SEGURANÇA DE COMUNICAÇÕES DIGITAIS EM SMARTPHONES

Guia de Referência Rápida

Evandro Lorens,
Bruno Werneck e
Marcia Tsunoda

APRESENTAÇÃO

Em tempos de comunicação digital instantânea, nos deparamos com questões importantes relacionadas à segurança e privacidade dos usuários. As preocupações são legítimas, considerando-se que comunicações sensíveis trafegadas pela rede e armazenadas nos smartphones possam ser acessadas indevidamente.

Não existe segurança 100%. Entretanto, o uso consciente e o melhor aproveitamento dos recursos de segurança oferecidos pelos equipamentos e plataformas de serviços podem ser o diferencial em ter ou não ter informações vazadas.

Este guia de referência rápida não é definitivo ou exaustivo em sua abordagem. Antes, se propõe a apresentar aspectos práticos do uso seguro das comunicações digitais via smartphones, com recomendações plausíveis e factíveis a qualquer usuário. A ideia é que seja atualizado sempre e incorpore, a cada edição, novidades relevantes no tema.

Evandro Lorens, Bruno Werneck e Marcia Tsunoda.

1. Os produtos e serviços citados nominalmente nessa publicação não representam endosso ou crítica a qualquer fabricante ou entidade. Seu uso se dá apenas na conveniência de apoiar o leitor com recomendações relacionadas a configurações. Não existe nenhum vínculo comercial ou de qualquer espécie dos produtos e serviços mencionados com os autores.

COMO FUNCIONAM AS COMUNICAÇÕES DIGITAIS NO MODELO CLIENTE-SERVIDOR

* Nestes pontos, pode ocorrer a encriptação da mensagem
** Nestes pontos, pode ocorrer a desencriptação da mensagem

ATAQUES MAIS COMUNS

Engenharia social

Alvos potenciais: o próprio usuário, secretárias, assessores, familiares e pessoas próximas

Argumentação comum: situação envolvendo solicitação ou oferta de ajuda para serviços (TI, telecom, entregas, etc.)

Característica: uso de informação disponível em fontes abertas ou fruto de mais engenharia social

Meios comuns: chat, e-mail, SMS, mensagem de aplicativos, ligação telefônica

Objetivo comum: obter credenciais de acesso ou facilidades para acessar recursos

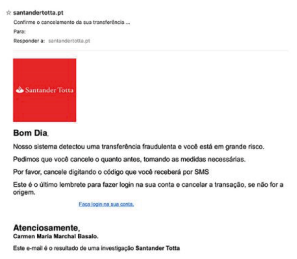
Phishing

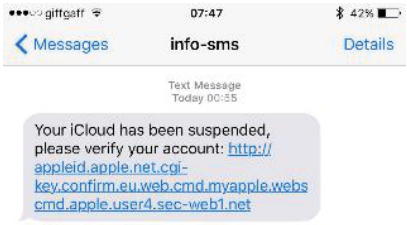
Argumentação: oferta de vantagens ou apresentação de situação urgente com link

Característica: engenharia social e pesquisa de dados abertos para phishing direcionado (spear phishing)

Meios comuns: chat, e-mail, SMS, mensagem de aplicativos, mídias sociais

Objetivo comum: instalação de malware, acesso a todos os recursos, controle remoto do dispositivo





Clonagem de chip

Formas comuns:

1) acesso físico ao dispositivo e uso de duplicador;

2) emissão de novo SIM pela operadora (cooptação de representantes).

Objetivos comuns: sequestro da linha, reconfiguração de aplicações de comunicação, recepção de segundo fator de autenticação (2FA) via SMS, furto de identidade, etc.

Contramedida: adicionar bloqueio do SIMCARD por PIN diferente do padrão (TIM: 1010, Vivo: 8486, Claro: 3636, Oi: 8888) .

Vulnerabilidades 0-day

Recursos afetados: sistemas operacionais (iOS, Android), aplicativos;

Característica: uso comercial por empresas de serviços e por mercenários;

Objetivos comuns: acesso privilegiado, controle total de recursos. Detecção difícil e dependente da percepção de "comportamento estranho" do dispositivo.

