes, em fontes abertas.

Em posse deles, o criminoso entra em contato com a empresa, alegando estar em frente ao estabelecimento e passando, inclusive, detalhes do local, afirmando que, caso não seja efetuado pagamento de determinado valor para alguma conta PIX, bandidos armados entrarão no local.

O QUE FAZER?

Ao receber ligações telefónicas suspeitas, desligar o telefone imediatamente e entrar em contato com a Polícia Militar. É ela quem pode ir até o local e verificar se há realmente pessoas suspeitas no entorno do estabelecimento.

APLICATIVO FRAUDULENTO MEDIANTE ENGENHARIA SOCIAL

Tanto no Google Play, como no App Stores existem centenas de aplicativos falsos, desenvolvidos com o objetivo de auxiliar criminosos a cometerem fraudes. Ainda, criando links falsos, sites, argumentos ou situações fictícias, eles induzem a vítima a baixar o aplicativo que, uma vez instalado no aparelho de telefone ou computador do alvo, conseguem coletar dados pessoais dele. Alguns podem trazer, por exemplo, malwares — que capturam dados pessoais e senhas — ou scammers — capazes de tirar proveito de informações de cartões de crédito digitados no aparelho.

ⓘ COMO PREVENIR?

Evite acessar sites de fontes desconhecidas e jamais clique em links que receber via mensagens de texto, WhatsApp ou e-mail. Além disso, existem aplicativos que imitam os de empresas reais, copiando inclusive suas cores, logos e até mesmo o nome, trocando apenas uma letra ou outra. Sendo assim, prestar muita atenção nos nomes dos aplicativos, no desenvolvedor deles e símbolos utilizados no app.

Nas plataformas de compra de app, é necessário verificar as avaliações de um aplicativo antes de baixá-lo, bem como a data de publicação dele.

CRÉDITO CONSIGNADO

Em uma versão mais atualizada deste golpe, organizações criminosas estão comprando, ilegalmente, pacotes com dados e documentos pessoais de diversos brasileiros. Em posse dos dados pessoais e bancários das vítimas, e por vezes, com a ajuda de funcionários do próprio INSS, os criminosos operam como se fossem agentes de instituições financeiras, autorizando o crédito em nome delas. A partir disso, a instituição financeira comunica o INSS, que vai registrar o empréstimo no CPF do aposentado ou servidor público.

O dinheiro cai na conta do beneficiário, porém as parcelas com juros também começam a cair na mesma conta. Para o golpista, a vantagem é ficar com as comissões que remuneram o agente de crédito por intermediar o empréstimo.

Há ainda o golpe em que esses agentes, ao negociarem as dívidas do solicitante, indicam uma conta de depósito para a quitação (amortização) do referido empréstimo consignado. Como o atendente tem posse de todas as informações da dívida, a vítima acredita estar em contato com a instituição financeira, e acaba depositando o valor.

ⓘ COMO PREVENIR?

Suspeitar, sempre, de contatos telefônicos em nome da Previdência Social.

Nunca depositar valores para contas PIX de pessoas físicas em casos de negociação de dívida e pesquisar sempre sobre a idoneidade de instituições desconhecidas. O ideal é sempre contratar um serviço de empréstimo através de plataformas oficiais dos bancos, ou presencialmente, nas próprias instituições.

PROGRAMA DESENROLA

Criminosos criam sites e perfis falsos nas redes sociais, aparentando ser do programa Desenrola, programa este que visa renegociar dívidas de brasileiros com instituições bancárias.

Utilizam-se de símbolos do governo e do programa para passar ainda mais credibilidade e ludibriar a vítima.

ⓘ COMO PREVENIR?

Verificar atentamente o endereço do site. Golpistas utilizam domínios com grafia parecida para enganar as vítimas.

Vale destacar que a renegociação do programa Desenrola acontece somente nos sites das próprias instituições bancárias.

Cuidado ao buscar o link do site em buscadores na internet, os criminosos têm a prática de pagar as plataformas para que os links falsos sejam os primeiros a aparecer nas pesquisas.

