2º de maio de 2024

Para os membros relevantes do Ministério das Finanças,

Estou escrevendo para submeter à sua consideração um relatório, "Trusted App Stores: Protecting Security and Integrity", em nome do Center for Cybersecurity Policy & Law. Agradecemos o desejo de ter um ecossistema digital vibrante e competitivo no Brasil. No entanto, gostaríamos de compartilhar as preocupações sobre o impacto da segurança cibernética de requisitos específicos, como os da Lei de Mercados Digitais da União Europeia, que os sistemas operacionais móveis devem permitir um maior número de formas de instalação de aplicativos em smartphones.

O Center for Cybersecurity Policy & Law está preocupado com o fato de que a proliferação de maneiras de instalar aplicativos será esmagadora para os usuários e abrirá vários caminhos para que pessoas mal-intencionadas os explorem. Isso não quer dizer que não haja nada que possa ser feito para proteger os usuários, mas será necessário que as empresas e os próprios usuários tomem medidas para garantir que eles estejam protegidos de maneiras que não precisavam no passado. Este documento descreve os possíveis riscos para os cidadãos, seus dispositivos e dados, bem como as abordagens para atenuar esses riscos. Concluímos com recomendações para ajudar reguladores e legisladores a garantir que os usuários possam continuar a confiar no ecossistema móvel e como mitigar possíveis implicações de segurança para usuários e empresas. Esperamos que este documento forneça insights úteis para o Brasil à medida que seu Ministério explora formas adicionais de promover a concorrência e, ao mesmo tempo, proteger a segurança e a privacidade de seus cidadãos.

Recomendamos que você considere cuidadosamente as possíveis consequências não intencionais das exigências de instalação de aplicativos de terceiros antes de adotar tais regulamentações. Uma abordagem mais equilibrada que preserve a escolha do consumidor e proteja a concorrência leal seria mais adequada para promover uma economia digital próspera no Brasil.

O relatório em anexo fornece uma análise mais detalhada para apoiar essas conclusões. Agradecemos a oportunidade de discutir essas questões com sua equipe. Se tiver outras dúvidas, entre em contato conosco.

Atenciosamente,

Heather West, Center for Cybersecurity Policy & Law, Venable LLP (HEWest@venable.com)
Belisario Contreras, Center for Cybersecurity Policy & Law, Venable LLP (BContreras@Venable.com)

*Sobre o Center for Cybersecurity Policy & Law:*

O Center for Cybersecurity Policy & Law é uma organização independente dedicada a aprimorar a segurança cibernética em todo o mundo, fornecendo ao governo, ao setor privado e à sociedade civil práticas e políticas para gerenciar melhor as ameaças à segurança.

Estabelecido em 2017 como uma organização sem fins lucrativos 501(c)(6), o Center combina experiência em políticas com poder de convocação para reunir líderes do setor com formuladores de políticas, formar coalizões e lançar iniciativas que produzam resultados no mundo real.

Aplicando uma abordagem baseada no gerenciamento de riscos e orientada para o consenso, o Centro busca desmistificar as complexidades e dissipar a confusão em torno da segurança cibernética, promovendo soluções pragmáticas e recomendações de políticas elaboradas a partir das perspectivas e práticas daqueles que estão na linha de frente da proteção da infraestrutura digital e dos sistemas de informação.

CENTER FOR
CYBERSECURITY
POLICY AND LAW

# Lojas de Aplicativos Confiáveis: Protegendo Segurança e Integridade

**Fevereiro 2024**

Compilado por:
Heather West | Diretora Sênior
+1 202.344.4597
HEWest@Venable.com

Tim McGiff | Project Manager
+1 202.344.4365
TCMcGiff@Venable.com

# Índice

## Resumo Executivo

À medida que a União Europeia (UE) implementa novas políticas e regulamentações para seu mercado digital, é necessário equilibrar cuidadosamente considerações econômicas com acesso, privacidade e segurança. Infelizmente, as regras do Ato de Mercados Digitais (DMA) às lojas de aplicativos móveis do podem minar controles de segurança fundamentais que tornaram o ecossistema de smartphones tão confiável e resiliente. O Center for Cybersecurity Policy and Law está preocupado que a proliferação de formas de baixar aplicativos seja avassaladora para os usuários e abra várias oportunidades para atores mal-intencionados explorá-los. Isso não implica que nada possa ser feito para proteger os usuários, mas exigirá ação das empresas e dos próprios usuários para garantir que estejam protegidos de maneiras que não precisaram no passado. Este documento destaca os riscos potenciais para os cidadãos da UE, seus dispositivos e dados, bem como abordagens para mitigar esses riscos. E conclui com recomendações para ajudar reguladores e formuladores de políticas a garantir que os usuários possam continuar confiando no ecossistema móvel, e como mitigar possíveis implicações de segurança para usuários e empresas. Esperamos que este documento também forneça ‘insights’ para outros países na busca para fomentar a concorrência em seus próprios mercados digitais, ao mesmo tempo em que protegem a segurança e privacidade de seus cidadãos.

