FIQUE ESPERTO!

Uma campanha:

Ministério Público e Polícia Civil de Caxias do Sul

As Promotorias de Justiça Criminal de Caxias do Sul, juntamente com a Polícia Civil do município, lançam uma campanha de alerta e prevenção aos crimes de estelionato e extorsão.

Confira alguns dos golpes mais comuns:

Bilhete premiado:

É um golpe antigo. Para simular o bilhete sorteado, o estelionatário faz um jogo na lotérica com os números sorteados, conseguindo o comprovante de aposta de um sorteio que ainda vai ocorrer.
Após, atua em locais de grande fluxo e aborda, preferencialmente, vítimas idosas ou que estejam saindo de um banco.

Dica

Evitar dar continuidade na conversa com pessoas estranhas, principalmente quando dizem estar com um bilhete premiado. Avisar imediatamente a polícia para efetuar a abordagem dos estelionatários, uma vez que atuam em vários estados e podem ter mandados de prisão abertos.

Publicidade em lista telefônica:

O estelionatário efetua ligações para alguma empresa e oferece gratuitamente o serviço de propaganda em algum site de listas de telefones, legando ser uma página muito acessada na internet.

Dica

Leia atentamente o que receber e se desconfiar de algo, não assine.
Caso tenha caído nesse golpe, procure um advogado de sua confiança para orientações cíveis e registre o fato na delegacia de polícia.

Torpedo premiado:

Também é um golpe dos mais antigos aplicados. A vítima recebe um sms, geralmente de um celular de outro estado, informando que foi contemplada num sorteio. Ao entrar em contato com o número, a vítima é colocada numa suposta central de atendimento que solicita depósitos de encargos.

Falso sequestro:

É aplicado com base em informações obtidas da própria vítima, no momento de desespero. O estelionatário liga aleatoriamente para telefones, diz que está com um parente da vítima, exige dinheiro para o resgate e faz ameaças. Normalmente, pessoas ao fundo imitam agressões e gritos. Se aproveitando do pânico causado, os golpistas convencem a vítima a não desligar e a depositar dinheiro em várias contas, por meio de caixas de atendimento bancários. Eles mantêm a vítima em pânico, sem tempo para que possa raciocinar sobre o fato.

Dica

Nunca forneça seus dados por telefone e invente um nome quando o estelionatário dizer que tem um parente seu sequestrado. Por precaução, ligue para o suposto parente.

Falso boleto:

Por meio de cavalo de troia ou outro malware, o estelionatário tem acesso aos dados do computador da vítima. Após efetuar negociação pela internet e receber um boleto do verdadeiro fornecedor, ela também recebe um segundo email, contendo um boleto com desconto. Porém, esse boleto não pertence à compra da vítima, mas a uma compra do estelionatário em um site de vendas.

Dica

Mantenha o antivírus do computador atualizado e, se receber emails nesta situação, entre em contato diretamente com o fornecedor para esclarecimentos.

Falso problema mecânico em veículos:

A vítima recebe uma ligação de um suposto parente, dizendo que está em uma oficina com o veículo quebrado. Ele alega ter esquecido a carteira em casa e pede que deposite uma quantia na conta do falso mecânico, prometendo devolver depois.

Sites de compras ou empréstimos pessoais:

A vítima procura em sites de pesquisas algum produto ou empréstimo pelo preço mais vantajoso, mas não se cerca de toda a precaução possível para efetuar a confirmação do negócio. No caso do empréstimo, o estelionatário exige vários depósitos de dinheiro para pagamento de taxas. No caso das compras, é emitido um boleto que contém o código de barras de uma compra realizada pelo próprio estelionatário, e não a compra da vítima. Após o pagamento do boleto, geralmente o site é deletado.

Envelope vazio:

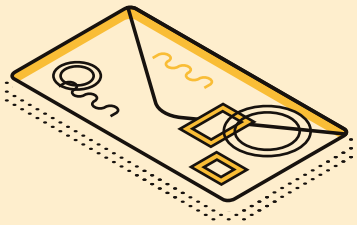
Por meio de sites comuns de vendas de objetos ou de veículos, o estelionatário inicia contatos com a vítima e apresenta uma proposta de compra. Após isso, o estelionatário vai até a cidade da vítima e pede para alguém depositar um envelope vazio ou contendo um cheque furtado, roubado ou sustado e de posse disso a vítima faz a transferência do veículo, sem verificar a compensação do título.

Phishing (Pesca e fraude eletrônica):

Tentativas de adquirir dados pessoais (senhas, dados financeiros, etc.). O fraudador se passa por uma pessoa/empresa/ente público confiável e envia um email/sms contendo, geralmente, um link que dá acesso a uma página falsa ou para instalação de um malware.

