ORIENTAÇÕES SOBRE UTILIZAÇÃO SEGURA DO WHATSAPP

COMO PREVENIR FRAUDES PELO WHATSAPP E O QUE FAZER SE VOCÊ FOR VÍTIMA

HIGOR VINICIUS NOGUEIRA JORGE

HÉLIO MOLINA JORGE JÚNIOR

VERSÃO 3/2021

Sumário

OS AUTORES

HIGOR VINICIUS NOGUEIRA JORGE é Delegado de Polícia e professor da Academia de Polícia na Polícia Civil do Estado de São Paulo, titular da cadeira 30 da Academia de Ciências, Artes e Letras dos Delegados de Polícia do Estado de São Paulo e membro da Associação dos Delegados de Polícia do Estado de São Paulo. Também é membro da Associação Internacional de Informática Forense (Asiif), da Associação Internacional de Investigação de Crimes de Alta Tecnologia (Htcia) e da Associação Internacional da Polícia (Ipa - Brasil), professor de inteligência cibernética do Ministério da Justiça, professor da pós-graduação Advocacia no Direito Digital e Proteção de Dados na Escola Brasileira de Direito (Ebradi), professor da pós-graduação em Compliance e Direito Anticorrupção e da pós-graduação em Direito Político e Eleitoral do Complexo de Ensino Renato Saraiva (Cers), professor da especialização Direito Digital Aplicado e Compliance Digital do MeuCurso, professor da especialização da Associação dos Diplomados da Escola Superior de Guerra, membro do grupo de estudos de direito digital e compliance da Federação das Indústrias do Estado de São Paulo (Fiesp) e investigador digital forense certificado pela REDLIF. Em 2017, 2019 e 2020 foi escolhido na categoria “Jurídica” entre os melhores Delegados do Brasil pelo Portal Nacional dos Delegados & Revista da Defesa Social. É coautor das obras “Manual de Interceptação Telefônica e Telemática” e “Fake News e Eleições – O Guia Definitivo” e coordenador dos livros “Enfrentamento da Corrupção e Investigação Criminal Tecnológica”, “Tratado de Investigação Criminal Tecnológica”, “Manual de Educação Digital, Cibercidadania e Prevenção de Crimes Cibernéticos” e “Legislação

Criminal Comentada", publicados pela editora Juspodivm, além ser autor/coautor de outras obras jurídicas. Possui o site www.higorjorge.com.br.

HÉLIO MOLINA JORGE JÚNIOR é engenheiro de materiais formado pela Universidade Federal de São Carlos – UFSCAR, especializando em direito penal e processo penal pelo MeuCurso e coautor das obras "Fake News e Eleições – O Guia Definitivo", "Enfrentamento da Corrupção e Investigação Criminal Tecnológica", "Tratado de Investigação Criminal Tecnológica" e "Manual de Educação Digital, Cibercidadania e Prevenção de Crimes Cibernéticos", publicados pela editora Juspodivm, além ser autor/coautor de outras obras jurídicas.

I. INTRODUÇÃO

Muita gente tem sofrido prejuízos em virtude de fraudes eletrônicas, sendo que parcela substancial destas fraudes são praticadas por intermédio do WhatsApp.

Nesse contexto, temos ressaltado que as pessoas precisam se conscientizar da importância do uso ético e seguro da plataforma e de outros recursos tecnológicos.

É possível observar que criminosos estão se aproveitando da intensa utilização dos recursos tecnológicos decorrente da pandemia para obter vantagens indevidas das vítimas, muitas vezes clonando seus celulares, criando perfis com as fotos das vítimas em redes sociais para pedir dinheiro ou convencendo as pessoas a clicarem em links que permitam fazer download de arquivos maliciosos que, se executados, monitoram tudo que é feito no computador, inclusive as senhas digitadas ou a transmissão de outras informações sensíveis.

Também são comuns links que direcionem o internauta a acessar sites de comércio eletrônico ou de leilões de veículos semelhantes aos verdadeiros. Os produtos são adquiridos e pagos pelas vítimas, todavia nunca serão recebidos.

Outra fraude muito comum envolve a criação de um site semelhante ao site de instituições financeiras, sendo que a vítima preenche seus dados, como se estivesse acessando sua conta bancária. Depois de um tempo, quando a vítima acessa seu extrato, observa que foi transferido dinheiro de sua conta.

