COMISSÃO PERMANENTE DE SEGURANÇA INSTITUCIONAL DO TRIBUNAL DE JUSTIÇA DO ESTADO DO AMAZONAS

PROTEJA-SE DE GgolpES

A INFORMAÇÃO É A MELHOR FORMA DE SE PROTEGER. COMPARTILHE!

CPSI-TJAM

SUMÁRIO

GOLPE DO PERFIL FALSO NO WHATSAPP	03
GOLPE DO VOUCHER/CUPOM DESCONTO EM RESTAURANTE	04
GOLPES EM PLATAFORMAS DE COMPRA/VENDA ONLINE	05
GOLPE DOS FALSO LINKS	06
GOLPE DO FALSO INTERMEDIADOR DE VENDAS	07
GOLPE DO FALSO EMPRÉSTIMO	08
GOLPE DO AMOR	09
GOLPE DO FALSO SEQUESTRO	10
GOLPE DA TROCA DO CARTÃO	11
GOLPE DO FALSO SITE DE LEILÃO	12
GOLPE DA EXTORSÃO/NUDES	13
GOLPE DA CLONAGEM DO WHATSAPP	15
GOLPE DO BILHETE PREMIADO	17
GOLPE DO PARENTE QUE QUEBROU O CARRO	18
GOLPE DO DEPÓSITO COM ENVELOPE VAZIO	19
GOLPE DA RECUPERAÇÃO DO VEÍCULO FURTADO	21
GOLPE DA FALSA LIGAÇÃO DO BANCO	22

GOLPE DO PERFIL FALSO NO WHATSAPP

Os criminosos vinculam uma imagem de perfil da vítima, geralmente retirada do seu próprio perfil de WhatsApp ou redes sociais.

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: suporte@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.

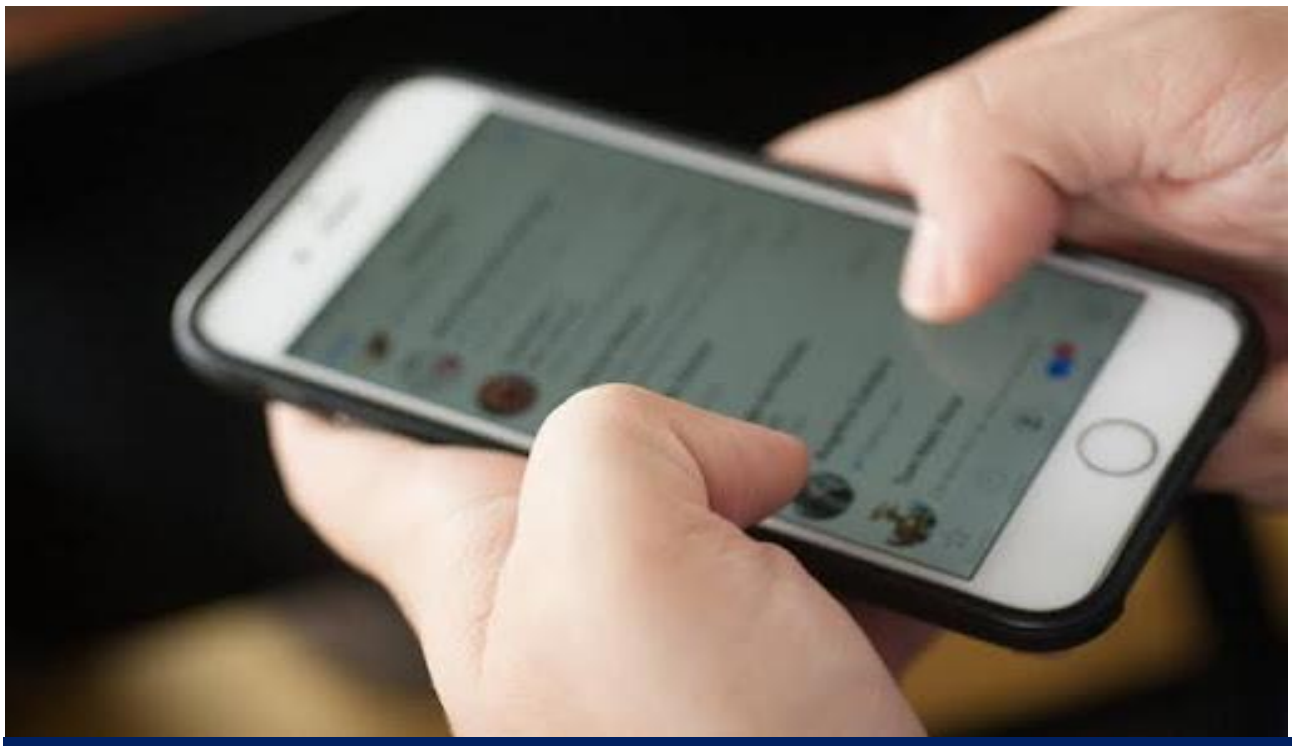
GOLPE DO VOUCHER/CUPOM DESCONTO EM RESTAURANTE