Sobre protocolos de comunicação

Típico: vulnerabilidade do SS7 (protocolo usado em redes 2G, 3G);

Objetivo: acesso parcial a recursos, basicamente voz (ligação falsa) e SMS (2FA).

Sobre redes Wi-Fi públicas (aeroportos, shoppings, hotéis)

Objetivos comuns: exploração de vulnerabilidades de protocolos Wi-Fi e DNS desatualizados;

Característica: engenharia social e coleta de dados dos equipamentos e usuários conectados.

RECOMENDAÇÕES

Segurança de senhas

O que não usar para compor senhas: dados pessoais, dados de familiares, dados sociais, dados de propriedades, documentos, datas, etc;

Evitar o reuso de senhas (“rodízio” e “mesma senha para tudo”);

Evitar armazenamento de senhas (rascunhos de e-mail, arquivos em nuvem, arquivos no computador, etc);

Usar gerenciadores de senhas (por exemplo, Lastpass, 1password, Enpass, etc);

Usar senhas mais complexas para acessos mais sensíveis (maior risco) como bancos, e-mail, nuvem, etc;

Pontos de Atenção: cuidado com dados e senhas em sites de compras, compra com 1-click, armazenamento de cartões, etc;

Desbloqueio de tela do smartphone

Evite usar desenho padrão (pontos conectados): fácil dedução, padrões “mais usados”, rastro de gordura corporal;

Não deixar sem bloqueio de tela;

Não usar senhas de 4 dígitos;

Evite usar senhas de 6 dígitos;

Preferir senhas alfanuméricas com mais de 8 caracteres;

Preferir combinação de senha alfanumérica com mais de 8 caracteres com biometria (digital, face, etc).

Atualizações

Preferir versões mais atuais dos sistemas operacionais (Android e iOS)

Configurar modo de atualização automática e verificar diariamente as atualizações dos aplicativos

Atualizar o sistema operacional sempre que correções estiverem disponíveis

“Mobile Security”

Utilizar aplicativo de segurança móvel (antivírus, antimalware, etc.) com pelo menos as funcionalidades: verificação de riscos à privacidade, proteção contra sites, links e downloads maliciosos, e filtragem de conteúdo inapropriado

Links e aplicativos

Não clicar em links recebidos por SMS, e-mail ou por outras mensagens

Instalar aplicativos somente de fontes confiáveis (Google Play Store e Apple App Store)

Não dar permissões para aplicativos (clique simples em caixa de mensagem) sem verificar a origem e necessidade da solicitação

Segregação funcional

Utilizar aparelhos diferentes para vida pessoal e para assuntos sensíveis de trabalho

Evitar manter informações sensíveis (dados pessoais, documentos, etc) nos rascunhos e mensagens de e-mail ou no armazenamento do smartphone (fotos de documentos, cartões de créditos, etc)