Nas próximas linhas abordaremos as modalidades de "clonagem do WhatsApp".

II. MODALIDADES DE CLONAGEM

a. CLONAGEM DE WHATSAPP BASEADA NO “SIM SWAP” E NA ENGENHARIA SOCIAL[1]

O WhatsApp[2] é um aplicativo de *smartphones* utilizado para troca de mensagens instantâneas, chamadas de voz, bem como o envio de fotos, áudios, vídeos e documentos, por intermédio de uma conexão com a internet, sendo considerado uma das principais ferramentas da atualidade para a comunicação entre as pessoas[3].

---

[1] Importante esclarecer que se trata da versão **1/2021**, uma versão incipiente e muito resumida sobre o assunto. Conforme forem acrescentadas outras informações e corrigidos eventuais erros serão divulgadas novas versões.
[2] Além do WhatsApp, outros aplicativos de comunicação, como por exemplo, o Telegram, precisam ter a verificação em duas etapas ativado para evitar dissabores ou até mesmo prejuízos para seus usuários.
3 JORGE, Higor Vinicius Nogueira. **Investigação Criminal Tecnológica**. Volumes I e II. Rio de Janeiro: Brasport. 2018. p. 07.

Nos últimos tempos notou-se um incremento na quantidade de fraudes[4] praticadas por intermédio do aplicativo e, por isso, é necessário conscientizar as pessoas sobre a necessidade de adoção de alguns procedimentos de segurança na utilização do WhatsApp, bem como o que deve ser feito pelas vítimas caso sofram esse tipo de fraude.

A fraude eletrônica denominada “SIM Swap” é praticada por aquele criminoso que, em conluio com funcionários de operadoras ou em posse de documentos falsos da vítima, transfere para seu celular o número utilizado pela vítima e passa a utilizar o WhatsApp dela. Uma característica desse tipo de fraude é que a vítima não consegue mais utilizar a linha telefônica e o WhatsApp, enquanto o criminoso se passa por ela para solicitar dinheiro dos seus contatos.

Em resumo, o delinquente subtrai (clona)[5] o número de celular da vítima, habilita a conta do WhatsApp dela no seu celular e passa a pedir dinheiro para todos os seus contatos.

Existe outra modalidade de fraude praticada por intermédio do WhatsApp cujo criminoso não realiza a clonagem da linha telefônica. Nestes casos a vítima continua usando a sua linha telefônica e o criminoso utiliza a denominada “engenharia social” para convencer a vítima a instalar arquivos maliciosos ou a fornecer informações sensíveis.

---

[4] Geralmente os autores dessas fraudes incorrem no crime de estelionato, furto mediante fraude ou falsa identidade, dependendo dos fatos.
5 Também denominado: “Sequestro de WhatsApp”.

A “engenharia social”

> É a utilização de um conjunto de técnicas destinadas a ludibriar a vítima, de forma que ela acredite nas informações prestadas e se convença a fornecer dados pessoais nos quais o criminoso tenha interesse ou a executar alguma tarefa e/ou aplicativo. Cabe destacar que geralmente os criminosos simulam fazer parte de determinada instituição confiável, como bancos, sites de grandes lojas, órgãos do governo ou outros órgãos públicos para que a vítima confie nos falsos dados apresentados, o que, na verdade, será a isca para que sejam fornecidas as referidas informações. Enquanto certas ameaças cibernéticas utilizam vulnerabilidades localizadas em uma rede ou servidor, na engenharia social o criminoso concentra-se nas vulnerabilidades que porventura a vítima possa ter e/ou apresentar frente a determinadas situações do seu cotidiano. Nestas situações o ponto nevrálgico é a falta de conscientização do usuário de computador sobre os perigos de acreditar em todas as informações que chegam até ele[6].

Para o criminoso conseguir usar o WhatsApp da vítima em seu celular será necessário convencer a vítima a informar o código de segurança que ela recebeu em seu celular, via SMS. Sem o código de segurança não é possível utilizar (clonar) o WhatsApp da vítima. O criminoso

[6] WENDT, Emerson; JORGE, Higor Vinicius Nogueira. Crimes Cibernéticos – Ameaças e Procedimentos de Investigação. 2. ed. Rio de Janeiro : Brasport, 2013.

costuma utilizar a engenharia social para convencer a vítima a informar o código de segurança que ela recebeu em seu telefone via SMS.

