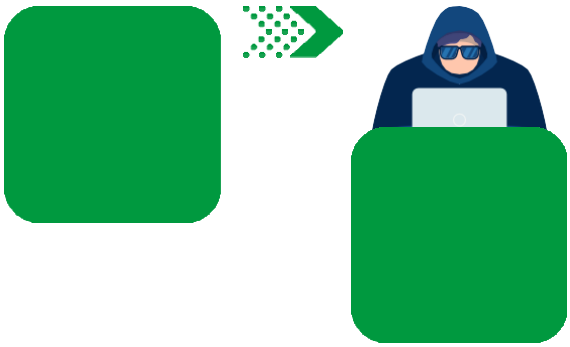
Clonagem de Whatsapp

POLÍCIA CIVIL PR

meios eletrônicos



1. Clonagem de WhatsApp

O golpe ocorre da seguinte forma:

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

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

Como evitar o golpe:

a) Ative a “Confirmação em duas etapas” no WhatsApp.
b) NUNCA forneça o código verificador que você recebe via SMS em seu celular.
c) Não instale apps de terceiros ou compartilhe informações pessoais a pedido de ninguém pelo whatsapp.
d) Desconfie de situações em que a pessoa solicita a realização de transferências e pagamentos em caráter de urgência.
e) Ligue para a pessoa que solicitou o dinheiro e verifique se realmente é ela quem está solicitando a transação.

Caso tenha sido vítima, o que fazer:

Vítima do celular clonado
a) Em posse de todas essas informações, procure a Delegacia de Polícia mais próxima.
b) Peça para amigos e familiares excluírem o telefone clonado de grupos e alertarem o máximo de contatos em comum sobre o ocorrido.

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

2. Boleto Falso

O golpe ocorre da seguinte forma:

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

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

Como evitar o golpe:

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

Caso tenha sido vítima, o que fazer:

a) Entre em contato com o banco e tente bloquear o valor.
b) Tire cópia do comprovante de pagamento e demais documentos correlatos.
c) Em posse de todas essas informações, procure a Delegacia de Polícia mais próxima de sua casa.

3. Fraudes bancárias

Alguns tipos de fraudes bancárias mais recorrentes:

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

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

Caso tenha sido vítima, o que fazer:

a) Entre em contato com o banco e tente bloquear o valor.
b) Tire cópia do comprovante de pagamento e demais documentos correlatos.
c) Em posse de todas essas informações, procure a Delegacia de Polícia mais próxima de sua casa.

4. Sites de comércio eletrônico fraudulentos

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

O golpe ocorre da seguinte forma:

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

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

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

Como evitar o golpe:

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

a) Procure utilizar terminais (computador, smartphone, tablet) que sejam seguros;

b) Leia atentamente as informações dos sites e do produto que deseja comprar. Normalmente, sites fraudulentos podem conter erros de português ou ainda sobre as informações técnicas do produto. Verifique também se há CNJP cadastrado na página ou canais de comunicação;

c) Faça uma pesquisa de mercado do valor do produto que deseja adquirir. Desconfie de preços muito baixos;

d) Realize pesquisas na internet para obter informações a respeito da reputação do site em que deseja efetuar compras. Essas informações podem ser obtidas através do Reclame Aqui ou de redes sociais. É possível ainda verificar a lista de sites reprovados, disponibilizada pelo Procon.

e) Verifique se o site é seguro, localizando o ícone de um cadeado, ao lado do endereço do site (URL). Ao clicar no cadeado, será exibido o certificado de segurança da página;

f) Evite clicar em links que direcionam a navegação diretamente ao site de compras. Ao invés disso, prefira digitar o endereço do site (URL) junto à barra de endereço de seu navegador. **Atenção:** os sites fraudulentos geralmente possuem o endereço muito semelhante ao site verdadeiro. Exemplo: www.americanas.com.br (site verdadeiro) e www.lojasamercanas.com.br (site falso – exemplo fictício). Note que no exemplo do site falso foi incluído o nome "lojas" e a letra "i" do nome "americanas" foi suprimida.

Caso tenha sido vítima, o que fazer:

a) Verifique se o site ainda está ativo e copie seu endereço (URL);
b) Faça um print da página e do produto anunciado;
c) Providencie uma cópia do boleto ou dados bancários utilizados para o pagamento, bem como do comprovante do pagamento;
d) Em posse de todas essas informações, procure a Delegacia de Polícia mais próxima de sua casa.

5. Extorsão por Nudes ou Sextorsão

O que é?

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

O golpe ocorre da seguinte forma:

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

Como evitar o golpe:

a) Evite compartilhar fotos e vídeos íntimos;

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

Caso tenha sido vítima, o que fazer:

a) Não apague as conversas mantidas com o criminoso;
b) Se a conversa ocorreu em rede social, salve o nome do perfil e o link completo do perfil (endereço completo que aparece ao se clicar na barra de endereço);
c) Em caso de contato por telefone, faça uma relação todos os números de telefone utilizados pelo criminoso, contendo data e horário das conversas;
d) Anote os dados de eventuais contas bancárias informados pelo criminoso;
e) Em posse de todas essas informações, procure a Delegacia de Polícia mais próxima de sua casa.

GOLPES NÃO ELETRÔNICOS

► Golpe do bilhete premiado

Golpe no qual uma pessoa, normalmente aparentando origem humilde, diz ter ganho na loteria ou diz ter uma indenização a receber no banco, porém sempre há um impedimento para receber o dinheiro. Apresenta sempre diferentes versões: ou está sem o documento, ou tem uma dívida no banco, ou a agência já está fechada e a pessoa precisa viajar para outra cidade. O golpista repassa à vítima os direitos do "prêmio" em troca de um valor mais baixo do que deveria receber e desaparece.