MAQUININHA QUEBRADA

Este golpe costuma ter alguns tipos de abordagens e variações. Ele começa quando a vítima faz um pedido por aplicativo e no momento da entrega é apresentada uma maquininha com o visor danificado ou o entregador se posiciona de uma forma que ela não veja o preço cobrado na tela.

O valor inserido é bem superior ao pedido e a vítima só percebe que fez um pagamento maior depois de um tempo.

Pode ocorrer também um formato que a compra já paga pelo aplicativo, mas a vítima é convencida que ocorreu um problema e é cobrada novamente ou cobrado algum frete adicional, normalmente também colocam um valor maior.

ⓘ COMO PREVENIR?

Sempre conferir o valor que está sendo cobrado quando realizar alguma compra cujo pagamento dar-se-á por maquininha de cartão.

Nunca aceitar efetuar pagamento em máquinas quebradas, e ficar atento às teclas que são digitadas pela pessoa responsável pela cobrança.

TROCA DE CARTÃO

Este golpe ocorre dentro de agências bancárias. O criminoso geralmente encontra-se vestido aparentando ser funcionário daquele banco, inclusive, utilizando crachá.

Ele observa a vítima na agência e, quando ela sai, ele a aborda e explica que algo deu errado em sua transação financeira, pedindo então, para ver o seu cartão. Quando a vítima entrega-o, rapidamente o criminoso faz a troca de cartão, alegando que de fato não houve problemas. Quando a vítima percebe que está com um cartão que não é o seu, vai até a agência ou, através do próprio aplicativo do banco, percebe que teve seus valores extraídos de sua conta. O criminoso, nestes casos, conseguiu ver a senha que a própria vítima digitava enquanto estava na agência.

ⓘ COMO PREVENIR?

Nunca entregue nem mesmo deixe um terceiro desconhecido ver o seu cartão bancário.

QR CODE FALSO

Este é um golpe em que o criminoso substitui o QR Code oficial de um estabelecimento por outro que direciona a vítima a algum link malicioso. Geralmente, esse link contém um malware capaz de roubar os dados do celular.

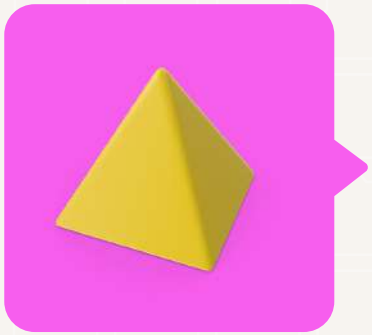
Deste modo, o criminoso consegue acessar aplicativos de bancos, redes sociais, além de ter acesso aos contatos e conteúdos da vítima.

ⓘ COMO PREVENIR?

“QR Codes” com erros de impressão, desalinhados ou com características visuais suspeitas, podem ser indício de um código falso.

Em casos de QR Codes físicos em estabelecimentos, importante verificar se não há adesivos por cima do código, e se ele foi fornecido pela empresa ou um por um funcionário autorizado.

Verifique, também, se a URL é confiável antes de acessá-la.



PIRÂMIDE FINANCEIRA

Também conhecida como ***Esquema de Ponzi***, este golpe promete rendimentos altos e rápidos para determinado investimento, porém, de forma insustentável. É necessário que a pessoa que decida investir traga mais pessoas para o negócio.

Nestes casos, o golpista, que será o líder e estará no topo da pirâmide, convida e convence pessoas a investirem determinado valor em algum negócio, garantindo-lhes um rendimento altamente rentável. Por vezes, a vítima começa obtendo retorno, o que faz com que ela acredite na idoneidade do procedimento. Porém, é comum que o golpista simplesmente "desapareça" com o dinheiro investido.

Vários produtos e investimentos podem ser usadas como plano de fundo para o golpe, como criptomoedas, investimentos em franquias, imóveis e outras coisas.

ⓘ COMO PREVENIR?

Antes de mais nada, estudar sobre o mercado financeiro e formas de investimento. Os golpistas passam uma sensação de urgência e de oportunidade única que vai acabar logo, por isso é importante estar atento a esses detalhes, avaliar os riscos, conhecer o "vendedor" da promessa. Sempre importante estar atento às informações da empresa de investimento, procurando saber sobre ela em sites, como "Reclame Aqui".

