Poder Judiciário do Estado do Amapá
Tribunal de Justiça

Recomendações para o uso seguro do WhatsApp

DEPARTAMENTO DE INFORMÁTICA E TELECOMUNICAÇÕES
UNIDADE DE SERVIDORES E SEGURANÇA DA INFORMAÇÃO

A utilização
Do WhatsApp no Brasil

O **WhatsApp** é um aplicativo que está instalado no smartphone de 99% dos brasileiros, e 93% usam o aplicativo todos os dias. Uma pesquisa sobre mensageria móvel no Brasil também revela que o Telegram chega a 27% dos celulares no País, dobrando a presença no último ano, não é exagero dizer que o WhatsApp se tornou essencial para a vida de muitas pessoas.

No entanto, alguns criminosos se aproveitam dessa "dependência" e do desconhecimento da maioria da população e com golpes muito bem arquitetados roubam dinheiro, informações e praticam crimes por meio do WhatsApp.

Diante deste cenário o Departamento de Informática e telecomunicações **(DEINTEL)** através da Unidade de Servidores e Segurança da Informação **(USSI)** desenvolveu essa cartilha informativa, com o objetivo de proporcionar o esclarecimento necessário para que os usuários (serventuários e magistrados) desse aplicativo de mensagem instantânea consigam identificar e se proteger das principais fraudes praticadas.

Os golpes do WhatsApp no Brasil

Sua alta popularidade aliada ao nível de desinformação da maioria das pessoas, põe o WhatsApp e seus usuários como um dos principais alvos para ataques criminosos dos mais variados tipos.

1. Roubo do WhatsApp (Código SMS)
2. Falsificação de identidade
3. Golpe do crédito

Listamos acima os três principais golpes hoje praticados no Brasil.

Leia essa cartilha até o final e saiba como esses golpes funcionam e quais as principais ações para evita-los.

3 Golpe do crédito

Esse golpe consiste em envio de mensagens em massa para diversas vítimas, se passando por agentes financeiros anunciando créditos pré-aprovados em bancos ou fintechs. Os criminosos com propostas tentadoras de altos rendimentos, juros baixos e condições especiais conseguem facilmente enganar as vítimas.

Mas para ter o acesso a essas vantagens é necessário antecipar o pagamento de taxas. Entretanto, após pagas, a vítima jamais receberá tais benefícios.

Sempre desconfie de propostas irrecusáveis com benefícios espetaculares, não transfira ou pague nenhum valor antecipado.

Desconfie de mensagens com prêmios e recompensas que você não tenha conhecimento, ou que não tenha se cadastrado previamente.

2 Falsificação de identidade

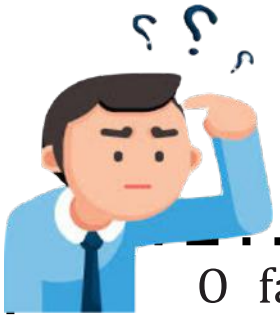
Nesse golpe o criminoso se passa por um de seus contatos e solicita que você realize uma transferência bancária (TED/DOC) a um outro favorecido.

O criminoso utiliza outros números de telefone e tenta convencer a vítima de que perdeu ou roubaram seu aparelho celular e necessita urgentemente de tal transferência e que lhe reembolsará o mais rápido possível.

Como o golpe funciona?

Através de vários mecanismos e consultas as redes sociais o criminoso consegue os contatos do alvo e sua foto de perfil do WhatsApp, ou outra foto qualquer que possa ser usada para o mesmo fim.

De posse dessas informações ele começa a enviar mensagens para os contatos adquiridos, informando que ele está provisoriamente com aquele número e solicitando que seja realizando uma transferência bancária dando alguma desculpa justificando o porquê ele próprio não realizá-la.



O fato dos números de telefone de todos os membros de um determinado grupo do WhatsApp ser uma informação pública entre os participantes, é uma maneira do criminoso conseguir os contatos do alvo, ou seja, possíveis vítimas; logo, basta ele pertencer a um ou mais grupos em comum, pois a probabilidade de algum membro deste grupo constar na lista de contatos da vítima é bastante elevada.

Como se proteger?