VPN

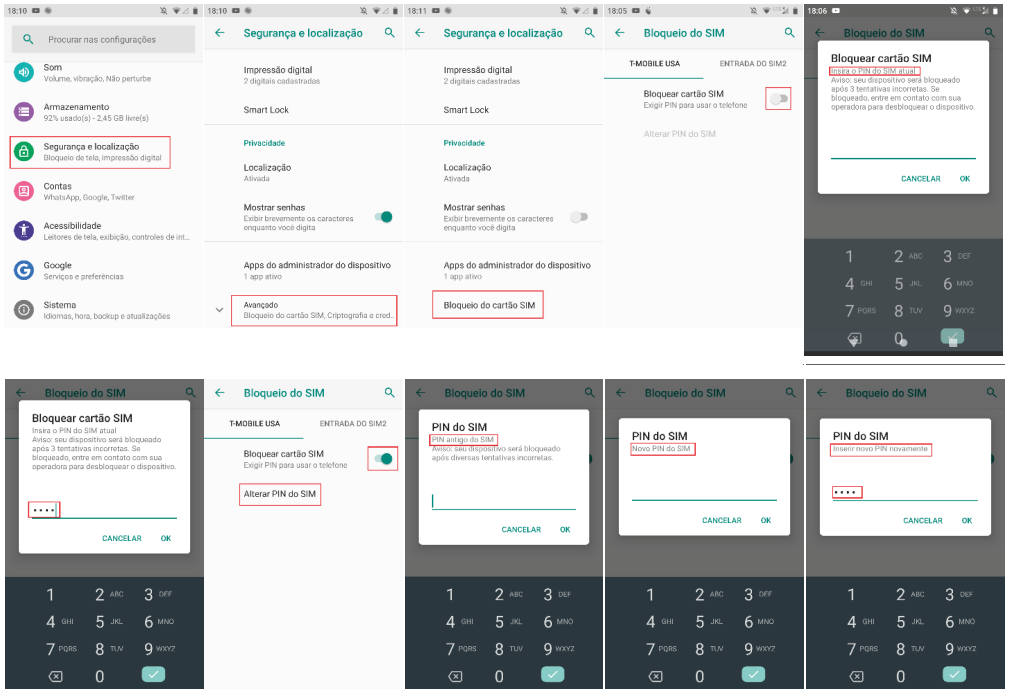
Utilizar Redes virtuais privadas (VPN - Virtual Private Network) para proteger o tráfego de dados em redes públicas ou inseguras

Criptografia

Preferir aparelhos com recurso de criptografia nativa por hardware (ativar!) (iPhone 7+, Samsung S8+, etc.)

Bloqueio de SIM Card

Ativar bloqueio do chip com PIN diferente do padrão da operadora (TIM: 1010, Vivo: 8486, Claro: 3636, Oi: 8888)



Miscelânea

Utilizar as funções de encontrar dispositivo (“Find my phone”) para casos de perda, furto ou roubo com permissão para remoção remota dos dados;

Monitorar atividades das contas para identificar atividades suspeitas: vários provedores de serviços (e-mails, mídias sociais, armazenamento remoto) emitem alertas quando um novo login é realizado em equipamentos desconhecidos;

Definir uma conta de e-mail para recuperação de acessos;

Realizar backup dos dados;

Em caso de suspeita de ataque:

1. *colocar o aparelho em modo avião;*

2. *desligar o aparelho;*

3. *restringir o acesso físico de terceiros ao aparelho;*

4. *em outro dispositivo, trocar suas senhas das principais contas (e-mail, bancos, nuvem, etc.);*

5. *acionar a perícia.*

SEGURANÇA NO WHATSAPP

Modelo cliente-servidor

Criptografia ponta a ponta – algoritmo de curvas elípticas Curve25519 (128 bits) não proprietário

Armazena mensagens em servidores enquanto não entregues por até 30 dias

Duplo fator de autenticação (2FA) – opcional!

Pontos de atenção:

1. WhatsApp Web – exibição das conversas do WhatsApp em outros computadores – acesso físico ou remoto a esses computadores;

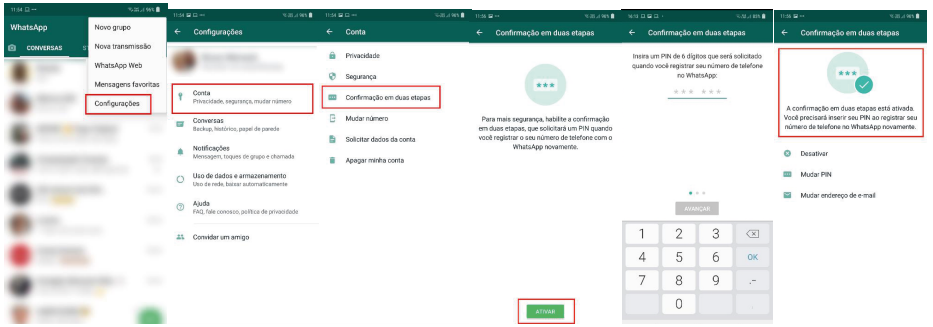
2. Conversas sensíveis em grupos e com contas de empresas – não há garantia de não vazamento ;