Exemplo: A vítima recebe uma mensagem por um aplicativo de comunicações com a informações de que foi sorteada e ganhou um notebook, um carro ou outro bem. Além disso, ela é informada que um código de confirmação foi enviado para o celular dela, via SMS, para poder receber o prêmio. Caso a vítima informe o código de confirmação para a suposta empresa de sorteios, sua conta de WhatsApp será clonada. Caso a vítima tenha configurado a verificação em duas etapas, conforme será demonstrado posteriormente, o criminoso terá dificuldades para sua empreitada delituosa.

Outra fraude muito comum atinge aqueles que utilizam plataformas de vendas pela internet. O vendedor recebe mensagem da suposta plataforma de comércio eletrônico, como Mercado Livre, Olx ou Webmotors, sendo informado que seu anúncio será excluído caso não informe um código de segurança que receberá nos próximos minutos. Em seguida, o criminoso tenta instalar em seu celular uma conta de WhatsApp com o número da vítima, a vítima recebe o código via SMS e informa referido código ao criminoso que, em posse do código, passa a utilizar o WhatsApp da vítima, principalmente visando convencer os amigos dela para que transfiram dinheiro para uma conta, que geralmente pertence a uma pessoa que nem sabe sobre a utilização indevida de sua conta.

i. PREVENÇÃO

A primeira sugestão de prevenção reside em nunca informar para outras pessoas eventuais códigos de segurança recebidos via SMS.

Outra medida de segurança indicada reside em ativar a verificação em duas etapas (autenticação de dois fatores) do WhatsApp, que permitire cadastrar um e-mail e um PIN de seis dígitos[7] que será exigido sempre que for necessário verificar a conta.

Importante memorizar o PIN cadastrado e saber que constantemente o usuário terá que inserir o PIN para utilizar o aplicativo e, se for necessário, futuramente, precisará do e-mail para restaurar sua conta.

De acordo com informações extraídas do site do WhatsApp[8]:

> A Verificação em duas etapas é um recurso opcional para adicionar ainda mais segurança à sua conta. Ao ativar a verificação em duas etapas, qualquer tentativa de verificação do seu número de telefone no WhatsApp terá de ser acompanhada por um PIN de seis dígitos criado por você através deste recurso.

---

[7] Importante não escolher um PIN que tenha relação com a vítima, como por exemplo, a sua data de nascimento ou outro número fácil de ser descoberto pelo criminoso, pois ele pode utilizar “engenharia social” para obter suas informações sensíveis.

[8] WhatsApp. **Utilizando a verificação em duas etapas**. Disponível em: < https://faq.whatsapp.com/pt_br/android/26000021>. Acesso em: 19 maio 2019.

> [...]
>
> Ao ativar este recurso, você terá a opção de inserir seu endereço de email. Este endereço de email será utilizado para que o WhatsApp possa lhe enviar um link para desativar a verificação em duas etapas caso você esqueça o PIN e também para ajudar a proteger a sua conta. Nós não verificamos este endereço de email para confirmar sua autenticidade. Recomendamos que você forneça um endereço de email autêntico, pois assim você reduz o risco de ficar sem acesso à sua conta caso esqueça o PIN.
>
> Importante: Se você receber um email para desativar a verificação em duas etapas sem tê-lo solicitado, não clique neste link. Outra pessoa pode estar tentando registrar o seu número no WhatsApp.
>
> Se você tiver a verificação em duas etapas ativada, não será possível reverificar seu número no WhatsApp dentro de um período de 7 dias após você ter usado o WhatsApp sem o seu PIN. Por isso, se você esquecer o seu próprio PIN e não tiver fornecido um email para desativar a verificação em duas etapas, não será permitido reverificar seu número no WhatsApp dentro do período de 7 dias após ter usado o WhatsApp por último. Após estes 7 dias, será permitido reverificar seu número no WhatsApp sem o PIN, mas você perderá todas as mensagens pendentes ao reverificar porque elas serão apagadas. Se a reverificação for feita após 30 dias desde a última vez que você utilizou o WhatsApp e sem o seu PIN, sua conta será apagada e uma nova será criada assim que o processo for realizado.

A configuração da verificação em duas etapas possui peculiaridades, conforme o modelo de celular. Abaixo são apresentadas, de forma sintética, as informações para a habilitação da verificação em duas etapas nos sistemas operacionais Android e iOS.