### Sobre o Centro de Cibersegurança e Direito

O Center for Cybersecurity Policy and Law é uma organização independente dedicada a aprimorar a cibersegurança em todo o mundo, fornecendo práticas e políticas para governos, setor privado e sociedade civil gerenciarem melhor as ameaças à segurança. Estabelecido em 2017 como uma organização sem fins lucrativos 501(c)(6) dentro do grupo de Serviços de Cibersegurança da Venable LLP, combina experiência em políticas com poder de convocação em níveis global, nacional e local para reunir líderes do setor com formuladores de políticas, formando coalizões e lançando iniciativas que produzem resultados do mundo real. Aplicando uma abordagem orientada para o consenso e baseada em gerenciamento de riscos, o Centro busca desmistificar as complexidades e dissipar a confusão em torno da cibersegurança, promovendo soluções pragmáticas e recomendações de políticas baseadas nas perspectivas e práticas daqueles na linha de frente da segurança da infraestrutura digital e sistemas de informação.

# Introdução

Em um mundo cada vez mais conectado, frequentemente usamos aplicativos em nossos smartphones para interagir com um ecossistema rico em serviços, informações e recursos. Os benefícios dos smartphones são amplamente reconhecidos[1]: eles são nossas janelas para o mundo, monitoram nossa saúde, compartilhamos informações com nossos amigos, compramos produtos e gerenciamos serviços. E, consequentemente, passamos muito tempo usando aplicativos móveis - quatro a cinco horas por dia, ou mais.[2] Assim, é crucial que nossos dispositivos e aplicativos permaneçam seguros e confiáveis.

Estudos sugerem que, nos Estados Unidos, 81% dos consumidores, com idades entre 18 e 34 anos, consideram seguros os dispositivos conectados que possuem.[3] As pessoas têm boas razões para confiar em seus dispositivos móveis e aplicativos, graças aos esforços dos desenvolvedores de sistemas operacionais e lojas de aplicativos para proteger esses ecossistemas.

Em nosso documento de 2021 *Mobile Future: Pathways to Continued Improvement in Mobile Security and Privacy*,[4] discutimos a segurança móvel com vinte e três especialistas em cibersegurança da indústria, academia e sociedade civil, e constatamos que "enquanto novas ameaças a dispositivos móveis continuam a surgir, as proteções existentes geralmente estão funcionando melhor do que em outras áreas de cibersegurança".[5] O consenso de nosso grupo de foco foi que o ambiente móvel se beneficiou de proteções integradas de segurança e privacidade no nível do sistema operacional (SO) e da loja de aplicativos, reduzindo significativamente o ônus sobre os usuários de se protegerem.

Aquele documento, de apenas três anos atrás, foi escrito no contexto das arquiteturas de dispositivos móveis e capacidades de segurança atuais de desenvolvedores de sistemas operacionais conceituados e suas lojas oficiais de aplicativos confiáveis. Ao longo da última década, o ecossistema de dispositivos móveis tornou-se progressivamente mais seguro - mas as regras do DMA da União Europeia para aplicativos, focado em competição[6], podem fazer o ecossistema regredir em vez de continuar esse progresso de segurança cibernética. Precisamos trabalhar juntos para garantir o progresso de segurança cibernética.

As disposições do DMA que exigem que os sistemas operacionais permitam a instalação de aplicativos de lojas de terceiros têm o potencial de serem avassaladoras para os usuários, representando um desafio para os administradores de empresas que implementam o gerenciamento de dispositivos móveis, e podem abrir novas oportunidades para atores mal-intencionados.