3. Permite desabilitar 2FA sem exigir nenhuma autenticação;

4. Declaração do fabricante: "*nós podemos coletar, usar, preservar e compartilhar informações de usuários se acreditarmos de boa fé que isso é necessário para (a) ... (b) ... (c) ..., e (d) cumprir os nossos termos e as nossas políticas. Isso pode incluir informações sobre como alguns usuários interagem entre si ao usar o nosso serviço.*";

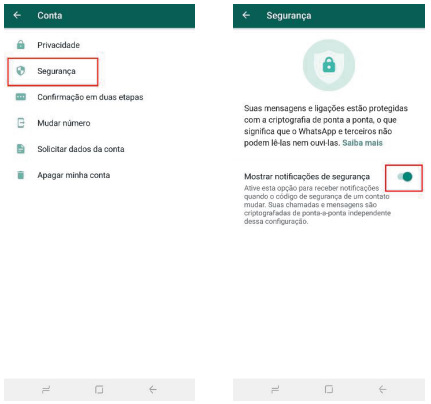
5. Permite realizar backup das mensagens (Google Drive ou iCloud) (opcional).

DUPLO FATOR DE AUTENTICAÇÃO



NOTIFICAÇÕES DE SEGURANÇA

- Mudanças em chaves de criptografia de parceiros



SEGURANÇA NO TELEGRAM

- ***Modo normal:*** modelo cliente servidor – tráfego e armazenamento criptografado em nuvem;
- ***Chat secreto:*** modelo cliente servidor (sem rastros no servidor) – criptografia ponta a ponta – duas camadas, temporizador de autodestruição.

> *Criptografia baseada em padrão AES (256 bits)*
> *Duplo fator de autenticação (2AF) – opcional!*
> *Senha de bloqueio (combinada com biometria)*

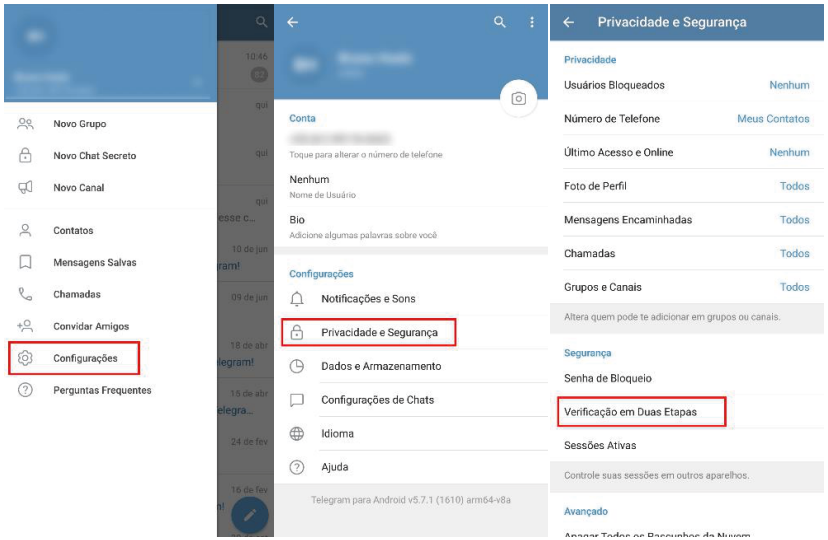
Pontos de atenção:

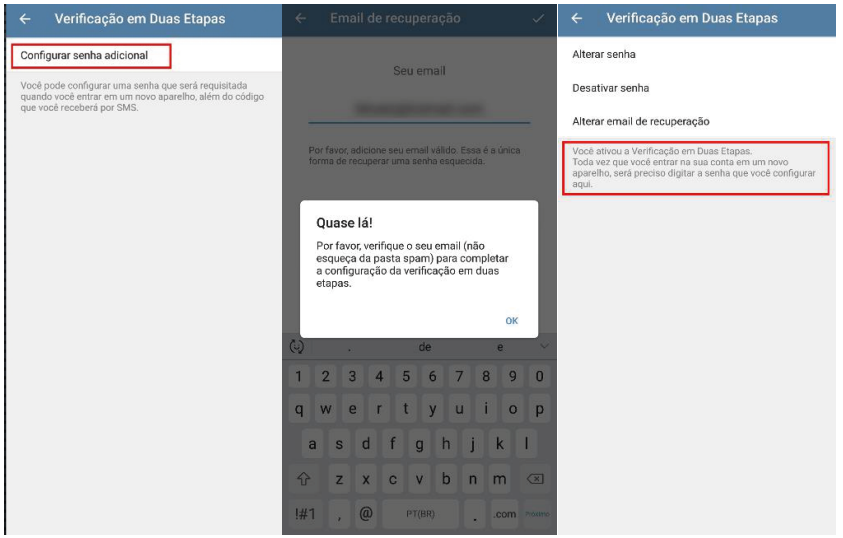
1. Telegram web e cliente desktop – exibição das conversas em outros computadores – acesso físico ou remoto ao computador;

2. Conversas sensíveis em grupos e com contas de empresas – não há garantia de não vazamento;

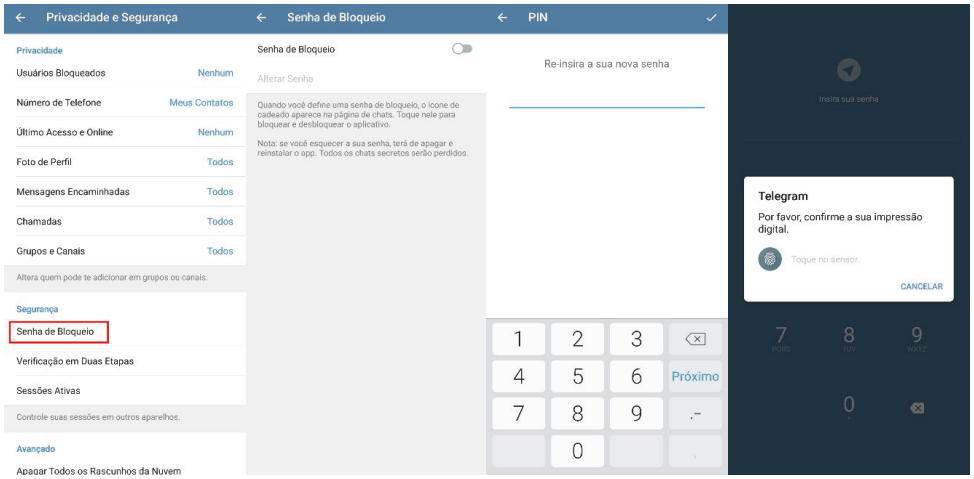
3. Declaração do fabricante: *"nós somente armazenamos os dados que o Telegram precisa para funcionar como um serviço de mensagens seguro e rico em recursos"*