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 do 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: suporte@whatsapp.com. Também é possível denunciar clicando no número do golpe e 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.

GOLPES EM PLATAFORMAS DE COMPRA/VENDA ONLINE

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

Os criminosos, de posse do número, se passam 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 de canais oficiais da plataforma.

O QUE FAZER?

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

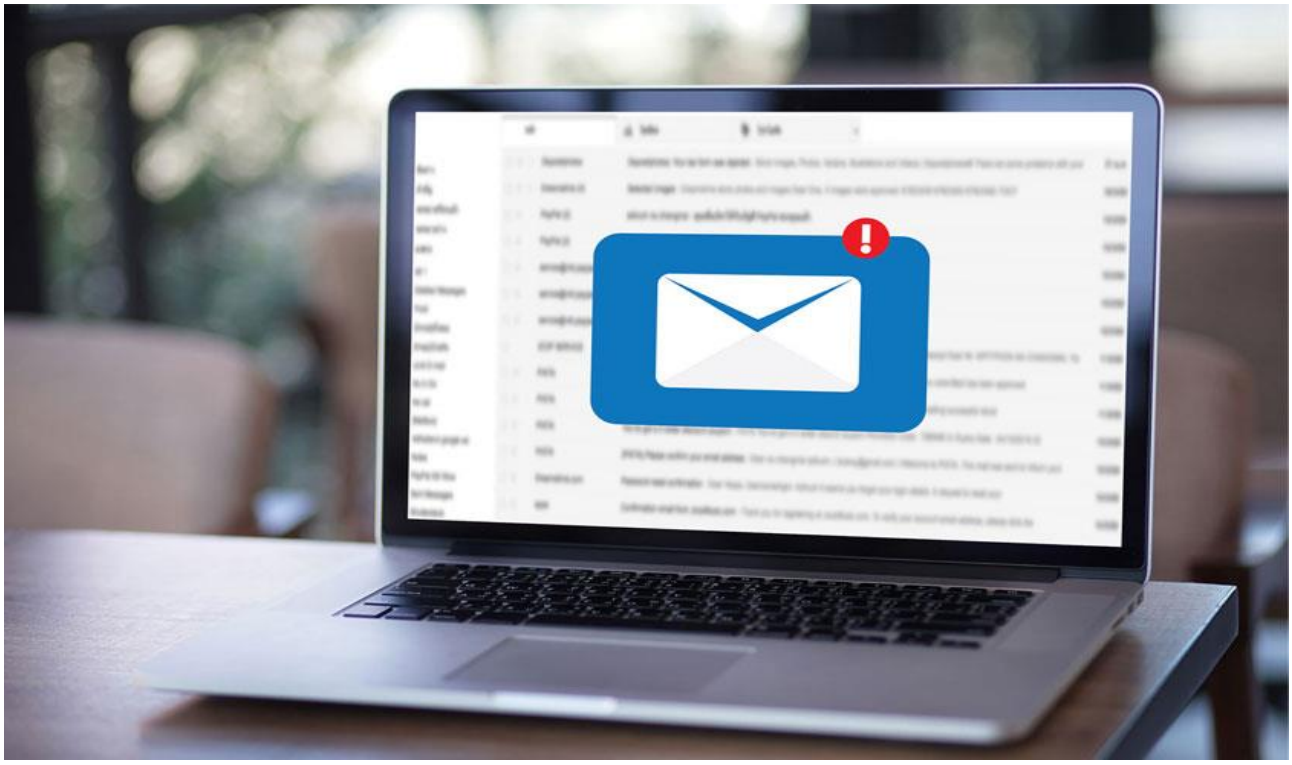
Após o envio do e-mail, realize o procedimento para recuperação da conta sucessivas vezes, para bloquear a conta e o criminoso não conseguir mais utilizá-la.

