Sugestões para o uso seguro do WhatsApp

Núcleo de Combate a Crimes Cibernéticos – Ncyber

MP DFT
Ministério Público
do Distrito Federal
e Territórios

Órgãos da Administração Superior do MPDFT

Procuradoria-Geral de Justiça do Distrito Federal e Territórios
Procuradora-Geral de Justiça Fabiana Costa Oliveira Barreto

Vice-Procuradoria-Geral Jurídico-Administrativa
Procuradora de Justiça Selma Leite do Nascimento Sauerbronn de Souza

Vice-Procuradoria-Geral de Justiça Institucional
Procurador de Justiça André Vinícius Espírito Santo de Almeida

Corregedoria-Geral
Procurador de Justiça José Valdenor Queiroz Júnior

Chefia de Gabinete da Procuradoria-Geral de Justiça
Promotor de Justiça Moacyr Rey Filho

Secretaria-Geral
Promotor de Justiça Wagner de Castro Araújo

Assessoria de Políticas Institucionais
Promotor de Justiça André Luiz Cappi Pereira
Promotor de Justiça Georges Carlos Fredderico Moreira Seigneur

Ouvidoria
Promotor de Justiça Libanio Alves Rodrigues

Esta é uma publicação do Núcleo Especial de Combate aos Crimes Cibernéticos (Ncyber).
Coordenadores: Promotores de Justiça Leonardo Otreira e Rodrigo Fogagnolo.
Endereço: Eixo Monumental, Praça do Buriti, Lote 2, Sala 919,
Sede do MPDFT, Brasília-DF.
Telefone: (61) 3343-6036.

Texto e imagens:
Promotor de Justiça Leonardo Otreira

Programação visual e diagramação:
Secretaria de Comunicação do MPDFT

1ª edição digital
Agosto/2020

Apresentação

O Whatsapp tornou-se rapidamente um dos principais meios de comunicação no país. Cerca de 90% dos brasileiros já utilizam o aplicativo de mensagens, mas, infelizmente, nem sempre com boas intenções. Esta cartilha foi concebida com o intuito de auxiliar os cidadãos na identificação de possíveis golpes e informar sobre o que se deve fazer em caso de captura de conta.

O material foi preparado pelo Núcleo Especial de Combate a Crimes Cibernéticos (Ncyber), área criada pelo Ministério Público do DF e Territórios, em maio de 2019, com o objetivo de oferecer apoio qualificado às promotorias de Justiça em investigações que envolvam o uso de tecnologias cibernéticas na prática criminosa.

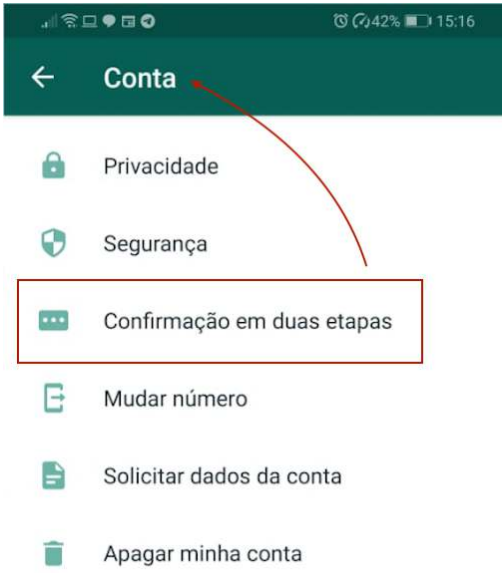
Desde a sua criação, o Ncyber tem atuado em diversas frentes, em ações judiciais ou extrajudiciais. O conhecimento partilhado nesta Cartilha tem foco preventivo e deve servir para trazer esclarecimentos quanto ao uso seguro do aplicativo Whatsapp.

Boa leitura.

Núcleo de Combate a Crimes Cibernéticos – Ncyber
Ministério Público do DF e Territórios – MPDFT

1. Golpe da "Captura de conta de *WhatsApp*" pelo código de acesso

A captura da conta de *WhatsApp* acontece quando o criminoso consegue ter acesso a conta da vítima e, passando-se por ela, solicita aos seus contatos que façam transferências bancárias a determinado favorecido.



1.1. Funcionamento do acesso ao aplicativo

Ao instalar o aplicativo do *WhatsApp* em um aparelho celular, o passo inicial é informar o número de telefone vinculado à conta.

Em situações ordinárias, o usuário informará o número do celular de sua titularidade.

Na sequência, o *WhatsApp* solicitará que seja informado o código de verificação que foi enviado por *SMS*:

Note que a mensagem informa expressamente que o código não deve ser compartilhado.

O código recebido deve ser digitado no campo correspondente. Após a digitação do código, o usuário passa a ter acesso à conta de *WhatsApp*.