---

[1] https://www.pewresearch.org/internet/2019/03/07/majorities-say-mobile-phones-are-good-for-society-even-amid-concerns-about-their-impact-on-children/

[2] Data.ai, através de Techcrunch, relata que usuários de mobile passam 4-5 horas por dia em apps - link

[3] https://staysafeonline.org/wp-content/uploads/2022/07/Cybersecurity-Awareness-Month-2020-Results-Report.pdf

[4] https://assets.website-files.com/62715f02a51b614ce64867fd/628e6ba29361afc22807be6b_mobile-future-pathways-to-continued-improvement-in-mobile-security-and-privacy.pdf

[5] https://assets.website-files.com/62715f02a51b614ce64867fd/628e6ba29361afc22807be6b_mobile-future-pathways-to-continued-improvement-in-mobile-security-and-privacy.pdf

[6] O texto do Digital Markets Act pode ser encontrado em https://eur-lex.europa.eu/eli/reg/2022/1925

Mitigar esses riscos exigirá apoiar os “gatekeepers” dos sistemas operacionais móveis para equilibrar a intenção do DMA ao adotar abordagens razoáveis para mitigar os riscos que acompanharão um ecossistema mais aberto.

Este documento irá esboçar brevemente as disposições da loja de aplicativos dentro do DMA, as ameaças ao ecossistema de dispositivos móveis exacerbadas por essas disposições, e examinar brevemente como proprietários de lojas de aplicativos nativas e sistemas operacionais de dispositivos móveis combateram historicamente essas ameaças. Este documento fará uma argumentação para os tipos de abordagens de implementação do DMA que os Estados membros da UE devem apoiar para garantir que usuários finais despreparados não se vejam de repente responsáveis pela segurança do ecossistema de dispositivos móveis.

O texto do DMA faz referência a potenciais formas de proteger os usuários, incluindo mecanismos técnicos e contratuais; além disso, legisladores e reguladores devem apoiar o papel dos desenvolvedores de sistemas operacionais para proteger os usuários por meio de análises de aplicativos, proteção avançada contra malware, requisitos de transparência e ajustes nas permissões e modelos de segurança incorporados aos sistemas operacionais de dispositivos móveis. É importante garantir que trabalhemos juntos para garantir um ecossistema móvel vibrante e inovador. Nós insistimos que os formuladores de políticas devem enfatizar a importância da segurança nos atos de implementação do DMA e, conforme os “gatekeepers” trabalham para estabelecer sua conformidade.

## Provisões do DMA para Loja de Aplicativos

Até março de 2024, as empresas abrangidas pela definição de "gatekeeper" que operam "serviços centrais de plataforma" estarão sujeitas às disposições do DMA relacionadas às suas lojas de aplicativos e interações do sistema operacional móvel com lojas de aplicativos de terceiros e aplicativos. “gatekeepers” são aquelas empresas, designadas pela Comissão Europeia, que têm um impacto significativo no mercado europeu e fornecem um serviço que intermedia a relação entre empresas (por exemplo, desenvolvedores de aplicativos) e usuários finais (por exemplo, usuários de smartphones que baixam aplicativos).[7] A intenção do DMA é facilitar para empresas europeias menores competir com empresas que podem ter uma posição mais "enraizada" no mercado.

As provisões do DMA exigem que os sistemas operacionais de dispositivos móveis permitam a instalação de aplicativos de lojas de aplicativos não “gatekeepers”” ou por meio de outros métodos, e que os sistemas operacionais permitam o mesmo acesso e ferramentas do sistema para aplicativos nativos e de terceiros.

O cerne dessas disposições inclui:

[7] Até a publicação deste documento, o sistema operacional iOS da Apple e o sistema operacional Android do Google são considerados serviços centrais de plataforma. O sistema operacional para desktop PC Windows da Microsoft também é considerado um serviço central de plataforma, mas está fora do escopo deste documento. https://ec.europa.eu/commission/presscorner/detail/en/ip_23_4328

- *Seção 6.4: O "gatekeeper" deve permitir e possibilitar tecnicamente a instalação e uso efetivo de aplicativos de software de terceiros ou lojas de aplicativos de software que usam, ou interoperam com, seu sistema operacional e permitir que esses aplicativos de software ou lojas de aplicativos de software sejam acessados por meio de outros meios que não os serviços centrais relevantes desse "gatekeeper".*