GOLPE DOS FALSOS LINKS

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

- O criminoso, então, encaminha um link malicioso dizendo que deve ser acessado para que a vítima receba o prêmio, benefício ou para evitar que a 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 da vítima.



COMO PREVENIR?

- Sempre desconfie de links encaminhados via WhatsApp ou SMS. 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.

GOLPE DO FALSO INTERMEDIADOR DE VENDAS

O criminoso consegue o telefone da vítima em sites de vendas online;

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 nessa 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 terceiro para receber o pagamento;

- Após recebido o 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;

- Busque outras formas de confirmar que realmente a pessoa que está vendendo é a mesma com quem se está fazendo 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.

GOLPE DO 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 a 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. 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 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 joias, numerários e outros itens, que supostamente foram retidos pela Receita Federal. Para retirá-la, a vítima precisa fazer um depósito de um valor, que geralmente varia de R$ 2.500,00 a R$ 4.000,00.

- 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 íntimos através mensagens.

O QUE FAZER?

- Se for vítima de extorsão, procure a **Delegacia de Polícia** mais próxima;

- Não deposite o valor solicitado.

GOLPE DO 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 os seus familiares. Solicitam, então, o telefone de outra pessoa da família, para que esta consiga o dinheiro solicitado;

- De 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 desse 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 está sendo induzido ao erro.

GOLPE DA TROCA DE CARTÃO

Os criminosos entram em contato com a vítima se passando pela instituição financeira do cartão de crédito e alegam que houve uma compra duvidosa. Com isso, solicitam que a vítima ligue no número indicado no verso do cartão para efetuar o seu cancelamento.

- O golpista continua na linha, coloca uma música similar àquela utilizada pela instituição bancária e solicita algumas informações. Sem perceber, a vítima repassa dados pessoais e a senha do cartão;

- Na sequência, o golpista informa que um funcionário da instituição irá até à residência da vítima efetuar a troca do cartão;

- De posse do cartão, os criminosos efetuam diversas transações bancárias.

COMO PREVENIR?

- Nunca forneça seus dados pessoais ou bancários via telefone;

- Caso receba ligações de instituições financeiras, dirija-se à agência bancária para confirmar a informação;

- Na impossibilidade de se dirigir até uma agência, encerre a ligação, espere alguns minutos e entre em contato com os canais oficiais do estabelecimento.

GOLPE DO FALSO SITE DE LEILÃO

Os criminosos criam sites falsos de leilão de veículos e vinculam imagens oficiais do Detran e do Tribunal de Justiça para dar veracidade.

Eles utilizam endereços on-line como: leilão-oficial, leilão-Detran-oficial, entre outros.

- A negociação ocorre via aplicativo de mensagens;

- O depósito é realizado em contas bancários de terceiros.

COMO PREVENIR?

- Nunca deposite valores antecipadamente e não caia na tentação de comprar veículos com valores abaixo do mercado;

- Veja o veículo antes de fechar o negócio;

- Vá até o endereço indicado nos sites para confirmar que se trata de um local oficial de leilão. Se for em outra cidade, entre em contato com a Polícia da cidade e tente confirmar se existe este estabelecimento.

O QUE FAZER?