1. VERIFICAÇÃO EM DUAS ETAPAS NO SISTEMA OPERACIONAL ANDROID

Acesse o WhatsApp, toque em “Configurações”, clique em “Conta”, em seguida, “Confirmação em Duas Etapas” e “Ativar”, para que o e-mail e o PIN sejam inseridos.

2. VERIFICAÇÃO EM DUAS ETAPAS NO SISTEMA OPERACIONAL IOS

Acesse o WhatsApp, toque em “Ajustes”, clique em “Verificação em Duas Etapas”, em seguida, “Ativar” e inserir o e-mail e PIN.

Importante consignar que o criminoso, em posse do código de segurança do WhatsApp da vítima, sabendo que não consegue clonar o WhatsApp dela em razão de estar habilitada a dupla verificação, costuma tentar convencer a vítima a informar o PIN de segurança escolhido quando habilitou a dupla verificação ou pode viabilizar o envio, por parte do WhatsApp, de um link para o e-mail da vítima que, se clicado por ela, desabilita a dupla verificação.

b. FALSA CONTA DO WHATSAPP (UTILIZAÇÃO DA FOTO E DOS DADOS DO WHATSAPP DA VÍTIMA PARA PEDIR DINHEIRO AOS FAMILIARES E AMIGOS)

Outro tipo de fraude que tem ocorrido com frequência consiste na utilização da foto e dos dados pessoais da vítima para pedir dinheiro para seus familiares e amigos. Nestas hipóteses, o criminoso habilita uma conta de WhatsApp com um número qualquer e utiliza foto/dados de um alvo para solicitar dinheiro a pessoas próximas. Cabe esclarecer que o criminoso utiliza informações das redes sociais da vítima ou de determinados bancos de dados privados para identificar e obter os contatos destas pessoas que receberão o pedido de dinheiro, via transferência bancária ou PIX.

Em uma parte considerável destes golpes o criminoso entro em contato com as vítimas informando que havia trocado o número do WhatsApp, sendo esse tipo de comentário um outro indicativo de fraude.

i. PREVENÇÃO

Para evitar essa modalidade de burla é recomendável conversar sobre o assunto com pessoas próximas para que não façam transferências quando solicitado pelo WhatsApp ou por outras redes sociais. Também é recomendável confirmar por outros meios a veracidade da solicitação.

A pressa da vítima é um fator que facilita a atuação do delinquente, sendo importante que a pessoa que recebe a solicitação de dinheiro reflita com calma antes de realizar a transferência para o solicitante e,

se possível, compartilhe as dúvidas com outras pessoas para que ajudem confirmar os fatos.

Outra questão recomendável é a configuração da privacidade da conta do WhatsApp para que a foto do perfil seja vista apenas pelos contatos do usuário (Configurações – Conta - Privacidade – Foto do Perfil – Meus contatos).

Importante também tomar muito cuidado com as informações e mídias publicadas nas redes sociais que atraiam a atenção de criminosos ou que facilitem eventuais golpes praticados por eles. É recomendável habilitar a configuração de privacidade que permita que as publicações da vítima sejam acessadas somente pelos seus amigos.

Muitas fraudes envolvem a utilização do PIX e se observar que aumentou a possibilidade de prejuízos, considerando que permite, em qualquer horário, de forma rápida e simplificada, a realização de transação financeira de modo que facilita a ação do criminoso e muitas vezes impede que a vítima tenha tempo hábil de bloquear a transação.

III. MEDIDAS REATIVAS

Geralmente a vítima percebe que não consegue mais utilizar sua conta de Telefone/WhatsApp ou é avisada por pessoas que sua conta está sendo utilizada para pedir dinheiro em seu nome ou que sua foto/dados estão sendo usados em um número desconhecido de WhatsApp habilitado pelo criminoso.

Caso o número de celular tenha sido subtraído, é necessário se dirigir a empresa de telefonia, para que o seu número seja devolvido e, por consequência, seja possível voltar a utilizar o WhatsApp.

Caso não for possível se dirigir a operadora de telefonia, é recomendável ligar na operadora e solicitar o bloqueio do número de telefone. Com o número de telefone bloqueado, o criminoso não conseguirá verificar a conta no telefone, em razão de não receber o código por SMS ou ligação telefônica[9].