- *Seção 6.7: O "gatekeeper" deve permitir que provedores de serviços e provedores de hardware, sem custos, interoperem efetivamente com e acessem, para fins de interoperabilidade, os mesmos recursos de hardware e software acessados ou controlados pelo sistema operacional ou assistente virtual [...]. Além disso, o "gatekeeper" deve permitir [...] interoperabilidade efetiva com e acesso para fins de interoperabilidade aos mesmos recursos de sistema operacional, hardware ou software, independentemente de esses recursos fazerem parte do sistema operacional, conforme estão disponíveis para, ou são usados por, esse "gatekeeper" ao fornecer tais serviços.*

Essas regras do DMA, quando combinadas com outras leis da União Europeia, exigirão efetivamente que os "gatekeepers" permitam baixar de forma fácil de aplicativos de terceiros e lojas de aplicativos em dispositivos móveis, permitam um acesso mais fácil a lojas de aplicativos de terceiros pelos usuários móveis e concedam aos desenvolvedores e aplicativos de terceiros o mesmo acesso, interoperabilidade e funcionalidade com os sistemas operacionais móveis que os "gatekeepers" desfrutam no momento.

Além dessas disposições - e destacando uma conscientização do risco de segurança e privacidade representado pela "abertura" do ecossistema móvel - há uma ressalva de segurança subestimada. O considerando 50 do DMA afirma que o acesso adicional fornecido a aplicativos de terceiros e lojas de aplicativos não deve comprometer a segurança do usuário e do dispositivo. No entanto, o DMA não detalha como espera que os sistemas operacionais protejam dispositivos móveis e usuários, dadas as restrições sobre como os sistemas operacionais podem diferenciar ou limitar o acesso a aplicativos. Se implementadas sem cuidado, as disposições acima do DMA podem agravar o atual ecossistema de ameaças móveis.

## Ameaças ao Ecossistema de Dispositivos Móveis

Combater malware é uma prioridade para desenvolvedores de sistemas operacionais de dispositivos móveis e organizações ao redor do mundo. Apesar de suas arquiteturas de segurança bem-sucedidas e protetoras, dispositivos móveis são um alvo tentador devido à sua ubiquidade, ao fato de nos acompanharem ao longo do dia e por serem uma parte fundamental de nossas vidas e interações digitais.

As ameaças à dispositivos móveis também cresceram à medida que os sistemas operacionais se tornaram verdadeiras plataformas em vez de ecossistemas fechados, e desenvolvedores de sistemas operacionais de dispositivos móveis e operadores de lojas de aplicativos respeitáveis têm trabalhado para conter ameaças por meio de escolhas de design na arquitetura do sistema operacional, isolamento de aplicativos e dados, moderação de aplicativos, verificações de funcionalidade e qualidade de aplicativos, e modelos de permissões cada vez mais granulares. O Relatório sobre o Panorama de Ameaças à dispositivos Móveis de 2019 da CrowdStrike constatou que plataformas de dispositivos móveis estão cada vez

mais sendo alvo de criminosos e que adversários menos habilidosos agora têm acesso a malwares móveis de prova de conceito que lhes permite tentar obter acesso a dispositivos móveis com facilidade.[8]

## Principais Ameaças à Dispositivos Móveis

Há uma infinidade de ameaças para, e no, ecossistema de dispositivos móvel, à medida que atores maliciosos e oportunistas buscam qualquer maneira de aproveitar essas plataformas incrivelmente populares. À medida que os “gatekeepers” e legisladores implementam o DMA, eles devem ter em mente maneiras de minimizar essas ameaças.

Aplicativos maliciosos sempre foram a ameaça mais significativa para dispositivos móveis devido ao potencial de interagir diretamente com dados sensíveis armazenados e a funcionalidade principal do dispositivo móvel. De acordo com estudos da Nokia[9] e da Kaspersky,[10] a maioria dos malwares contra dispositivos móveis chega por meio de aplicativos trojanizados. Esses aplicativos fingem ser algo que as pessoas realmente desejam baixar, como um aplicativo de lanterna ou versões gratuitas de software caro - mas o aplicativo trojanizado está escondendo comportamentos indesejados, como a coleta de informações ou credenciais sensíveis.[11] Isso é possível porque os aplicativos solicitam permissões que não seriam necessárias para sua função superficial, como um aplicativo de lanterna que solicita dados de localização ou contatos armazenados no telefone.[12] O usuário instala o que parece ser um aplicativo ou jogo benigno, geralmente de graça, mas abre seu dispositivo e dados para atores maliciosos. Check Point relatou um aumento nesses apps, especificamente aqueles que se propõem a oferecer um teste grátis ou funcionalidade extra.[13] Eles observam que há risco em confiar no familiar, pois muitos desses aplicativos utilizam nomes de marcas e produtos conhecidos – mas, na realidade, roubam dados, credenciais ou adicionam o dispositivo a uma botnet.[14]