Se estiver negociando ativos do mercado financeiro, acessar o site da CVM (Comissão de Valores Imobiliários). Além disso, desconfiar de promessas ricas.

INVESTIMENTOS

Os criminosos usam pessoas jurídicas com aparente credibilidade para oferecer investimentos pessoais com ganhos e taxas de juros acima dos comumente praticados no mercado. Eles alegam que atuam no mercado de ações ou que possuem algum produto de grande valia.

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

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

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

ⓘ COMO PREVENIR?

Sempre suspeitar de ofertas de investimentos com ganhos acima daqueles praticados pelo mercado bancário regular, ainda que apresentados por empresas com aparente credibilidade, ou por pessoas conhecidas e familiares, que podem estar na base do sistema e por isso receberam algum "rendimento", os fazendo crer na rentabilidade do negócio.

Verificar se existe autorização do Banco Central e fiscalização do Conselho de Valores Mobiliários.

Lembre-se, esse esquema a qualquer momento pode ser interrompido e quebrado, deixando inúmeras vítimas.

FALSO MOTOBOY

A pessoa recebe uma ligação de um golpista passando-se por um funcionário de seu banco e confirmando uma compra feita em seu nome.

Após a pessoa dizer que desconhece a compra, o falso funcionário informa que verificou que seu cartão foi clonado e pede que o cartão seja cortado, mas sem danificar o chip para poderem “investigar”, solicitando sua senha para que possa gerar um novo cartão que será entregue em até dois dias. Informa também que enviará um motoboy do banco para retirar o cartão na sua residência.

Outro golpista vai até o endereço da vítima e recolhe o cartão. Agora de posse dos criminosos, o cartão com o chip preservado será utilizado para compras e outras transações.

ⓘ COMO PREVENIR?

Instituições bancárias não ligam solicitando senhas de cartões e não se deslocam às residências para recolher cartões, portanto, ao receber esse tipo de ligação, desligue imediatamente.

OFERTA DE EMPREGOS

Visando obter dados pessoais e cadastrais para a prática de golpes posteriores, criminosos divulgam vagas de emprego em plataformas como Facebook, OLX e sites de emprego.

Na vaga ofertada, divulga-se um número de telefone para contato, e além do currículo, os criminosos solicitam cópia de RG, CPF e, por vezes, outros documentos pessoais. Em alguns casos, inclusive, divulgam um local para a seletiva. No momento em que os candidatos deslocam-se até o local indicado, percebem ter caído em um golpe.

ⓘ COMO PREVENIR?

Antes de enviar o currículo para alguma empresa, verificar através de suas plataformas oficiais se a vaga realmente existe.

Jamais enviar qualquer documento pessoal para números desconhecidos nem preencha em sites de empregos o número de sua carteira de trabalho ou de qualquer outro documento que permita o fraudador se passar por você.

MALHA FINA / REGULARIZE SEU CPF

O golpista encaminha um comunicado falso por e-mail informando divergências na declaração do Imposto de Renda do destinatário.

No corpo do e-mail consta ainda a informação que a declaração está em análise e passará pela Malha Fiscal.

Por fim é disponibilizado um link para download de um suposto relatório.

Ao clicar no link, o usuário pode estar expondo seus dados, como número do CPF, da conta bancária, endereço, entre outros.

ⓘ COMO PREVENIR?

Desconfie de e-mails ou mensagens que solicitam informações pessoais.

Nunca clique em links suspeitos ou desconhecidos.

Não abra arquivos anexados, pois podem ser programas que captam informações confidenciais do usuário.

Lembre-se que a Receita Federal não envia comunicações por e-mail ou mensagens de texto.

Eventuais solicitações são feitas pelo Portal e-CAC ou pelo aplicativo oficial da instituição.

AMEAÇA POR TELEFONE

O criminoso faz contato com a vítima por telefone dizendo que estaria “decretada à morte” em razão de ter passado informações à Polícia.

Afirma que fotos da vítima estão circulando em diversos grupos de WhatsApp ligados à criminosos.

Muitas vezes menciona o endereço da vítima e até nomes de familiares para dar credibilidade a sua versão.

Na sequência exige a transferência de valores para não cumprir as ameaças.

ⓘ COMO PREVENIR?