Feche suas redes sociais para pessoas desconhecidas

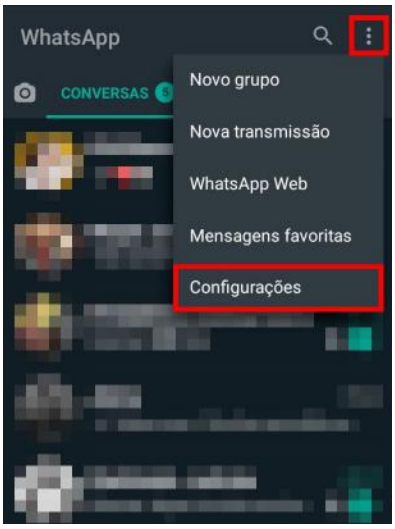
Sempre que possível configure suas redes sociais como bloqueadas para pessoas desconhecidas. Isso elimina em grande parte a possibilidade de coleta de informações que possam ser utilizadas em um golpe pelo WhatsApp.

Permita que apenas seus contatos visualizem sua foto de perfil do WhatsApp

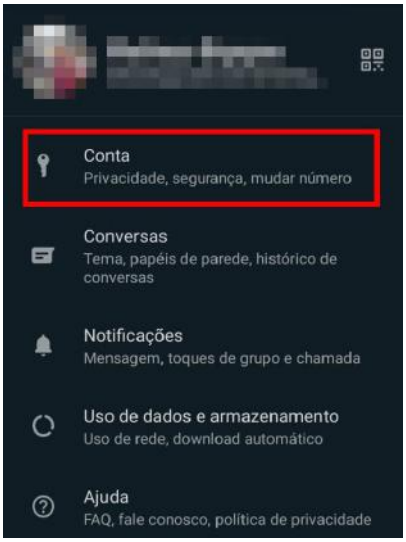
Configure seu aplicativo do WhatsApp para que somente seus contatos possam visualizar sua foto do perfil, isso impede que o criminoso saiba qual foto você está usando, podendo assim utiliza-la em alguma fraude se passando por você.