Esses aplicativos maliciosos frequentemente conseguem esconder sua verdadeira natureza. Há uma proliferação de aplicativos trojanizados -- incluindo ferramentas de hacking, acesso, spyware, adware, discadores e programas de piadas -- que têm comportamento irritante ou prejudicial que o usuário não deseja.[15] Existem até provedores de malware como serviço que criam aplicativos para assumir contas e unir dispositivos móveis a botnets.[16]

---

[8] https://www.crowdstrike.com/resources/reports/mobile-threat-report-2019/

[9] https://www.nokia.com/networks/security-portfolio/threat-intelligence-report/

[10] https://securelist.com/mobile-malware-evolution-2020/101029/

[11] https://www.mcafee.com/blogs/mobile-security/mobile-spyware/, https://www.appdome.com/dev-sec-blog/mobile-payment-security/

[12] https://blog.avast.com/flashlight-apps-on-google-play-request-up-to-77-permissions-avast-finds

[13] Check Point, 2023 Cyber Security Report, 2023

[14] https://www.verizon.com/business/resources/T9bc/reports/mobile-security-index-report.pdf

[15] https://docs.broadcom.com/doc/istr-23-03-2018-en

[16] https://www.androidpolice.com/android-botnet-trojan-steal-banking-data/

Alguns desses aplicativos também são altamente direcionados. Por exemplo, vários golpes de aplicativos de empréstimo instantâneo circularam pela Índia e outros países da Ásia, África e América Latina. Após a instalação, o aplicativo pode realmente fornecer um empréstimo, mas também colhe informações do telefone, tanto informações sobre o usuário quanto outros dados no telefone, incluindo fotografias nuas, que são usadas para assediar, intimidar e extorquir.[17]

Com a principal ameaça à dispositivos móveis identificada, a pergunta natural é: "mas como esses aplicativos maliciosos são instalados?" Lojas de aplicativos nativas, como Google Play Store e Apple App Store, não são infalíveis em manter fora aplicativos ruins, mas a vasta maioria dos aplicativos em suas lojas são benignos, devido aos esforços para manter suas lojas seguras. Os vetores mais arriscados para malwares vêm de lojas de aplicativos de terceiros e do “sideload”. Embora quantificar com precisão a quantidade de risco apresentado por cada método seja excepcionalmente difícil, alguns estudos sugerem riscos substanciais para os usuários.

## Lojas de Aplicativos de Terceiros

Embora alguns estudos tenham sugerido que grandes lojas de aplicativos de terceiros podem ser seguras em comparação com lojas de aplicativos nativas, como a Google Play Store, evidências indicam que as lojas de terceiros aumentam o risco de segurança e privacidade para os usuários de dispositivos móveis – mas isso não ocorre porque elas não estão associadas ao sistema operacional. Em vez disso, geralmente não conseguem exercer a mesma diligência na fiscalização de seus aplicativos - provavelmente uma das razões pelas quais os principais sistemas operacionais móveis historicamente não permitiram lojas de aplicativos de terceiros por padrão.[18] E existem exemplos de lojas de aplicativos que têm por objetivo espalhar aplicativos maliciosos.[19] Em grupos de foco de 2021, a CrowdStrike observou que a maioria do malware contra dispositivos móvel é distribuída por fontes de terceiros que não realizam verificações abrangentes dos aplicativos que fornecem.[20]

Embora seja difícil quantificar o risco exato, um estudo de 2020 constatou que os usuários de Android de "outros principais mercados alternativos" eram, em média, cinco vezes mais arriscados e tinham até dezenove vezes mais chances de encontrar malware ou um aplicativo malicioso do que aqueles que usavam a Google Play Store.[21] Além disso, a empresa de segurança cibernética Symantec relatou em 2018 que 99,9% do malware móvel que descobriram estava hospedado em lojas de aplicativos de terceiros.[22]

---

[17] https://www.bbc.co.uk/news/world-asia-india-66964510

[18] https://citrixready.citrix.com/content/dam/ready/partners/wa/wandera/wanderas-web-gateway-for-mobile/mobile-threat-landscape-2020-whitepapers.pdf

[19] https://www.makeuseof.com/what-are-the-dangers-of-third-party-app-stores/#:~:text=Many%20malicious%20actors%20have%20created,hidden%20trackers%20and%20malicious%20code.