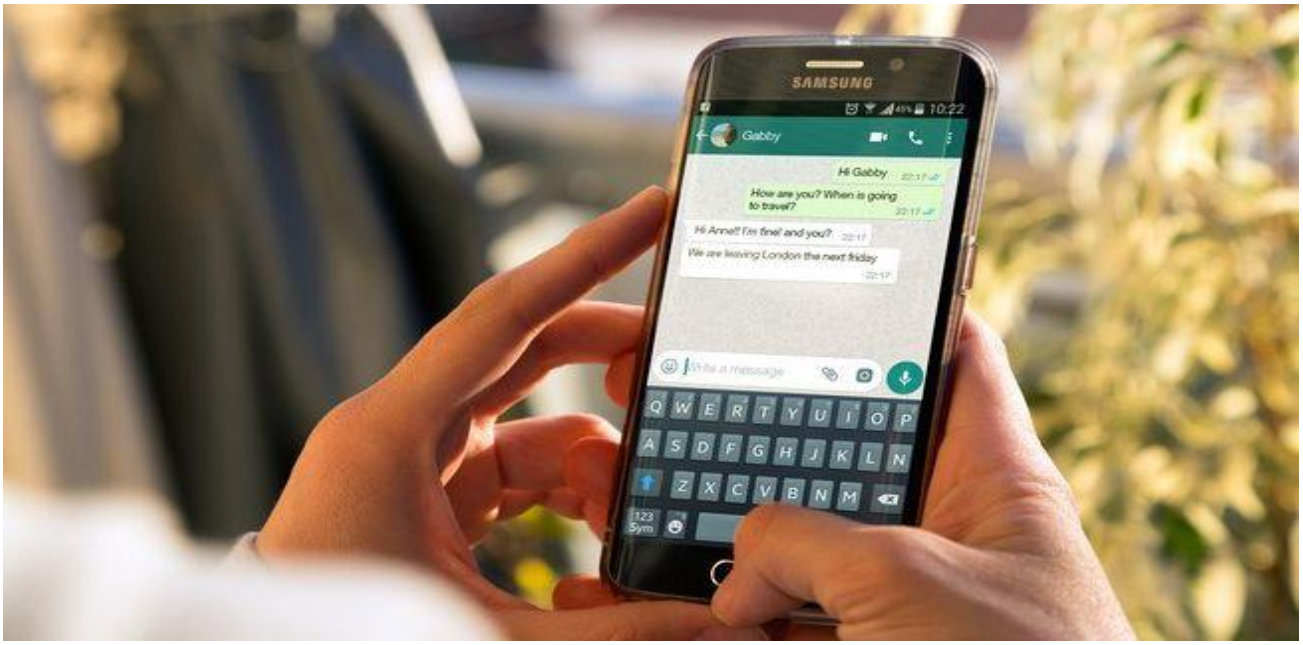
Entre em contato com o Detran da sua cidade, ou dirija-se até a Delegacia de Polícia mais próxima para confirmar a informação.

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 se 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 daí, 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, inicia 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 a exposição social cede à extorsão e acaba fazendo o depósito dos valores solicitados pelos golpistas.

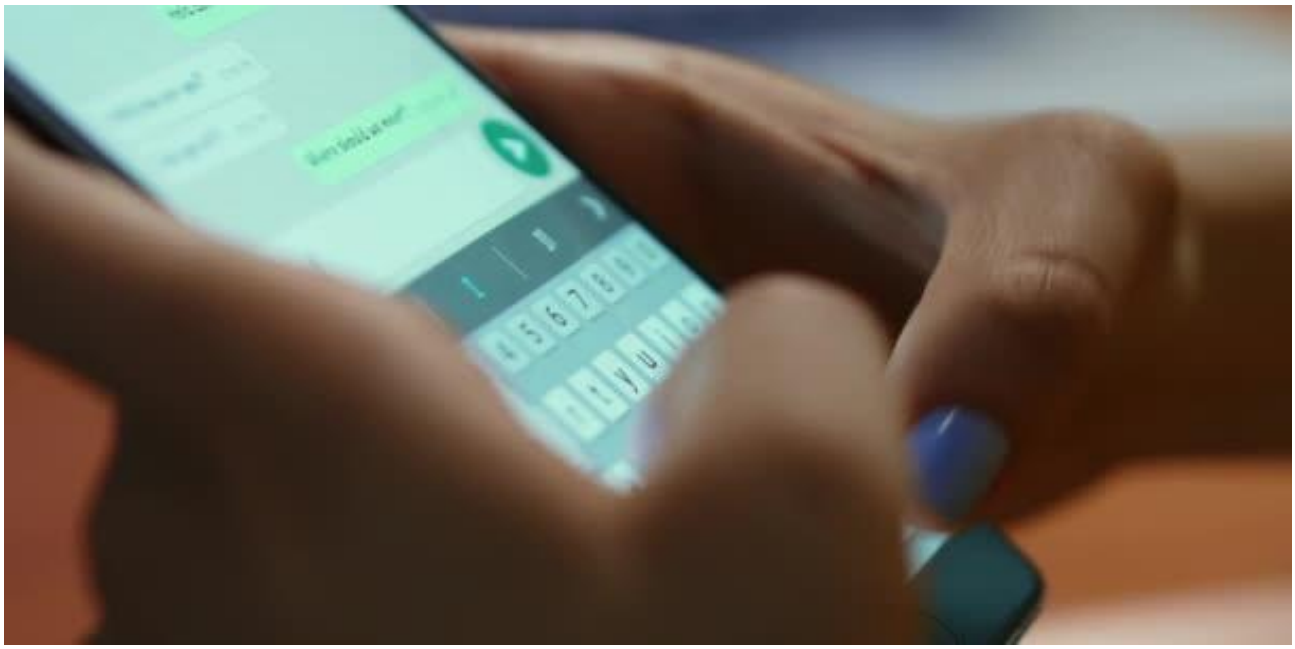
COMO PREVENIR?