1.2. Conduta do criminoso

Cientes da necessidade de obter o código para ter acesso à conta, criminosos têm criado estratégias para enganar a vítima a fim de que ela forneça essa informação.

Isso é feito por meio da chamada "engenharia social". Os criminosos normalmente procuram por alvos em sites de anúncios. Por esse método, não só conseguem o número de celular da vítima (que é normalmente fornecido para que interessados façam contato), como dele se utilizam para formar a "história de cobertura" que será contada para obtenção do código de acesso.

Nesses casos, o criminoso se passa por representante do site de anúncio utilizado pela vítima fazendo com que ela acredite que o fornecimento daquele código é necessário para alguma providência relacionada ao seu anúncio.

Por exemplo: na ligação, o criminoso informa que o anúncio foi replicado por terceiro ilegítimo, avisa que o site está fazendo a verificação para encontrar o verdadeiro anunciante e solicita o código para que se autentique o anúncio.

Após obter o código, o criminoso tem acesso à conta de *WhatsApp*. A vítima verá no seu aplicativo um aviso informando que o número foi registrado em outro telefone:

Na maioria dos casos, o criminoso ativa a verificação em duas etapas, até então desabilitada, para impedir que a vítima recupere a conta por meio do recebimento de outra mensagem de *SMS* ou ligação telefônica (ao digitar o código recebido, será pedida a senha da verificação de duas etapas, criada pelo criminoso e desconhecida pela vítima).

Para obter a vantagem ilícita, inicia diálogos com contatos da vítima, passando-se por ela, para solicitar ao interlocutor que faça uma transferência para determinada conta bancária, sob a justificativa de que o próprio solicitante não poder fazê-la naquele momento, a despeito da urgência.

1.3. Providências de segurança

Como visto, a captura da conta de WhatsApp pressupõe comportamento ativo da própria vítima, que fornece o código de verificação ao criminoso.

Recomendações:

Não forneça números recebidos por *SMS* a ninguém.

Em razão da insegurança do meio digital, nenhuma empresa adota como procedimento de verificação o fornecimento direto de códigos por meio de ligações de seus funcionários.

Habilite no seu *WhatsApp* a "Verificação em duas etapas".

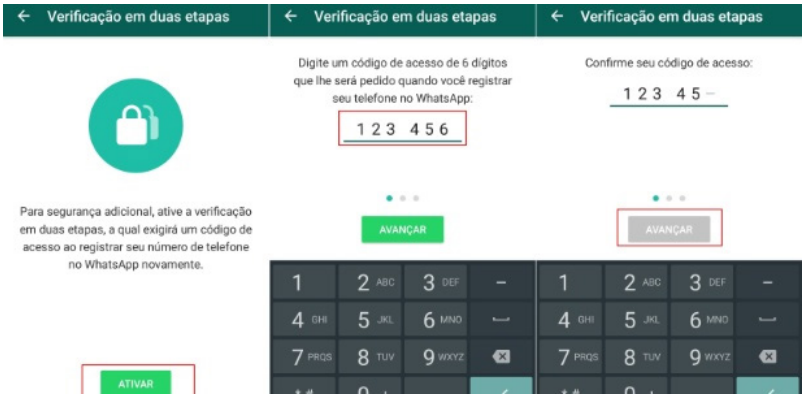
Seguindo protocolos de segurança já existentes em outras aplicações, o *WhatsApp* incorporou a chamada autenticação de dois fatores (ou "Verificação em duas etapas").

Essa providência impede que o criminoso tenha acesso à conta da vítima, mesmo na hipótese de obter o código de verificação enviado por *SMS*.

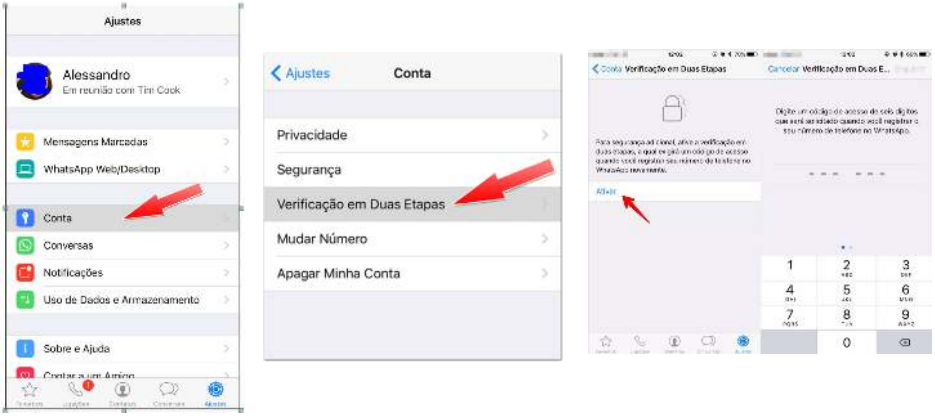
A verificação em duas etapas consiste em um código ("PIN") composto por seis números escolhidos pelo usuário.