Teste da máquina de cartão ou recarga:

A vítima recebe uma ligação de alguém se passando por funcionário da empresa responsável pelas máquinas. Tal pessoa informa a necessidade de fazer uma atualização do aparelho. Com códigos passados pelo estelionatário, o atendente habilita a máquina para recargas de celular. Após isso, diz que irá fazer alguns testes e que irá resetar o aparelho. Os testes são, na verdade, recargas para vários celulares.



Falso comprador em sites de anúncio ou redes sociais:

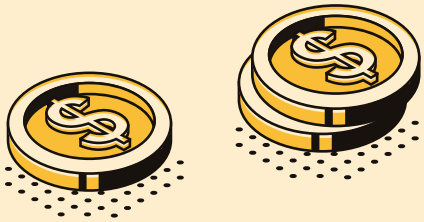
O estelionatário busca nos principais sites de anúncios ou nas redes sociais objetos de seu interesse e inicia contato com a vítima se mostrando muito interessado no produto. As negociações ocorrem em aplicativos de mensagens e nunca de forma pessoal, com o estelionatário se passando por outra pessoa (geralmente uma vítima anterior que forneceu fotos de seus dados bancários e identidade). Fechada a negociação, ele envia uma ted falsificada para a vitima ou um comprovante de depósito efetuado em caixa eletrônico (envelope vazio). Imediatamente informa que um parente ou um amigo irá buscar o objeto, sendo que na verdade se trata de um freteiro contratado pelo estelionatário e que não sabe da armação.
A característica deste fato é a velocidade entre o pagamento e a busca do objeto, além da pressão imposta para que a vítima entregue o objeto rapidamente. Nos casos em que a vítima descobre o golpe, o estelionatário começa a efetuar ameaças para que a vítima encaminhe o objeto.

Dica

Jamais forneça fotos de seus documentos ou cartões bancários, para que o suposto comprador efetue o pagamento, pois isso será utilizado pelo suspeito no golpe com a próxima vítima. Desconfie se toda a negociação ocorrer pelo aplicativo e o estelionatário não quiser ver o produto antes de comprar. Confira a ted ou o comprovante de depósito em sua agência bancária e não entregue o objeto antes do desbloqueio dos valores e de receber definitivamente o dinheiro.

Envio de nudes:

O estelionatário se passa por uma formosa mulher nas redes sociais e envia um vídeo ou fotos de "nudes", solicitando que a vítima também faça isso. De posse das fotos e vídeos das vítimas, os criminosos informam que vão enviar os materiais aos amigos e parentes das vítimas, solicitando quantias em dinheiro para não fazer a divulgação.



Envelope vazio:

Por meio de sites comuns de vendas de objetos ou de veículos, o estelionatário inicia contatos com a vítima e apresenta uma proposta de compra. Após isso, o estelionatário vai até a cidade da vítima e pede para alguém depositar um envelope vazio ou contendo um cheque furtado, roubado ou sustado e de posse disso a vítima faz a transferência do veículo, sem verificar a compensação do título.

História de amor:

O estelionatário se passa por um militar de alguma força estrangeira, ganhando a confiança e a admiração da vítima com o passar do tempo. As conversações ocorrem geralmente por aplicativos de mensagens de redes sociais. De posse da confiança da vítima, solicita dinheiro para efetuar a viagem ao Brasil e conhecer a mesma pessoalmente.

Clonagem do Whatsapp:

Essa modalidade de fraude ocorre geralmente após a vítima efetuar um anúncio em sites de venda, no qual é publicado o celular da vítima. O estelionatário se passa por um atendente do site e alegando questões de segurança, solicita que a vítima informe o código que será enviado por sms. Ocorre que o código informado pertence ao aplicativo whatsapp e de posse dele, o estelionatário consegue habilitar o celular com os dados e informações da vítima, passando a solicitar valores aos contatos salvos.

Dica

Leia com atenção o sms recebido e habilite em seu celular a verificação em duas etapas. Entre no aplicativo e siga os itens da seguinte forma: whatsapp > item > configurações > conta > confirmação em duas etapas.

Prevenção:

- **Nunca passe qualquer dado pessoal por telefone.**
- **No golpe do falso sequestro, não diga o nome de seu parente ou familiar.**
- **Não ligue para o número do sms premiado e desconfie de ligações recebidas em modo restrito ou de outras áreas.**
- **Caso supostos parentes lhe peçam dinheiro, ligue para o número correto dos mesmos para confirmar.**
- **Consulte páginas específicas ou o procon para encontrar sites confiáveis de compras online.**

Esteja atento às dicas desta cartilha. Caso algum golpe se assemelhe, procure pelas autoridades responsáveis. Você também pode repassar este material para que mais pessoas tenham acesso e se mantenham informadas sobre os crimes de estelionato e extorsão.

Divulgação:

POLÍCIA CIVIL
ESTADO DO RIO GRANDE DO SUL

MINISTÉRIO PÚBLICO
ESTADO DO RIO GRANDE DO SUL