Caso o criminoso não tenha ativado o PIN da dupla verificação do WhatsApp, depois que a vítima voltar a utilizar o seu número de telefone, bastará instalar novamente a conta do WhatsApp no referido telefone, em razão da linha telefônica ter sido devolvida. Essa é a maneira mais rápida da vítima voltar a usar a sua conta de WhatsApp clonada por criminosos.

Cabe esclarecer que o WhatsApp só pode permanecer ativo com um número de telefone em um aparelho de cada vez, exceto quando ocorre o espelhamento. Exemplo: O criminoso espelha a conta da vítima por intermédio do WhatsApp Web e se passa por ela. O exemplo é incomum, porque seria muito fácil para vítima saber que foi habilitado o WhatsApp Web e acompanhar tudo que o criminoso está fazendo,

[9] É necessário esclarecer que o bloqueio do número de telefone utilizado pelo criminoso e a desativação do serviço de telefonia não impossibilitará o criminoso de continuar utilizando a conta de WhatsApp da vítima por intermédio de uma rede Wi-Fi. Por isso, é necessário enviar o e-mail para o WhatsApp com o objetivo de desativar temporariamente a conta, conforme será exaustivamente demonstrado nas páginas seguintes.

utilizando o WhatsApp Web, tendo em vista que a vítima continuará tendo acesso a sua conta (ambos terão acesso a conta – WhatsApp convencional e WhatsApp Web).

Importante salientar que não é comum a clonagem da linha telefônica da vítima para poder clonar a conta do WhatsApp. Geralmente, os crimes praticados são aqueles baseados na clonagem da conta do WhatsApp em razão do fornecimento de código de segurança. Também é comum a utilização de Conta de WhatsApp Falsa. Neste caso, o criminoso passa a usar a foto e os dados da vítima em um número qualquer.

Criminosos costumam convencer a vítima a fornecer o código de segurança, sendo que a vítima perde o acesso a sua conta do WhatsApp e o criminoso passa a utilizá-la. Quando a vítima nota esse fato é recomendável reinstalar o WhatsApp no seu celular e inserir os dados do seu número de telefone. Em seguida a vítima receberá via SMS o código de segurança para que volte a utilizar sua conta. O problema é que em muitos casos o criminoso habilita a dupla verificação por intermédio do e-mail e PIN (o PIN definido pelo criminoso é desconhecido da vítima). Nessas situações, a vítima não conseguirá voltar a usar a conta de forma imediata, pois não saberá o PIN e será necessário enviar um e-mail para support@whatsapp.com com a seguinte frase no corpo do e-mail: "Perdido/Roubado: Por favor, desative minha conta", sendo necessário informar o seu número de telefone no padrão internacional. Exemplo: +55-17-99754-xxxx. O número +55 é o código do país, no caso, o código do Brasil. Esse e-mail enviado ao WhatsApp suspenderá temporariamente a conta da vítima na plataforma e permitirá que ela a recupere.

Adiante consta um modelo de solicitação perante o WhatsApp para ser enviada por e-mail.

Segundo informações oriundas do WhatsApp, a empresa não consegue localizar o aparelho subtraído, nem desativar o WhatsApp por intermédio de outro aparelho.

É importante esclarecer que, caso possua backup do WhatsApp no Google Drive, iCloud ou OneDrive, a vítima pode restaurar o histórico de conversas. A medida é realizada exclusivamente pela vítima, tendo em vista que o WhatsApp não tem acesso aos referidos backups.

Cabe informar que, de acordo com a empresa, quando a conta é desativada[10]:

- A conta não será completamente apagada.
- Seus contatos ainda poderão ver o seu perfil.
- Seus contatos poderão enviar mensagens para você, e essas mensagens permanecerão pendentes por até 30 dias.
- Se você reativar a sua conta antes que ela seja apagada, você receberá as mensagens pendentes no seu novo aparelho e permanecerá nas conversas em grupo de qual fazia parte.

[10] WhatsApp. **Aparelhos perdidos ou roubados.** Disponível em: <https://faq.whatsapp.com/pt_br/general/24460358>. Acesso em: 19 maio 2019.

- Se a sua conta não for reativada dentro de 30 dias, ela será completamente apagada.