- Nunca compartilhe fotos íntimas pela internet. Depois de compartilhado, a foto ou vídeo podem circular entre milhares de pessoas;

- Desconfie sempre de solicitações de amizade, através de redes sociais, de pessoas que você não conhece;

- Não forneça seus dados pessoais (como nome completo, CPF, RG, endereço, número de conta bancária e senha) para estranhos, em ligações telefônicas, mensagens SMS ou WhatsApp;

- Cuidado com operações bancárias (depósitos ou transferências em dinheiro) para pessoas do seu círculo familiar ou de amigos, principalmente quando isso é solicitado exclusivamente através do WhatsApp.



O QUE FAZER?

Se você sabe de alguém que pode estar praticando algum destes golpes, **denuncie pelo telefone 181 ou procure a Delegacia de Polícia mais próxima**;

Caso você seja vítima de algum destes golpes, procure imediatamente a Polícia Civil. Você também pode **registrar o boletim de ocorrência** através da Delegacia de Polícia Virtual do Amazonas http://www.policiacivil.am.gov.br/pagina/id/15/.

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 para que informe seus dados pessoais (nome, RG, CPF, endereço) e um código de 6 dígitos que receberá no telefone.

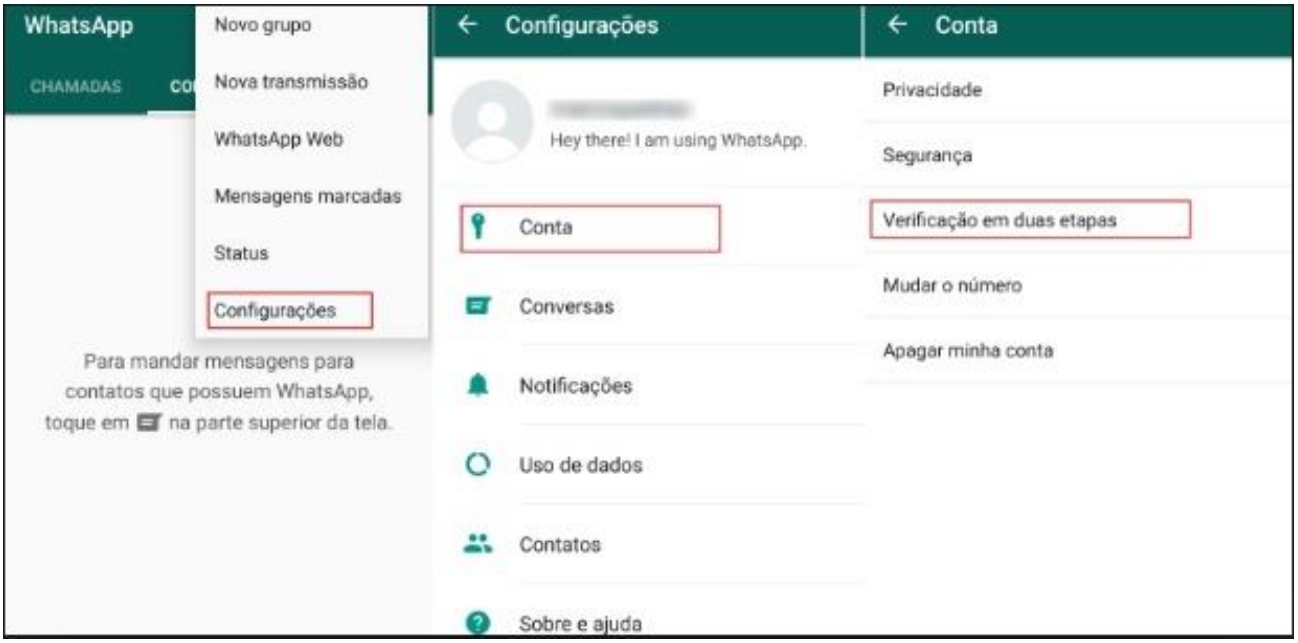
Esse código, na verdade, é uma verificação do WhatsApp, ou seja, a partir do fornecimento dessa chave o golpista desviará o WhatsApp da vítima para o aplicativo dele. Nesse caso, a vítima perde o acesso ao aplicativo de mensagens.