Como Configurar No Android

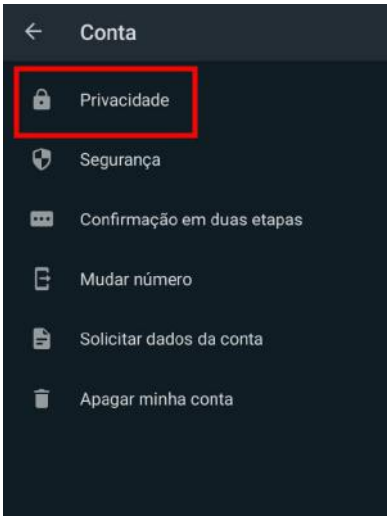
1



2

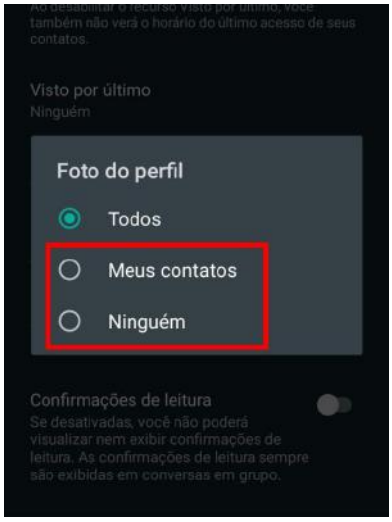


3



4

5



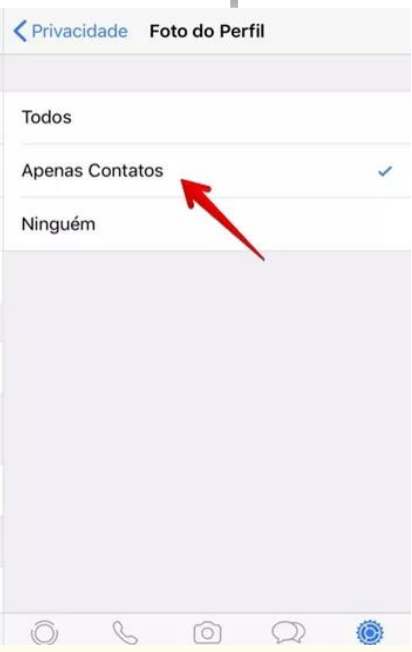
Como Configurar No Iphone

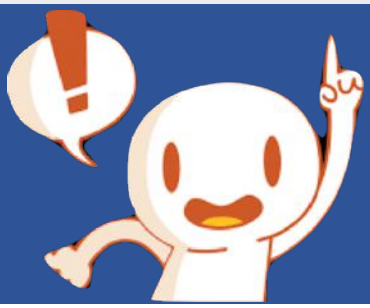
1

2

3

4





Atenção

Nessa modalidade de ataque, o criminoso não tem acesso a conta do WhatsApp do usuário forjado, ou seja, não tem acesso aos seus contatos nem suas conversas.

A vítima é a pessoa a quem se destina a mensagem, o usuário com o WhatsApp falsificado é apenas o mecanismo para a conclusão da fraude.

Desconfie de mensagens solicitando transferências bancárias ou pagamento de algum boleto, mesmo sendo de seus contatos. Sempre que puder ligue e confirme.

1

Roubo do WhatsApp (Código SMS)

Esse golpe é o mais comum e o mais nocivo se comparado aos demais, por este motivo ele está em primeiro lugar no ranking das fraudes praticadas pelo WhatsApp.

Nesse tipo de ataque o criminoso consegue acesso a conta do WhatsApp da vítima, podendo em determinados casos ter acesso a alguns de seus contatos.

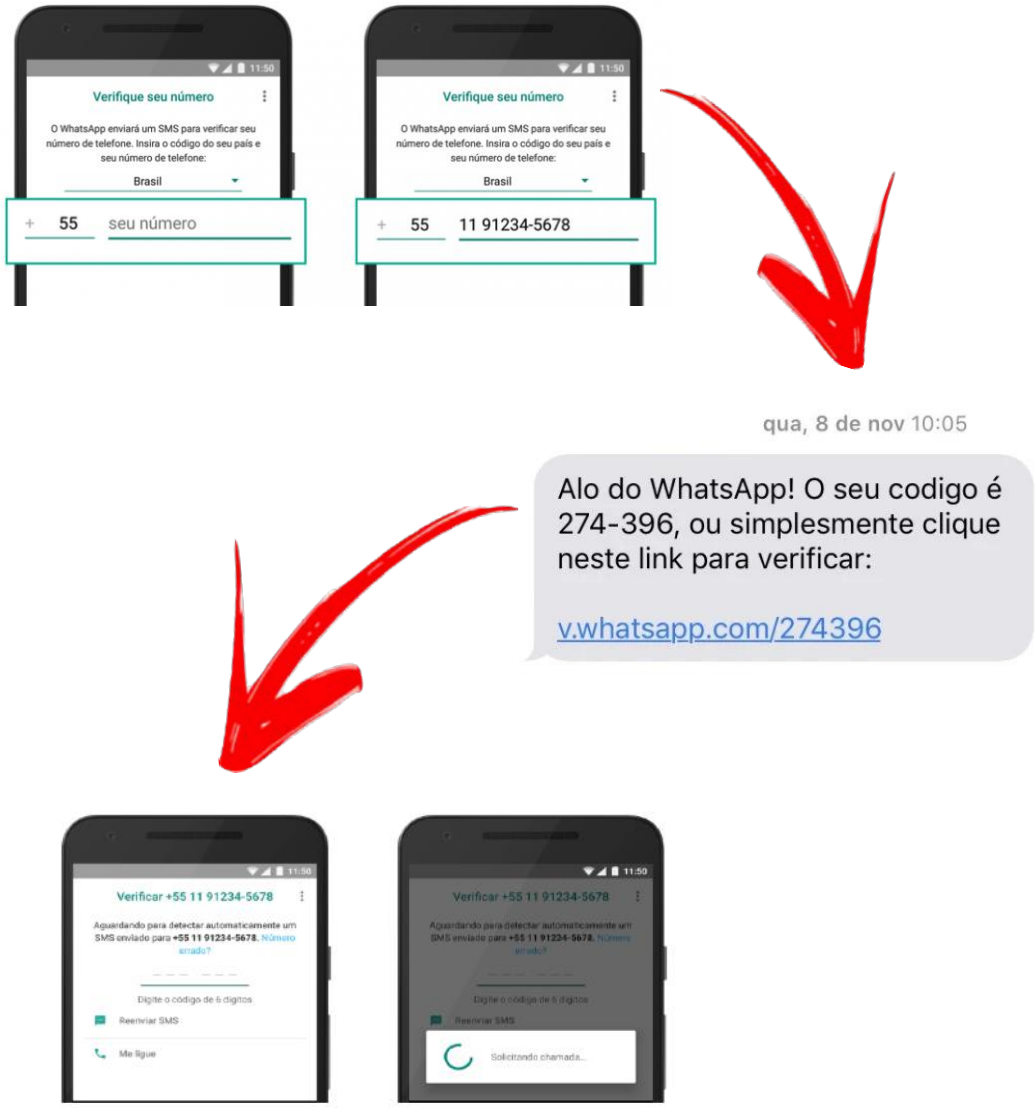
Como o golpe funciona?