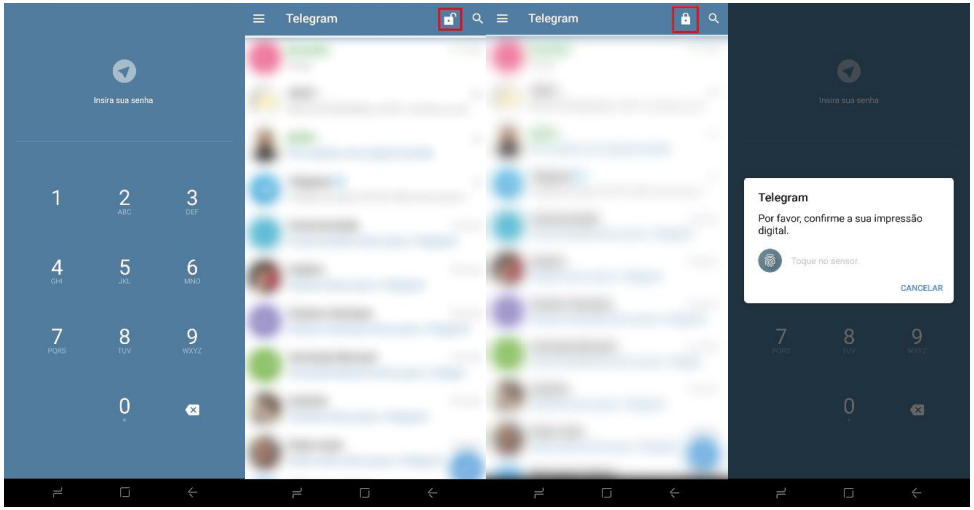
DUPLO FATOR DE AUTENTICAÇÃO



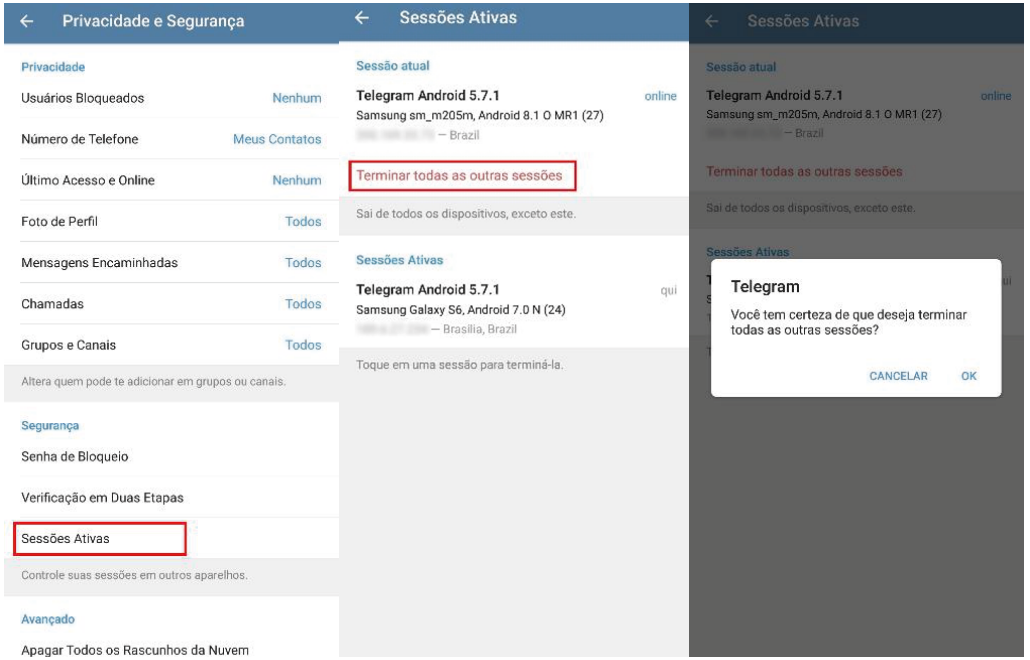


ATIVAÇÃO DE SENHA DE BLOQUEIO





CONTROLE DE SESSÕES ATIVAS



LEITURAS RECOMENDADAS

A Arte de Enganar: Ataques de Hackers: Controlando o Fator Humano na Segurança da Informação - Kevin D. Mitnick e William L. Simon

Cartilha de segurança para Internet CERT.br – disponível em https://cartilha.cert.br/livro/cartilha-seguranca-internet.pdf

SS7 vulnerabilities and attack exposure report, 2018 – disponível em https://www.ptsecurity.com/ww-en/analytics/ss7-vulnerability-2018/

Telegram FAQ for the Technically Inclined – disponível em https://core.telegram.org/techfaq

WhatsApp Encryption Overview – disponível em https://www.whatsapp.com/security/WhatsApp-Security-Whitepaper.pdf

1ª Edição

Agosto de 2019

POLÍCIA FEDERAL

APCF
ASSOCIAÇÃO NACIONAL DOS PERITOS CRIMINAIS FEDERAIS

MINISTÉRIO DA JUSTIÇA E SEGURANÇA PÚBLICA

PÁTRIA AMADA BRASIL
GOVERNO FEDERAL