Mantenha suas contas de redes sociais no modo privado para que somente amigos tenham acesso ao seu conteúdo.

Não responda as mensagens e bloqueie os números de telefone.

Por mais verdadeira que pareçam as ameaças, não faça transferências bancárias, pois elas não cessarão.

INTELIGÊNCIA ARTIFICIAL PARA CLONAR VOZES

Os criminosos acessam as redes sociais de uma pessoa e utilizam ferramentas de inteligência artificial para clonar sua voz (3 segundos de fala são suficientes para criar áudios longos).

Com a voz clonada, os criminosos entram em contato com familiares ou amigos se passando pelo "dono" da voz e pedem o envio de dinheiro ou informações pessoais.

Os familiares e amigos, acreditando estar conversando com a verdadeira pessoa cumprem as orientações do golpista.

ⓘ COMO PREVENIR?

Mantenha suas contas de redes sociais privadas.

Diminua a quantidade de informações pessoais que você compartilha na internet.

Se algum amigo ou familiar solicitar dinheiro, tente entrar em contato por outro meio de comunicação para confirmar a veracidade do pedido.

Confira sempre a conta bancária do destinatário.

PAGUE E RECEBA UM PRESENTE

Golpistas entram em contato com a vítima por mensagens, dizendo que ela tem um presente a receber, mas que, para isso, precisará pagar uma taxa de entrega via PIX ou cartão.

Com isso, enviam um link ou os dados para o pagamento da taxa e, quando a vítima o realiza, o golpista some.

Em alguns casos, o golpista vai até o endereço da vítima realizar a entrega e no momento da cobrança passa valores altíssimos na maquininha de cartão, causando prejuízos financeiros que podem ser significativos.

ⓘ COMO PREVENIR?

Confirme se a operação é legítima.

Desconfie de taxas cobradas na entrega.

Preste atenção no visor da maquininha de cartão.

Fique atento às entregas e mensagens não solicitadas.

Não forneça nenhum código para desconhecidos.

Não permita que ninguém veja sua senha enquanto digita e não entregue seu cartão nas mãos de terceiros.

CARREGADOR DE CELULAR COMPARTILHADO

O equipamento de celular funciona não apenas como transmissor de energia ao ser conectado por um cabo, mas também como emissor de informações armazenadas no telefone.

Assim, um carregador modificado pode copiar essas informaçãos e ficarem armazenadas para uso posterior.

O acesso ao smartphone pode fazer com que eles roubem dados sigilosos e, em casos mais sérios, bloqueiem totalmente o dispositivo.

ⓘ COMO PREVENIR?

Evite utilizar carregadores de celular ou cabos USB em locais públicos, como praças de alimentação, shoppings, aeroportos, rodoviárias, hotéis e outros locais, pois estes podem conter em sua estrutura dispositivos capaz de esconderem programas maliciosos (vírus) capazes de infectar seu dispositivo enquanto recarrega a bateria roubando senhas, dados bancários e outras informações pessoais.

Procure sempre utilizar seu próprio carregador de celular, mas se precisar usar esse serviço em caso de necessidade, desligue o aparelho antes de colocá-lo para carregar e só ligue depois de retirar do carregador ou cabo.

DESCONTO NO IPVA

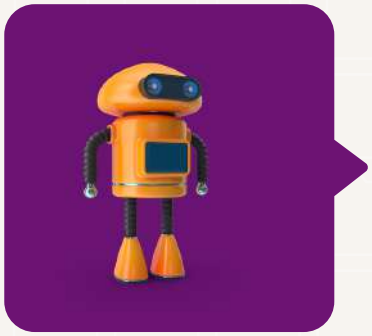
Golpistas criam clones dos sites do DETRAN e anunciam em plataformas digitais com um endereço similiar ao oficial.

Anunciam falsos descontos no IPVA para quem realizar pagamento por PIX em sua plataforma.

ⓘ COMO PREVENIR?

O Detran/SC NÃO oferece desconto no IPVA para pagamentos via PIX.