[20] 2021 Center paper

[21] https://arxiv.org/pdf/2010.10088.pdf

[22] https://docs.broadcom.com/doc/istr-23-03-2018-en

Isso levou a um consenso entre especialistas em segurança e reguladores de que baixar aplicativos de lojas de aplicativos de terceiros é muito mais arriscado do que de uma loja nativa confiável. Grandes organizações governamentais e privadas desaconselham o download de aplicativos de fontes não oficiais e não confiáveis, incluindo avisos em vários momentos emitidos pela ENISA, Europol,[23] NSA dos EUA,[24] FTC dos EUA responsável pela proteção do consumidor, NCSC do Reino Unido,[25] CERT-In da Índia,[26] CISA do DHS dos EUA[27], NIST do Departamento de Comércio,[28] CERT NZ da Nova Zelândia,[29] entre outros. Apesar disso, estudos mostraram que os consumidores usarão lojas de aplicativos de terceiros se os aplicativos forem gratuitos ou tiverem versões modificadas de jogos e aplicativos conhecidos.[30] Os usuários não estão considerando sua segurança – eles apenas querem obter rapidamente e preferencialmente de graça aquele aplicativo que parece bom demais para ser verdade.

## "Sideloading"

Em comparação, o "sideloading" não requer nenhum tipo de loja de aplicativos tradicional, e um aplicativo baixado fora das lojas de aplicativos nativas pode ser distribuído ou anunciado com pouco contexto de fundo, sem verificação e com alegações falsas ou enganosas sobre segurança e autenticidade. Não há intermediário para realizar essa diligência, pois o "sideloading" pode ocorrer de qualquer lugar – um site, um anexo de mensagem ou um link obscuro.

O "sideloading" requer que o indivíduo confie em um terceiro que pode não ter a reputação, experiência ou meios para garantir que o aplicativo não tenha sido adulterado, embora os usuários não pensem nisso quando encontram um novo jogo que desejam experimentar. Embora muitos sites e lojas de terceiros possam ser seguros, é improvável que um usuário encontre o mesmo nível de transparência em relação à forma como o aplicativo foi avaliado e às permissões que ele pode solicitar, sendo muito mais fácil fingir ser algo que não é sem a infraestrutura de uma loja de aplicativos confiável.

O "sideloading" é o método mais arriscado para os usuários adquirirem aplicativos para dispositivos móveis. Embora esse risco tenha sido tradicionalmente compensado pelo fato de que o "sideloading" muitas vezes exige um nível de conhecimento técnico que muitos usuários finais não possuem, se os sistemas operacionais móveis permitirem o sideloading por padrão, essa fricção desaparecerá. Mesmo usuários bem informados que fazem sideload muitas vezes estão confiando em

---

[23] Europol: https://www.europol.europa.eu/sites/default/files/documents/infographic_-_apps.pdf

[24] U.S. NSA Mobile Device Best Practices V3: https://media.defense.gov/2020/Jul/28/2002465830/-1/-1/0/MOBILE_DEVICE_BEST_PRACTICES_FINAL_V3%20-%20COPY.PDF

[25] U.K. NCSC: https://www.ncsc.gov.uk/files/Protecting-devices-from-viruses-malware-infographic.pdf

[26] https://www.cert-in.org.in/s2cMainServlet?pageid=PUBVLNOTES02&VLCODE=CIAD-2020-0013

[27] U.S. CISA: https://www.cisa.gov/sites/default/files/publications/CEG_Mobile_Device_Cybersecurity_Checklist_for_Organizations_0.pdf

[28] U.S. NIST: https://www.nccoe.nist.gov/sites/default/files/legacy-files/mtc-nistir-8144-draft.pdf

[29] N.Z. CERT: https://www.cert.govt.nz/individuals/guides/keep-mobile-phone-safe-secure/

[30] https://www.jamf.com/blog/what-are-third-party-app-stores-and-are-they-safe/

desenvolvedores e lojas de aplicativos desconhecidos, e nenhuma quantidade de conhecimento técnico irá diminuir o risco a menos que você apenas baixe diretamente de empresas bem estabelecidas.