Nas hipóteses de Conta de WhatsApp Falsa, em que o criminoso passa a usar a foto e os dados da vítima, em um número qualquer, para pedir dinheiro para pessoas próximas da vítima é importante, com a maior celeridade possível, utilizar as redes sociais para informar que estão usando sua foto/dados para pedir dinheiro, visando alertar futuras vítimas sobre os fatos.

a. MODELO DE E-MAIL ENVIADO PELA VÍTIMA PARA SOLICITAR BLOQUEIO PROVISÓRIO DO APLICATIVO[11]

De: [nome da vítima] <e-mail>

Para: support@whatsapp.com

Assunto: Perdido/Roubado: Por favor, desative minha conta – solicitação de desativação temporária de conta

Senhor Representante do WhatsApp,
informo que o número do meu celular +55-11-99720-**** foi subtraído (clonado) e um criminoso está utilizando minha conta de WhatsApp.

---

[11] Medida a ser adotada no momento que a vítima toma conhecimento que sua conta de WhatsApp (e provavelmente também o número de celular) foi clonada.

Além disso, informo que o criminoso está usando minha conta para cometer crimes e, por isso, solicito que seja feita a preservação dos registros da minha conta para auxiliar eventual investigação pela Polícia Civil.
Considerando os fatos supra, solicito o **bloqueio imediato e temporário da minha conta do WhatsApp (+55-11-99720-****).**

[nome da vítima]

IV. LINKS RECEBIDOS PELA VÍTIMA

É necessário tomar cuidado com os links recebidos pelo WhatsApp/Telegram, e-mails ou disponibilizados em sites/blogues que possuem anexos que ao serem acessados, podem permitir o download e instalação de artefatos maliciosos no computador. Por isso, recomenda-se cautela com todo conteúdo recebido, principalmente quando tratar-se de ofertas muito vantajosas ou qualquer outro conteúdo de chame a atenção da vítima.

Os artefatos maliciosos instalados nos dispositivos eletrônicos operados pela vítima podem torná-los mais lentos ou até mesmo monitorarem tudo que ela faz.

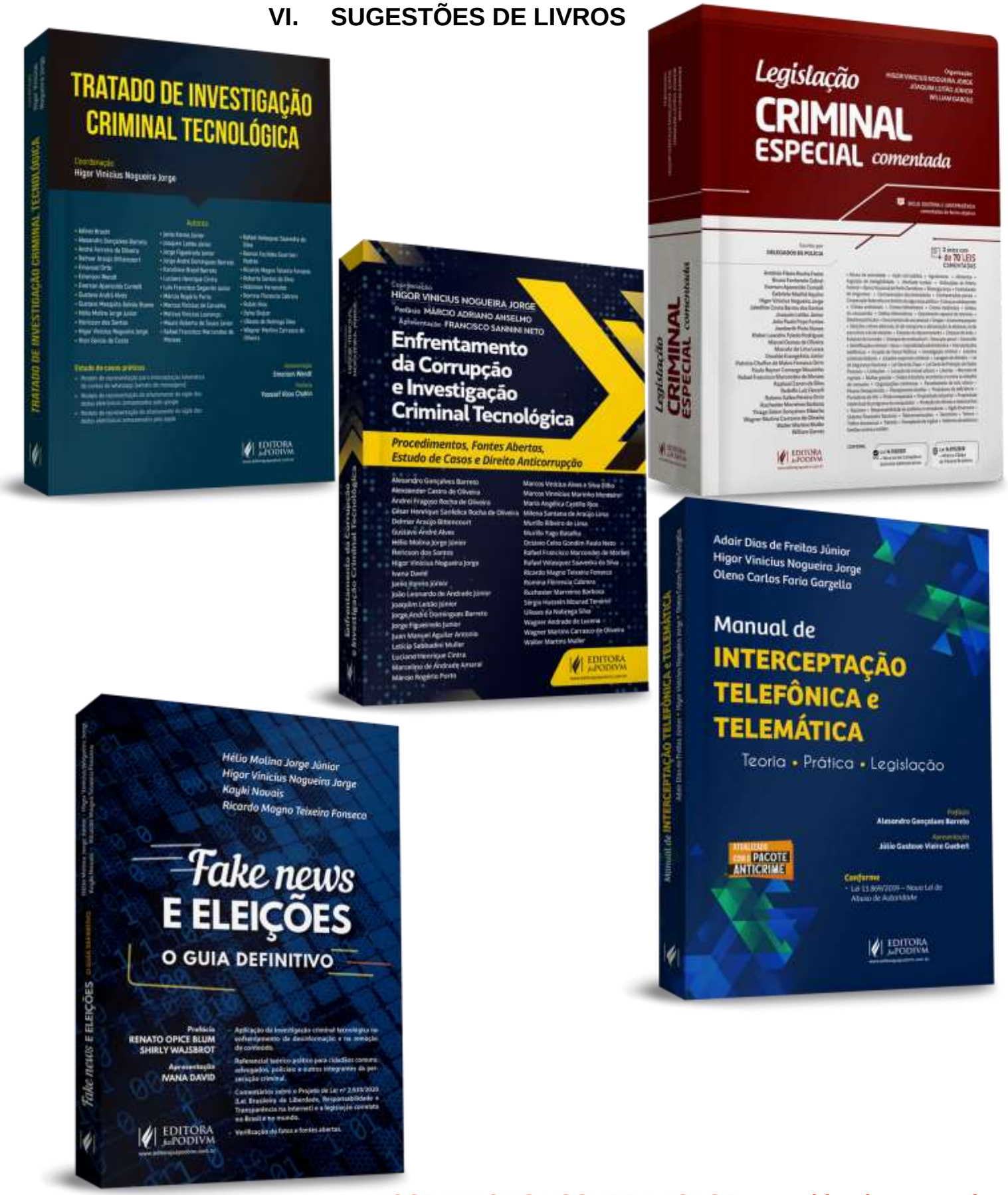
É recomendável instalar um antivírus, preferencialmente pago, no celular e demais dispositivos informáticos, bem como utilizar apenas aplicativos confiáveis e autênticos.