O processo de configuração de qualquer dispositivo para acessar o WhatsApp passa por uma fase de verificação do número de telefone do usuário.

No momento da configuração, o usuário informa ao aplicativo qual o seu número de telefone. Para confirmar essa informação o aplicativo envia uma SMS para o número cadastrado com um código de verificação.

Esse código recebido deve depois ser inserido no aplicativo, sendo a chave para a validação do número de telefone informado no momento da configuração.

Como o golpe funciona?



Como o golpe funciona?

A possibilidade da utilização da conta do WhatsApp independente do dispositivo e do número de telefone, utilizando-se apenas de um código SMS para essa validação é o fator preponderante para o sucesso do golpe.

Então através de engenharia social (*habilidade de obter informações confidenciais utilizando técnicas de persuasão*) o criminoso solicita a vítima que informe o código SMS que acabou de receber.

Depois de receber o código SMS o criminoso se apodera da conta do WhatsApp da vítima.

Como o golpe funciona?

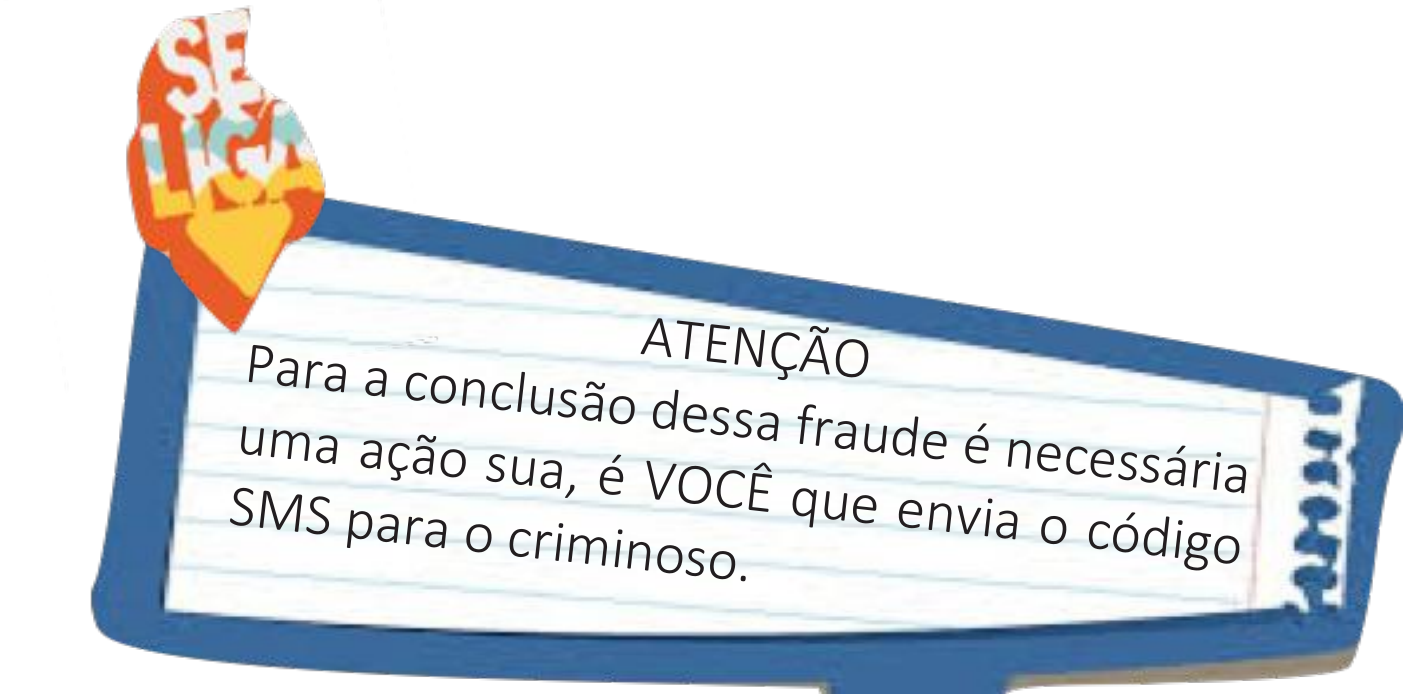
Os criminosos criam os mais diversos mecanismos para obter o código de validação SMS, incorporando diversos personagens, em diversas situações, fazendo com que o usuário acredite que o fornecimento daquele código é necessário para alguma providência relacionada à situação forjada.