## A Falha da Responsabilidade do Usuário Final

Estudos mostram que as decisões de segurança de um usuário não necessariamente se correlacionam com seu conhecimento das ameaças à segurança.[31] Apesar do dano muito real que aplicativos maliciosos podem causar, os usuários de dispositivos móveis raramente estão dispostos a gastar tempo considerável para examinar criticamente as permissões solicitadas pelos aplicativos e frequentemente não compreendem as implicações se tentarem.[32] E quando os usuários são interrompidos por avisos de segurança, eles geralmente os ignoram.[33]

Muitos usuários nem mesmo adotam medidas básicas de segurança para seus dispositivos móveis - por exemplo, um estudo constatou que 40% dos usuários relataram que não atualizam seu sistema operacional e aplicativos a menos que seja conveniente, e 28% não usam um bloqueio de tela.[34] Outro estudo constatou que três quartos dos usuários de smartphones acreditam que os aplicativos que baixam das lojas de aplicativos são inerentemente seguros,[35] o que os torna pouco propensos a serem céticos em relação a eles. Esse estudo constatou até mesmo que os usuários de aplicativos não conseguiam, ou não se importavam em, diferenciar o nível de segurança fornecido por várias lojas de aplicativos. Estudos recentes adicionais confirmam que os usuários se preocupam com os riscos de segurança, mas carecem do conhecimento e das habilidades para se protegerem efetivamente - e muitas vezes nem tentam fazê-lo.[36]

Embora esperemos que os usuários desempenhem um papel mais ativo na proteção de si mesmos online, as melhores práticas buscam cada vez mais remover o máximo possível desse fardo deles. Estratégias nacionais de cibersegurança e práticas recomendadas do governo buscam cada vez mais reequilibrar a responsabilidade longe dos usuários e colocar o ônus de proteger dispositivos, dados e pessoas nas empresas que os distribuem. Em 2023, agências nacionais de cibersegurança dos Estados Unidos (CISA), República Tcheca, Israel, Cingapura, Coreia, Noruega, OAS/CICTE CSIRTAmericas Network e Japão ((JPCERT/CC e NISC) lançaram conjuntamente orientações sobre a mudança do equilíbrio de risco longe dos usuários finais.[37] Muitas organizações nos setores público e privado também optam por usar Gerenciamento de Dispositivos Móveis (MDM) para garantir que apenas aplicativos aprovados sejam instalados em dispositivos que também têm acesso a dados ou aplicativos sensíveis, e essas ferramentas podem, no futuro, permitir que os administradores determinem quais lojas de aplicativos são permitidas.

---

[31] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5352308/

[32] https://link.springer.com/chapter/10.1007/978-3-031-35822-7_36

[33] https://news.sophos.com/en-us/2016/08/19/why-people-ignore-security-alerts-up-to-87-of-the-time/

[34] https://www.pewresearch.org/short-reads/2017/03/15/many-smartphone-owners-dont-take-steps-to-secure-their-devices/

[35] https://www.sciencedirect.com/science/article/pii/S0167404812001733#fn6

[36] https://dl.acm.org/doi/fullHtml/10.1145/3491102.3517504#sec-21

[37] https://www.cisa.gov/resources-tools/resources/secure-by-design

Dada a extensão e complexidade dos riscos mencionados acima, é irracional esperar que os usuários finais de repente tenham a consciência e o entendimento necessários sobre segurança e privacidade móvel, incluindo como se proteger por meio de segurança em camadas, configurando uma combinação ideal de configurações para seu risco aceito e outros métodos simplesmente inviáveis em escala. É provável que os usuários finais assumam que as lojas de aplicativos universalmente disponíveis são seguras. Existem outras abordagens - mas elas exigirão proteções semelhantes às que os ““gatekeepers”” já implementaram em suas próprias lojas de aplicativos.

## Como Google e Apple Combatem essas Ameaças

Muitas lojas de aplicativos nativas, como a Apple App Store e o Google Play Store, e outras que não foram determinadas como “gatekeepers” sob o DMA, adotam extensas medidas para mitigar os riscos identificados acima, por meio de políticas e processos projetados para examinar novos aplicativos e atualizações em busca de malware ou alterações significativas na funcionalidade original do aplicativo. Tanto a Apple quanto o Google criaram políticas e processos que se estendem desde o desenvolvedor, por meio de suas lojas oficiais de aplicativos, até os consumidores. Embora nenhuma loja de aplicativos seja completamente segura, esses esforços resultaram no Google Play Store e na Apple App Store ganhando uma reputação de confiança e segurança do consumidor por meio de anos de investimento e aprendizado para informar suas abordagens na proteção dos usuários.