O que fazer:

Não aceite ofertas de enriquecimento rápido e não converse com pessoas estranhas com propostas envolvendo dinheiro e bens.

► Golpe da saidinha de banco

Em razão da dificuldade que muitas pessoas idosas possuem com tecnologia, por vezes este público precisa de auxílio para o uso de caixas eletrônicos. Golpistas se aproximam de vítimas em potencial identificando-se como funcionários do banco e oferecem ajuda, coletando dados pessoais como senha e código de segurança do cartão.

O que fazer:

Não aceite ajuda de qualquer pessoa, busque sempre alguém com identificação do banco ou na dúvida, prefira o uso de caixas no interior da agência bancária.

► Golpe do empréstimo consignado

Em posse de dados pessoais de pessoas idosas, estelionatários falsificam documentos pessoais e realizam empréstimos em nome dessas pessoas.

O que fazer:

Nunca assine nada sem ler ou algum papel em branco, e desconhecendo o empréstimo procure o banco ou a delegacia de polícia mais próxima.

► Golpe do falso sequestro

Alguém liga para o celular da vítima e ouve choro e pedidos de ajuda. Diz se tratar de alguém da sua família e que esta pessoa foi sequestrada. Quem atende geralmente fica nervoso (a) e confuso, passando informações sobre a vítima em potencial. O golpista exigirá dinheiro em troca da liberdade do familiar “sequestrado”.

O que fazer:

Primeiro, não se apavore, busque auxílio de alguém para contactar o familiar supostamente sequestrado ou com pessoas próximas a ele e nunca repasse valores em dinheiro.

► Golpe do processo judicial

Uma carta ou telefonema de um escritório de advocacia avisa que o aposentado(a) tem o direito a uma causa ganha na justiça, mas que é necessário pagar os honorários e custas judiciais para que este escritório entre com a ação. Por vezes apresentam dados pessoais furtados de outras fontes para o convencimento da vítima. O depósito é realizado em contas de pessoas inexistentes ou que desconhecem o fato, nunca recebendo valores de qualquer ação.

O que fazer:

Em caso de dúvida, busque um advogado da sua confiança para verificar a possibilidade de ser verdade os fatos narrados.

► Golpes de compra no cartão de crédito

Por telefone estelionatários ligam para confirmar a compra de algo, geralmente de alto valor. E com a conversa extrai dados pessoais da vítima.

O que fazer:

Jamais confirmar informações pessoais por telefone, se precisar conferir algo consulte o seu gerente.

► Cartão retido no caixa eletrônico

Estelionatários instalam um equipamento para travar cartão magnético em caixas eletrônicos, a fim de reter os dados.

O que fazer:

Caso esteja em uma agência bancária em horário de expediente, chame um funcionário identificado. Caso ocorra em outro local ou fora da agência, ligue para um telefone do banco e cancele imediatamente o cartão.

► Carro do familiar

Por telefone, um jovem já começa chamando a pessoa de “tio” ou “tia” e diz que o carro quebrou no meio da estrada. Em seguida, pede dinheiro para o conserto. A vítima, sem graça por esquecer o nome do suposto sobrinho, acaba depositando o dinheiro.
Na dúvida, não deixe de perguntar o nome da pessoa e dos pais dela. Afinal, não há problema em não reconhecer a voz de um parente por telefone, e isso é melhor do que perder dinheiro.

► Venda Panelas/colchão

O vendedor de porta distrai a vítima e passa o cartão da vítima em valor muito superior ap valor combinado (podendo ser até dez vezes o valor real).

► Normas Gerais de Segurança:

- Mantenha-se atento quando caminhar nas ruas, tenha cuidado com pertences pessoais, como bolsa, carteira e celular. Nos casos dos homens, evite andar com a carteira no bolso de trás da calça, utilize bolsos da frente ou paletó com bolsos internos por exemplo, evitando os famosos batedores de carteira;
- Nunca aceite serviços que não pediu, mesmo que de graça ou em forma de uma gentileza;
- Nunca guarde grandes quantidades de dinheiro em casa e caso queira ter alguma reserva, mantenha-a em lugar seguro;
- Muitos golpistas escolhem suas vítimas pelos bens e objetos de valor que a vítima possui, como bolsas de marca ou joias por exemplo. Evite expô-las quando sair sozinho(a);
- Jamais pare para falar com algum desconhecido que lhe ofereça “oportunidade única” ou “chance maravilhosa de ganhar dinheiro”, mantenha os passos firmes e recuse a oferta de forma educada. Se a pessoa insistir, entre em uma loja, isso afasta pessoas indesejáveis;
- Nunca assine documentos sem lê-los e consulte alguém da sua confiança sobre questões financeiras e patrimoniais, em especial quando envolverem questões como procurações, compras, empréstimos e negociações imobiliárias, mesmo quando o documento seja apresentado por um parente;
- Tenha muito cuidado com empréstimos, mesmo que esteja precisando deles. Consulte sempre alguém que entenda de taxas bancárias para um aconselhamento;
- Não empreste seu nome ou CPF à ninguém;
- Quando sacar dinheiro, tente ocultar a ação ao máximo, pois muitos delinquentes observam pessoas no caixa para seguí-los e assaltá-los.
- Se possível, consultar um parente/conhecido sobre a transação que está realizando para verificar se há sinais de fraude.