Por exemplo

O criminoso entra em contato com a vítima e informa que é do ministério ou secretaria da saúde, avisando que está fazendo uma pesquisa relacionada ao covid-19, e pede que o usuário informe um código que ele enviará por SMS para validar se está falando com a pessoa certa.

Por exemplo

Ao perceber um anúncio do OLX, o criminoso entra em contato com a vítima e se passando por um atendente do aplicativo, informando que precisará validar o anúncio na plataforma e para isso será necessário informar um código SMS que será enviado.



INFORMAÇÕES

Assim que o golpe é aplicado, a vítima recebe uma mensagem do aplicativo informando que sua conta do WhatsApp está sendo executando em outro dispositivo.

Quando o golpe é aplicado o criminoso habilita a verificação em duas etapas, que impossibilita a vítima de reaver sua conta do WhatsApp em seu dispositivo.

Mesmo quando o golpe é concluído o criminoso não conseguirá ter acesso as conversas antigas, ainda que o usuário tenha configurado para realizar o backup das conversas em seu dispositivo.

A efetivação do golpe não dará ao criminoso acesso a lista de contatos do celular da vítima, porém ele terá acesso aos contatos que estejam em possíveis listas de transmissões que a vítima eventualmente tenha criado.

Como se proteger?

JAMAIS repasse números ou códigos SMS enviados para o seu dispositivo.