Confira seu o endereço do site é oficial ou possui algumas letras repetidas a fim de enganar o cidadão. Em Santa Catarina o site oficial é www.detran.sc.gov.br



ROBÔ DO PIX

Sob a promessa de dinheiro fácil, os golpistas oferecem uma ferramenta que supostamente seria capaz de fazer inúmeros comentários em sorteios que acontecem nas redes sociais, aumentando suas chances de vencer e acumular prêmios em espécie.

Para isso, a vítima precisa acessar um link, preencher alguns dados pessoais e realizar uma transferência bancária via PIX.

Além de não obter qualquer retorno financeiro, os dados pessoais fornecidos poderão ser utilizados na aplicação de novos golpes.

ⓘ COMO PREVENIR?

Não acredite em ofertas extraordinárias e que prometem altos lucros em pouco tempo.

Pesquise sobre o assunto em sites de confiança.

PARE E PENSE! Não aja por impulso, principalmente quando a oferta estiver acabando ou parecer imperdível.

Desconfie de anúncios que contenham imagens de celebridades, pois elas são utilizadas indevidamente para passar mais credibilidade ao golpe.

Não acesse links desconhecidos, nem cadastre seus dados pessoais ou de cartão de crédito em sites suspeitos.

Não realize pagamentos ou transferências bancárias sem antes certificar-se da idoneidade do fornecedor do produto/serviço.

FALSOS PRECATÓRIOS

Golpistas acessam os julgamentos acessíveis ao público e em posse dessas informações confeccionam um ofício com o timbre do Poder Judiciário, com os dados processuais, valores a receber, entre outras informações.

Então entram em contato com as possíveis vítimas utilizando os nomes dos advogados dos casos e com informações reais para dar veracidade ao golpe.

A partir daí os golpistas exigem a antecipação do pagamento de valores a título de custos para expedição do precatório.

ⓘ COMO PREVENIR?

O precatório é uma requisição devida a qualquer pessoa que saiu vitoriosa de uma ação judicial movida contra o poder público (União, Estados, Municípios, Autarquias, Fundações). O pagamento obedece a uma ordem cronológica que está disponível na página de Assessoria de Precatórios do TJSC.

Ressalta-se aos credores que é impossível antecipar um precatório por meio de pagamento.

Importante anotar que a Assessoria de Precatórios do TJSC não faz ligação e nem envia e-mail para credores. Além disso, qualquer proposta de antecipação do título mediante pagamento prévio deve ser rejeitada.

FALSO ALUGUEL

Os golpistas clonam anúncios de imóveis disponíveis na internet e se passam pelos proprietários. Após, anunciam o imóvel para aluguel com o preço abaixo do praticado no mercado. A publicidade é perfeita, com foto e e-mail do proprietário.

Os interessados entram em contato e a negociação do aluguel ocorre. Porém, o responsável pelo golpe sempre dá desculpas para não mostrar nada do imóvel além do que está no anúncio.

Por fim, após o pagamento, na maioria dos casos realizado via PIX, o golpista some deixando os interessados sem dinheiro e sem acesso ao suposto imóvel.

Às vezes ao entrar em contato com o anunciante, este diz que já há algumas pessoas na frente para visitar o imóvel e oferece a opção de pagar um sinal para reservar o apartamento, criando uma urgência.

ⓘ COMO PREVENIR?

Desconfie de anúncios com valores muito abaixo do mercado.

Dê preferência por alugar um imóvel com um corretor ou imobiliária de sua confiança. Se for alugar on-line, busque realizar o aluguel em sites conhecidos e que garantam a devolução do dinheiro do cliente em caso de problemas com o imóvel.

Confira se o endereço realmente existe.

Antes de locar, agende uma visita.

Dê preferência para pagamentos feitos com cartão.

GOLPES NA BLACK FRIDAY

Período de promoções em que criminosos aproveitam-se da empolgação dos consumidores em comprar produtos abaixo do preço, e efetivam golpes mediante fraudes eletrônicas utilizando-se do tema.

ⓘ COMO PREVENIR?

Ao ver promoções, você pode ver a reputação de grandes varejistas na internet e evitar problemas. É possível ler o conteúdo das reclamações, as respostas das empresas e a avaliação dos consumidores no site. Pesquise sempre.