Veja a seguir, como ela pode ser feita nos seguintes dispositivos:

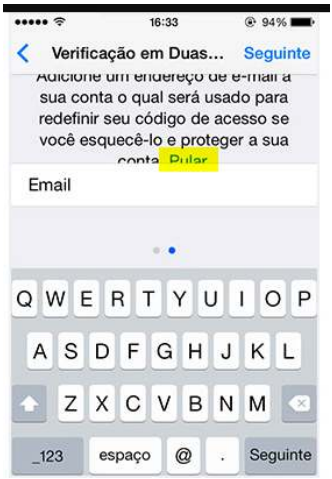
- Android



- iPhone



Atenção: ao habilitar a verificação em duas etapas, o usuário será indagado se quer oferecer um endereço de e-mail para receber o código em caso de esquecimento. A sugestão é que pulem essa etapa e não forneçam qualquer e-mail. Escolha um código do qual você irá se lembrar com facilidade (e que não seja sequencial ou de fácil obtenção – por ex.: 123456; 0001111 etc.).



Para mais informações, consulte o link abaixo:
https://faq.whatsapp.com/general/security-and-privacy/account-security-tips

Em caso de captura da conta

- Enviar e-mail para *WhatsApp*

Envie imediatamente um e-mail para "support@whatsapp.com" e "support@support.whatsapp.com", indicando:

- No título: "Conta capturada por criminoso. Bloqueio imediato".

- No corpo do texto deve constar a seguinte informação: "Meu nome é "Fulano de tal". Sou titular da conta de *WhatsApp* vinculada à linha n. +55 DDD XXXX. Essa conta foi invadida por criminoso. Bloquear imediatamente. Após, solicito desde já a recuperação da conta".

Segundo informações da empresa, a conta será bloqueada e recuperada em favor da vítima no prazo de 7 dias após o bloqueio.

Atenção: ao informar o número vinculado à conta, colocar o código +55 e o DDD (ex.: +55 61 9....-....).

- Digitar várias vezes o PIN da verificação em duas etapas

Na maioria dos casos, após receber o código da vítima e capturar a conta, o criminoso ativa a verificação em duas etapas, até então desabilitada, para impedir que a vítima a recupere por meio do recebimento de outra mensagem de *SMS* ou ligação telefônica (ao digitar o código recebido, será pedida a senha-pin da verificação de duas etapas, criada pelo criminoso e desconhecida pela vítima).

Por padrão de segurança, o *WhatsApp* informa que a inserção do PIN incorreto na etapa de verificação em duas etapas poderá levar ao bloqueio da conta.

Dessa forma, após perceber que a conta foi capturada, pode ser útil realizar novamente, pelo aplicativo, o processo de obtenção de código via *SMS* (ou ligação) e, após digitá-lo, ao ser solicitado o número PIN da verificação em duas etapas, digitar números aleatórios seguidas vezes, a fim de bloquear a conta e impedir que o usuário se comunique com os contatos.

Outras informações

É oportuno esclarecer que o criminoso, após acessar a conta de *WhatsApp* da vítima, **não tem acesso às conversas anteriores**.

Isso porque, por padrão, as mensagens estão salvas no aparelho celular da vítima. Diferentemente de outras aplicações, como o *Telegram*, o *WhatsApp* não mantém conversas salvas em servidor próprio.

Ocorre que alguns serviços – que não são prestados pelo *WhatsApp* – fornecem opções de backup das conversas em nuvem. Por exemplo: usuário de *iPhone* tem a opção de guardar na nuvem da empresa (*Icloud*) o backup das conversas do *WhatsApp*. Dessa forma, quando o usuário substitui seu *iPhone* por outro, as conversas são baixadas do *Icloud* e novamente carregadas no *WhatsApp*.

Como o criminoso, em regra, somente tem acesso à conta de *WhatsApp*, ele não consegue baixar as conversas da nuvem, uma vez que precisará do *Apple Id* e senha.

E quanto aos contatos?

Do mesmo modo, o criminoso também não tem acesso à agenda de contatos da vítima. O que acontece é que, ao "logar" na conta, os grupos que a vítima integrava, ou as listas de

transmissão por ela criadas, são carregados novamente. Assim, o criminoso passa a ter acesso aos contatos desses grupos ou dessas listas de transmissão e com eles faz contato.

2. Golpe: passando-se pela vítima com outro número

Criminosos têm adotado outra forma de se passar pela vítima e solicitar de seus contatos a realização de transferências de dinheiro.