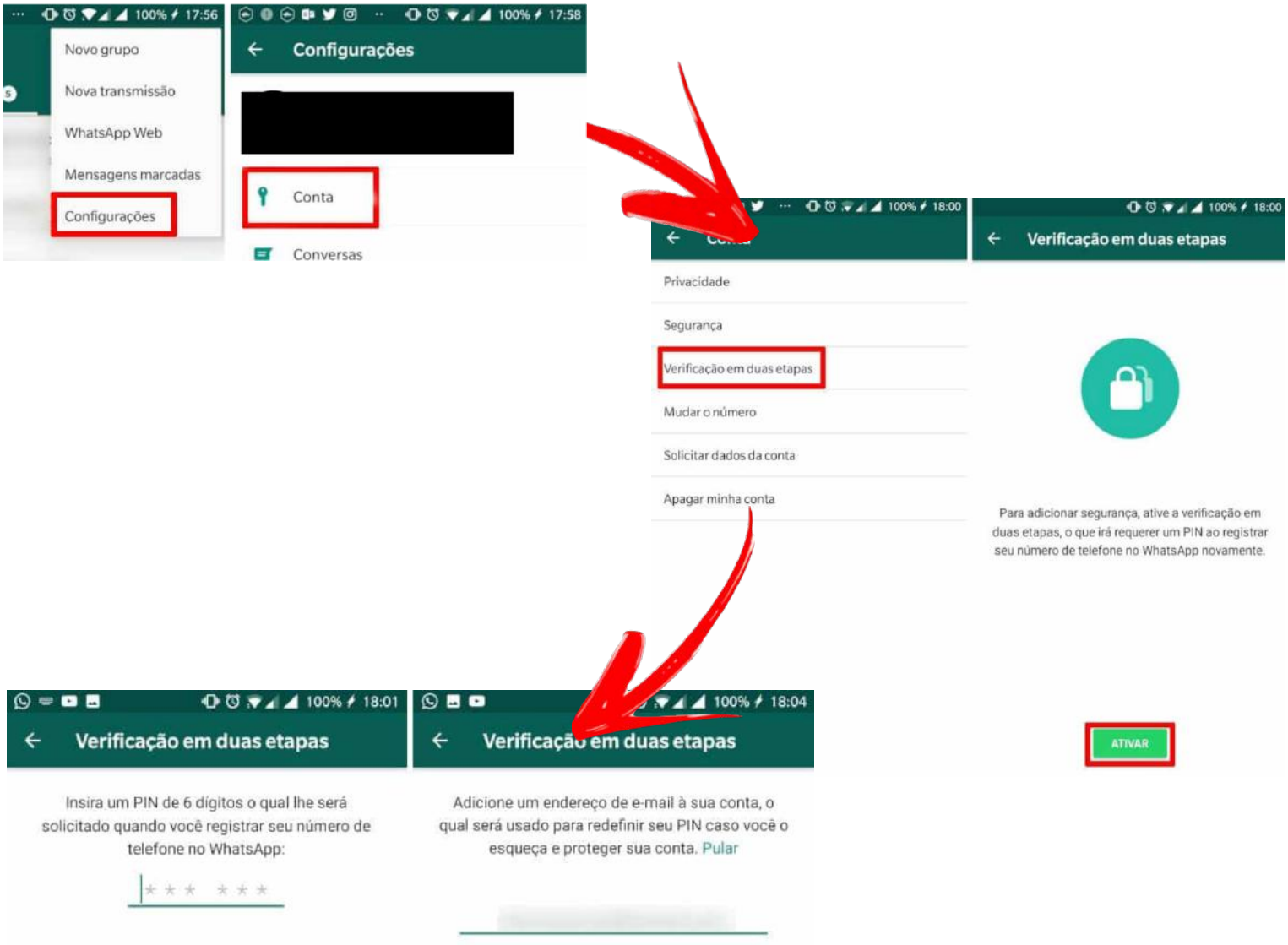
Os códigos SMS enviados para seu dispositivo devem ser única e exclusivamente utilizados em seu próprio aparelho, para a validação de algum aplicativo. **NÃO** informe qualquer código SMS sob nenhuma hipótese, se solicitado por alguém via ligação ou qualquer aplicativo.

Habilite a autenticação em duas etapas do WhatsApp em seu dispositivo.

O WhatsApp permite criar um segundo fator de validação, um código PIN criado pelo usuário, que será exigido sempre que uma conta for vinculada a outro dispositivo, aumentando ainda mais a segurança e consequentemente dificultando as ações dos criminosos.