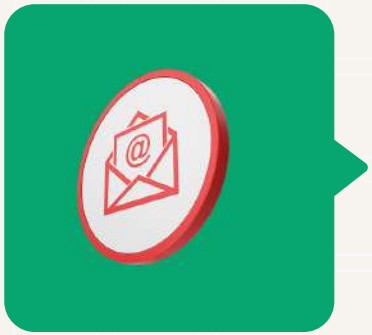
Busque por sites comparadores de preços e produtos. Alguns informam realmente se o preço está promocional ou se teve um ajuste antes da data para informarem uma “falsa promoção”.

Utilize cartões virtuais para realizar as compras nessa data. Caso você tenha realizado uma compra em algum site criminoso, você pode excluir o cartão virtual a qualquer momento.

Se realizar o pagamento via boleto bancário, verifique quem é a empresa beneficiária que aparece no documento. Algumas utilizam nome fantasia diferente da Razão Social não caracterizando golpe.

Não use computadores públicos para realizar a compra.

Não aja com emoção. Desconfie de preços muito menores que o valor real do produto.



E-MAIL VAZIO

Um criminoso utilizando um endereço eletrônico verdadeiro envia vários e-mails sem nenhum conteúdo e geralmente com algum assunto como “Olá”, “Oi”, “Eu” ou outras palavras que acabam sendo atrativas para um clique.

O e-mail vazio consegue passar pelos filtros de segurança dos servidores facilmente.

Uma vez recebida a mensagem, o criminoso identifica um e-mail válido e uma possível vítima. A partir disso, o destinatário irá receber mais e-mails, agora com tentativas reais de golpes, como Phishing e anexos maliciosos, ataques ransomwares, entre outros.

O golpe do e-mail vazio é muito mais um teste dos criminosos para saber quais e-mails são válidos para ataques do que uma ameaça proprieamente dita.

ⓘ COMO PREVENIR?

Procure nas configurações do servidor de seu e-mail alguma configuração para bloquear mensagens sem conteúdo. Essa é uma maneira de avisar ao criminoso que seu endereço não está váldio.

Caso tenha recebido um e-mail de algum endereço desconhecido e que o assunto cause estranheza não interaja e exclua-o.

Marque o remetente com SPAM, assim as próximas mensagens irão para o “lixo eletrônico” do servidor de e-mail.

Não clique em links ou baixe anexos suspeitos.

CONTA DO INSTAGRAM INVADIDA

Criminosos invadem o perfil de um alvo e o usam como isca para tentar ganhar dinheiro dos seguidores do perfil invadido: eles fazem stories se passando pelo dono da conta avisando que um parente está se mudando do Brasil e, por isso, está vendendo alguns itens como eletrodomésticos ou eletrônicos.

Os preços são baixos porque a pessoa precisa agilizar a saída do país.

De outro modo, anunciam celulares que suspostamente foram trazidos por algum parente dos exterior, geralmente a preços bem baixos, ou utilizam-se de perfis de estabelecimentos comerciais, enviando mensagens que oferecem vantagens, como sorteios ou promoções.

A negociação acontece pelo Direct do Instagram, momento em que a vítima acredita estar conversando com o verdadeiro “dono” do perfil. O criminoso, então, envia uma chave Pix e pede o comprovante – após o pagamento ser efetuado, o golpista bloqueia a vítima.

Outra variante são as contas invadidas postarem publicidade de supostos investimentos de alto rendimento, quando a vítima faz contato, achando que está falando com um conhecido, é indicado para um suposto intermediador, este irá pedir pagamentos para que o investimento seja efetivado.

ⓘ COMO PREVENIR?

Desconfie de publicações na internet que ofereçam serviços e bens por um valor abaixo do preço de mercado.

Se estiver em negociação, peça para realizar de outra forma além do Direct do Instagram, como por WhatsApp, ligação ou pessoalmente.

Confira os dados da chave PIX conferem com o nome do perfil.

Se teve sua conta conta invadida, veja na próxima página como recuperar.

INSTAGRAM HACKEADO?