Utilizando-se de um número de celular qualquer, diferente do da vítima, após obter informações de contatos e sua foto de perfil, o criminoso envia mensagens para os contatos da vítima, passando-se por ela e informando ao interlocutor que houve troca do número. Na sequência, solicita que seja realizada a transferência de valores a determinada conta bancária.

Nesse caso, a vítima permanece com acesso à sua conta de *Whatsapp* e sequer percebe que alguém está se passando por ela.

2.1. Conduta do criminoso

De modos que variam a depender do caso concreto, o criminoso consegue ter acesso a contatos da vítima, bem como à foto utilizada no perfil do *WhatsApp.*

A partir daí, passando-se pela vítima, o criminoso solicita aos contatos obtidos a transferência de valores para determinada conta bancária, sob a justificativa de que o próprio solicitante não pode fazê-la naquele momento, a despeito da urgência.

2.2. Providências de segurança

Mantenha suas redes sociais fechadas para pessoas não adicionadas.

Algumas redes sociais oferecem a possibilidade de que as informações do usuário sejam visíveis somente às pessoas por ele autorizadas.

Muitas vezes, o criminoso utiliza informações coletadas no perfil aberto da vítima para se passar por ela. Por isso, procure a opção de restringir o acesso aos conteúdos publicados no seu perfil.

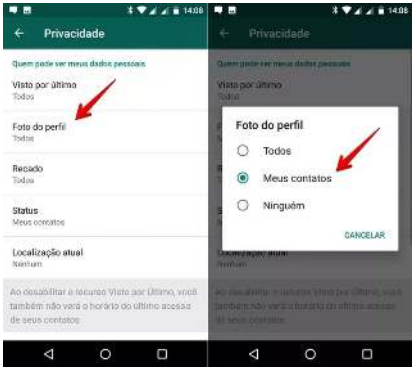
Torne sua imagem de perfil do *WhatsApp* visível apenas para os seus contatos

O *WhatsApp* oferece a opção de o usuário escolher quem pode ter acesso à sua foto de perfil. Habilite a opção que restringe a visualização aos seus contatos.

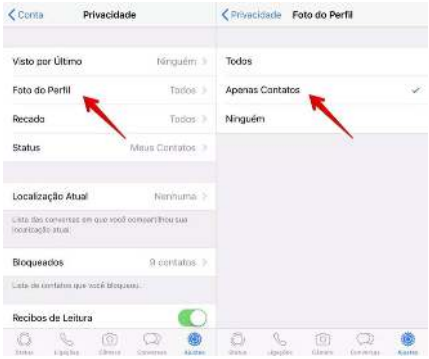
Essa providência impede que pessoas que não pertencem ao seu ciclo de amizades visualizem a foto do seu perfil e obtenham uma cópia da imagem para a prática de crimes.

Veja como proceder:

- Android



- iPhone



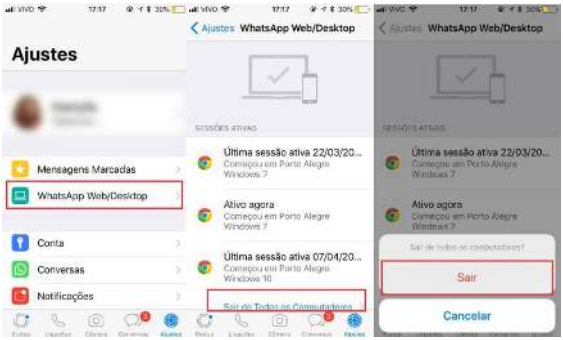
Consulte este link para mais informações:
https://faq.whatsapp.com/general/security-and-privacy/staying-safe-on-whatsapp

3. *WhatsApp Web*

A função *WhatsApp Web* permite ao usuário utilizar a aplicação pelo computador.

A ativação desse recurso exige a leitura, pela câmera do celular, do *QR Code* que aparece na tela do computador. É possível também marcar a opção de "permanecer conectado", o que fará com que o *WhatsApp Web* permaneça ativo ininterruptamente.

Tenha por hábito **sempre verificar as conexões que estão ativas,** encerrando as que não estão mais em utilização:



MPDFT
60 ANOS

MP_DFT

Ministério Público
do Distrito Federal
e Territórios

Missão do MPDFT

Promover a justiça, a democracia, a cidadania e a dignidade humana, atuando para transformar em realidade os direitos da sociedade.

Ouvidoria
MPDFT

127
www.mpdft.mp.br/ouvidoria

Eixo Monumental, Praça do Buriti, Lote 2,
Sede do MPDFT, Brasília-DF, CEP 70.091-900
Telefone: (61) 3343-9500 | www.mpdft.mp.br

mpdftoficial mpdftoficial mpdft mpdftoficial