V. INFORMAÇÕES A SEREM PRESTADAS PARA A POLÍCIA CIVIL

Caso o usuário do WhatsApp for vítima de crime ele deve procurar uma Delegacia de Polícia onde será elaborado um Boletim de Ocorrência sobre os fatos e terá início a investigação criminal tecnológica sobre o delito.

Além disso, é importante apresentar o maior número possível de informações e evidências sobre os fatos e informar para os policiais civis o número do telefone/WhatsApp que foi subtraído, as datas que percebeu que o fato ocorreu e, nos casos que o criminoso se passou pela vítima para auferir dinheiro de conhecidos, os nomes dos conhecidos que tenham realizado as transferências bancárias, pensando tratar-se da vítima, além de cópias das conversas mantidas entre eles e dos comprovantes das transferências para identificar os beneficiários das transações.

VI. SUGESTÕES DE LIVROS



VII. REFERÊNCIAS

BARRETO, Alessandro. **Fake news: atribuição de autoria no encaminhamento de mensagens no WhatsApp**. Migalhas. Disponível em: <https://www.migalhas.com.br/dePeso/16,MI290599,61044-Fake+news+atribuicao+de+autoria+no+encaminhamento+de+mensagens+no>. Acesso em: 21 jul. 2010.

FREITAS JÚNIOR, Adair Dias; JORGE, Higor Vinicius Nogueira. GARZELLA, Oleno Carlos Faria. **Manual de Interceptação Telefônica e Telemática**. Salvador: Juspodivm. 2020.

JORGE, Higor Vinicius Nogueira. **Investigação Criminal Tecnológica**. Volumes I e II. Rio de Janeiro: Brasport. 2018.

JORGE, Higor Vinicius Nogueira (Coord.). **Tratado de Investigação Criminal Tecnológica**. 2ª edição. Salvador: Juspodivm. 2021.

RODRIGUES, Renato. Kaspersky Daily. **Anunciou na Internet? Novo golpe rouba seu WhatsApp**. Disponível em: <https://www.kaspersky.com.br/blog/golpe-rouba-whatsapp-olx-webmotors/11852/>. Acesso em: 08 jan. 2020.

TUPINAMBÁ, Marcos; Jorge, Higor Vinicius Nogueira. **Orientações sobre o WhatsApp**. Versão 2017.5. Divulgação interna.

WENDT, Emerson; JORGE, Higor Vinicius Nogueira. **Crimes Cibernéticos – Ameaças e Procedimentos de Investigação**. 2. ed. Rio de Janeiro : Brasport, 2013.

WHATSAPP. **Contas roubadas - O que fazer se sua conta for roubada**. Disponível em: <https://faq.whatsapp.com/26000244/>. Acesso em: 03 jun. 2019.