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 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.



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.

- 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).

GOLPE DO 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, se inicia toda uma 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 com garantia de que o humilde suposto ganhador não seja enganado e, então, entregam o "bilhete premiado".

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!**

GOLPE DO PARENTE QUE QUEBROU O CARRO

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 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;

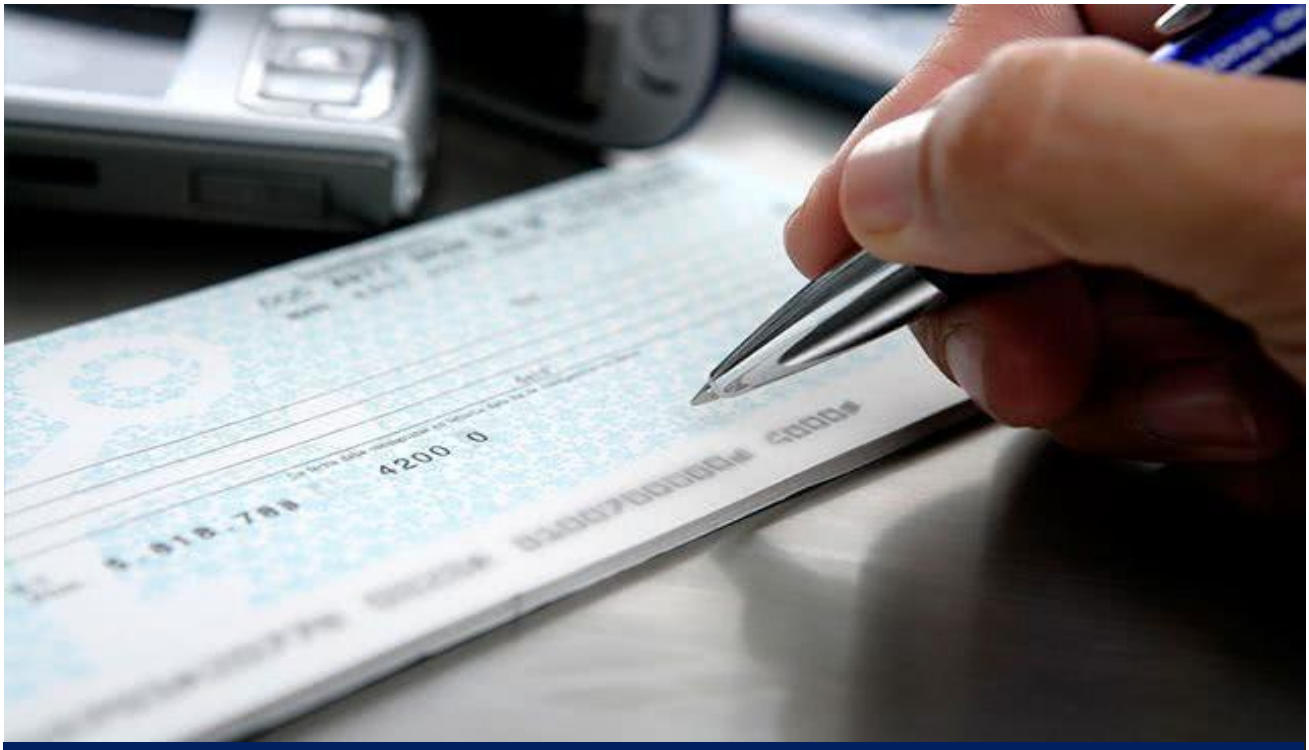
- Desligue o telefone e faça contato com o familiar que você achava estar falando. Caso a pessoa esteja realmente em apuros, você ainda poderá ajuda-la.

GOLPE DO 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 confirmação da entrada do dinheiro na conta. Isso vale para qualquer situação.

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 se passa por suposto servidor da justiça, 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.

Nenhum servidor público, de qualquer órgão que seja, requisitará serviços de "motorista" por telefone mediante pagamento de diárias antecipadas.

GOLPE DA 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 notícia 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.

O QUE FAZER?

Procure uma Delegacia de Polícia mais próxima para informar o fato.

GOLPE DA FALSA LIGAÇÃO DO BANCO

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

Este 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 de 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 na agência.

O QUE FAZER?

Procure uma Delegacia de Polícia mais próxima para informar o fato.

DENUNCIE

DISQUE 181

OS DADOS SÃO SIGILOSOS E SERÃO APURADOS POR UMA EQUIPE DE POLICIAIS