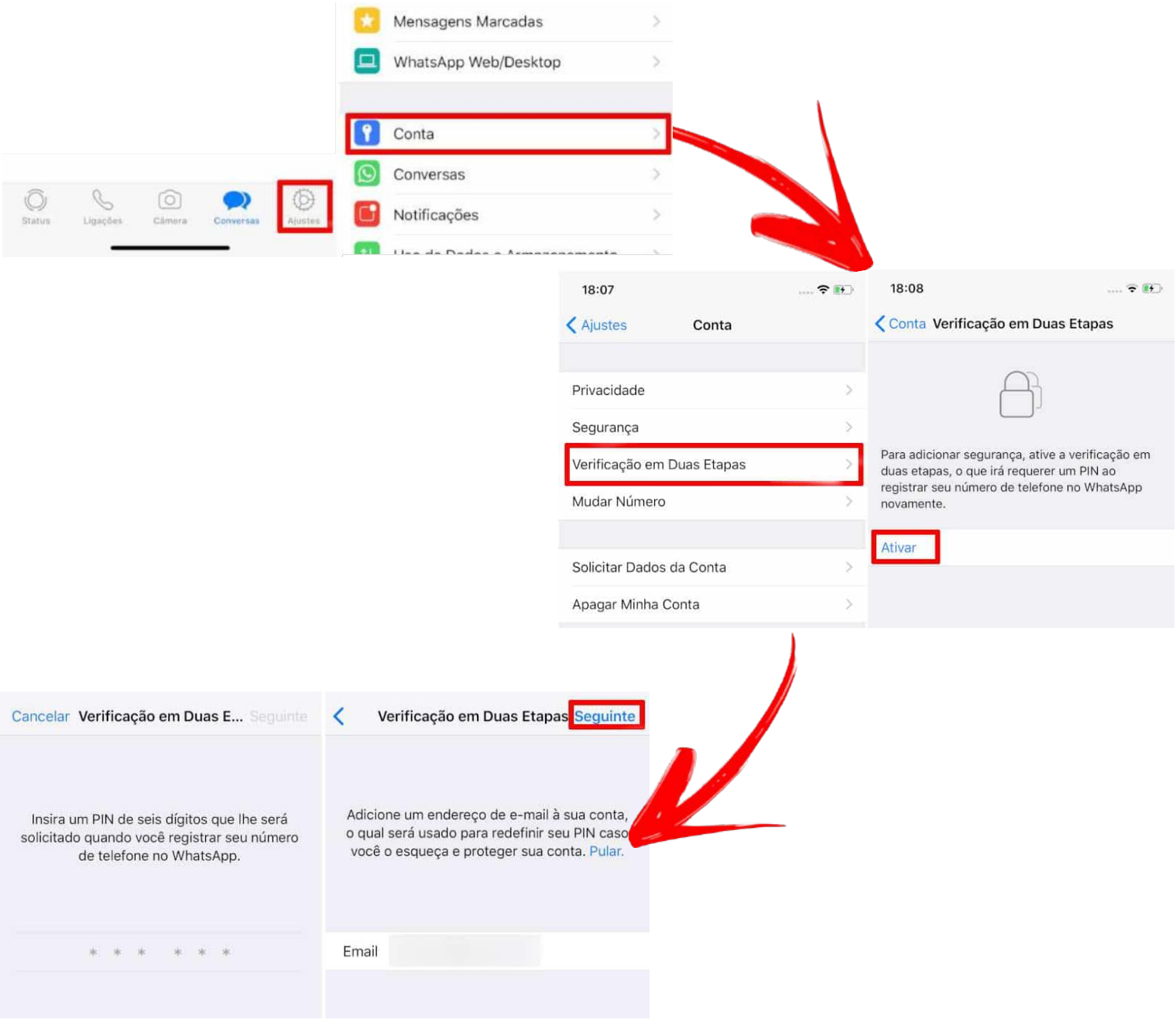
Habilitar Verificação em duas etapas

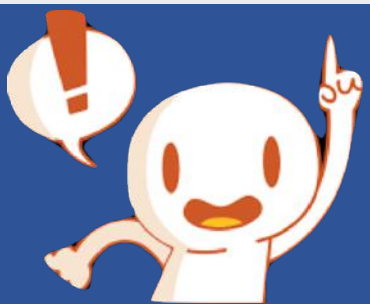
Se Liga Dicas
Android
Como Configurar



Habilitar Verificação em duas etapas

Se Liga Dicas
iOS
Como Configurar





Atenção

Nessa modalidade de ataque, o criminoso não tem acesso a conta do WhatsApp da vítima, ou seja, pode ter acesso a alguns de seus contatos, mas não de suas conversas anteriores.

A vítima é tanto a pessoa a quem se destina a mensagem, quanto o usuário com a conta do WhatsApp roubada.

Jamais Informe a terceiros senhas e códigos SMS enviados a seu dispositivo, e sempre desconfie de contatos que, através números desconhecidos, solicitem transferências em dinheiro a outros favorecidos .

Atenção

Caso você tenha sua conta do WhatsApp roubada, você pode desativa-la solicitando via e-mail para o endereço ***support@whatsapp.com*** contendo no assunto: ***"Conta capturada por fraude. Bloqueio imediato".***

No corpo do e-mail é necessário informar o motivo da solicitação do bloqueio (PERDA/ROUBO), seu nome e o número a qual sua conta estava vinculada, ou seja: +55 (XX) XXXXX-XXXX. (Padrão internacional).

Não esqueça de informar a todos os seus contatos sobre o ocorrido, eles podem está sendo vítimas de fraudes partindo de sua conta do WhatsApp roubada.