VEJA COMO RESOLVER EM 10 PASSOS:

1. Faça o *logoff* (sair) de todas as contas no aplicativo do Instagram;

2. Insira o nome de usuário da sua conta;

3. Selecione a opção "***Esqueceu a senha?***";

4. Selecione a opção "***Precisa de mais ajuda?***";

5. Verifique se reconhece o trecho do seu e-mail ou o número de telefone vinculado que aparece na tela;

6. Caso o hacker tenha conseguido alterar o e-mail ou o telefone de recuperação, toque na opção "***Não consigo acessar este e-mail ou número de telefone***";

7. Selecione a opção "***Minha conta foi invadida***" e toque em avançar;

8. Selecione a opção "***Sim, eu tenho uma foto na minha conta.***";

9. Insira seu endereço de e-mail no campo disponível e depois toque em "***Enviar***". Você receberá um código de confirmação no e-mail informado;

10. Será solicitado que você tire uma selfie para auxiliar na recuperação da conta hackeada. Siga os procedimentos na tela.

Se tudo correr bem, você receberá, por e-mail, um link para recuperar sua conta.

Dicas para evitar a invasão de sua conta:

Ative a autenticação em 2 fatores;

Evite tornar público o seu número de telefone vinculado ao Instagram. Os criminosos utilizam essa informação, combinada com engenharia social para hackear sua conta;

Prefira aplicativos autenticadores para realizar o duplo fator de autenticação das suas contas em redes sociais. Pesquise no Google como funcionam essas ferramentas;

Jamais forneça a ninguém os links ou códigos de confirmação que lhe forem enviados por e-mail ou sms.

FOI VÍTIMA DE ALGUM GOLPE?

Registre um Boletim de Ocorrência na Polícia Civil de Santa Catarina. Você pode fazer o seu on-line pelo site ***delegaciavirtual.sc.gov.br*** , clicar em “Registrar Boletim de Ocorrência” e seguir os próximos passos que aparecerem na tela. Você também pode ir à uma Delegacia de Polícia Civil mais próxima para fazer o seu registro.

Mantenha um registro com todos os detalhes relacionados ao golpe, incluindo datas, horários, nomes, números de telefone e quaisquer outras informações relevantes. Isso pode ser útil nas investigações posteriores.

CONHECE ALGUÉM QUE ESTÁ COMETENDO GOLPES?

Você pode fazer uma denúncia anônima para a Policia Civil de Santa Catarina em um de nossos canais:
- Pelo site ***delegaciavirtual.sc.gov.br*** e clicar em “Comunicar Central de Denúncias”;
- WhatsApp ***(48) 98844-0011***;
- Telefone pelo Disque Denúncia ***181***

VOCÊ SABE A DIFERENÇA ENTRE FAZER UMA **DENÚNCIA E UM BOLETIM DE OCORRÊNCIA (BO)?**

A principal diferença entre um boletim de ocorrência e uma denúncia é que o BO é um relatório oficial de um incidente, enquanto a denúncia é um ato legal que acusa alguém de atividade criminosa e inicia o processo judicial.

O boletim de ocorrência frequentemente é o primeiro passo para a coleta de informações em casos que podem levar a uma denúncia e, subsequentemente, a um processo criminal.

+DICAS

CRIANÇAS E CELULARES

Aos pais que costumam permitir que seus filhos usem seus dispositivos celulares para jogar ou assistir a vídeos, é importante que nunca deixem senhas e informações pré-cadastradas no aparelho. É importante saber que a criança pode inadvertidamente clicar em anúncios publicitários e realizar compras não intencionais, ou até mesmo se deparar com anúncios contendo links maliciosos.

TESTES ON-LINE

Evite ao máximo participar dos jogos de perguntas e respostas, assim como dos "testes de personalidade" em redes sociais. Alguns deles solicitam permissão para utilizar sua foto em simulações como "veja como será sua aparência daqui a dez anos."

Muitos desses testes têm a intenção de capturar suas informações pessoais e acessar seu dispositivo. Ao interagir com esse tipo de conteúdo, você pode inadvertidamente autorizar a instalação de códigos maliciosos em seu telefone ou computador.

O Ggolpe tá aí.

CAI QUEM NÃO SE INFORMA.

POLÍCIA CIVIL DE SANTA CATARINA

www.pc.sc.gov.br

48 3665.8100

@policiacivilsantacatarina

/pcscoficial

@pcscoficial

delegaciageral@pc.sc.gov.br