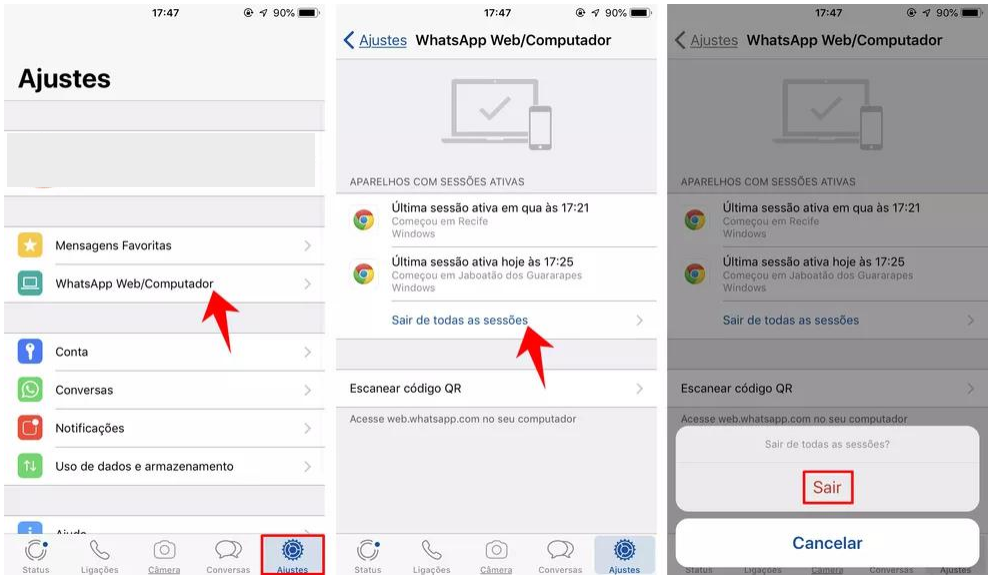
WhatsApp web

Permite um usuário se conectar ao WhatsApp através de um navegador web, possibilitando agilizar sua utilização através de um computador ou notebook ligado na internet juntamente com seu celular.

A segurança por trás dessa modalidade de acesso é a obrigatoriedade do usuário scanear com seu dispositivo um *QRCODE* que lhe é apresentado no momento do acesso.

#FicaaDica

Sempre fique atento ao número de conexões ativas de sua conta através do WhatsApp Web.



Evite utilizar sua conta através do WhatsApp web em computadores públicos ou de utilização compartilhada.

Mantenha sempre o aplicativo do WhatsApp atualizado;

Utilizar a Verificação em duas etapas;

Evite utilizar conexões com a internet públicas ou compartilhadas;

Utilize apenas a loja oficial de seu smartphone para a instalação de aplicativos (Play Store/Apple Store);

Evite participar de grupos de WhatsApp suspeitos ou com muitas pessoas desconhecidas;

Não abra ou execute arquivos ou links suspeitos;

Poder Judiciário do Estado do Amapá
Tribunal de Justiça

Departamento de Informática e Telecomunicações

O risco compromete a existência. Pratique segurança

Departamento de Informática e Telecomunicações
Diretor: Marco Antônio Campos Soares Craveiro
E-mail: marco.craveiro@tjap.jus.br

Divisão de Telemática
Diretor: Jonas Gil da Silva
E-mail: jonas.silva@tjap.jus.br

Unidade de Servidores e Segurança da Informação
Bruno Willian Silva Lima
Edna Karla Silva Melo
Francisco Boa Barbosa Júnior
Leandro Ferreira de Oliveira Bezerra
Marcelo de Souza Mendonça
Marcos Roberto Fonseca Magalhães
E-mail: ussi@tjap.jus.br

REFERÊNCIAS

- https://mpdft.mp.br/portal/pdf/imprensa/cartilhas/cartilha_sugestoes_uso_seguro_whatsapp_mpdft.pdf

- https://faq.whatsapp.com/general/security-and-privacy/

- https://www.forbes.com/sites/zakdoffman/2020/05/29/new-whatsapp-warning-as-malicious-hack-returns-heres-what-you-must-do-now/#2b781b10166a

- https://www.bbc.com/portuguese/geral-50294962