Lojas de aplicativos nativas líderes, como a Apple App Store e o Google Play Store, alcançam segurança por meio da implementação de processos, como estabelecer requisitos e diretrizes básicas, exigir autoavaliações e revisar os aplicativos.[38] Os desenvolvedores de aplicativos devem atender com sucesso aos vários requisitos de segurança, privacidade e transparência para seus aplicativos, a fim de serem apresentados em uma dessas lojas de aplicativos. Isso pode incluir garantir que um aplicativo faça o que é anunciado, solicite apenas permissões apropriadas e tenha políticas de privacidade funcionais. As lojas de aplicativos da Apple e do Google também exigem transparência em suas listagens de lojas de aplicativos, incluindo permissões que o aplicativo usa e informações sobre coleta de dados.[39], [40]

Lojas de aplicativos nativas também podem ter proteções adicionais fora da revisão do próprio aplicativo, como a verificação de contas de desenvolvedores. Por exemplo, o Google Play Store analisa "a conta Google do desenvolvedor, ações, histórico, detalhes de faturamento, informações do dispositivo e muito mais" para identificar possíveis sinais de alerta.[41]

Quando se trata de revisar uma submissão de aplicativo, lojas de aplicativos nativas podem adotar diversas ações para garantir sua funcionalidade: a loja pode revisar as autoavaliações do desenvolvedor, aplicar várias revisões automatizadas e ter um revisor humano revisando manualmente o aplicativo. Essas revisões podem usar uma variedade de ferramentas e técnicas para realizar revisões estáticas e dinâmicas em busca de malware ou outros aspectos potencialmente prejudiciais ou

---

[38] https://developer.apple.com/app-store/review/guidelines/, https://play.google.com/about/developer-content-policy/

[39] https://support.google.com/googleplay/android-developer/answer/10144311?hl=en

[40] https://developer.apple.com/app-store/user-privacy-and-data-use/#:~:text=In%20order%20to%20submit%20new,websites%20owned%20by%20other%20companies.

[41] https://developers.google.com/android/play-protect/cloud-based-protections

indesejados. Além disso, além das inspeções de rotina de aplicativos recém-submetidos, lojas de aplicativos nativas, como a da Apple, revisam as atualizações de aplicativos para garantir que qualquer nova funcionalidade permaneça segura. Por fim, as lojas de aplicativos nativas costumam acionar revisões com base em reclamações de consumidores ou notificações de pesquisadores de segurança de que um aplicativo está envolvido em comportamentos indesejados.

Se um aplicativo não atender e manter os requisitos e diretrizes necessários para inclusão na loja de aplicativos, o aplicativo geralmente será removido. A escala dessas questões é notável, com a Apple detalhando que rejeitou mais de 1,5 milhão de submissões de aplicativos e removeu mais de 186.000 aplicativos de sua loja de aplicativos em 2022.[42] Essas remoções promovem um ambiente seguro e confiável na loja de aplicativos, protegem os usuários de danos e incentivam os atores maliciosos a procurar outros meios mais frutíferos de infectar dispositivos.

No nível do consumidor, a Apple e o Google fizeram esforços significativos para tornar suas proteções e requisitos de segurança e política facilmente acessíveis e compreensíveis pelos usuários de suas lojas de aplicativos. Além disso, ambos buscaram criar mais transparência em relação às permissões que os aplicativos verificados solicitam, para que os consumidores possam tomar decisões informadas sobre o nível de privacidade e segurança desejado, além da linha de base da loja de aplicativos oficial. O Google Play Store até começou a exibir um distintivo nos aplicativos que passaram por uma revisão independente de segurança.[43] Esses processos e políticas provaram ser eficazes, mas representam investimentos significativos.

### Segurança para Lojas de Aplicativos é um Investimento

Como estabelecido acima, atribuir a responsabilidade da segurança aos usuários finais é ineficaz e vai contra as melhores práticas de cibersegurança, que cada vez mais promovem políticas e processos para garantir que o usuário seja protegido por padrão. Embora grandes entidades bem financiadas, como o Google e a Apple, tenham a experiência, os recursos e a disposição para fazê-lo de maneira eficaz, poucas outras podem dizer o mesmo.

Os tipos de proteções mencionadas acima, que raramente, se alguma vez, são implementadas na mesma medida por lojas de aplicativos de terceiros, eliminam a maioria dos aplicativos maliciosos, de baixa qualidade e enganosos. Lojas de aplicativos nativas não têm o mesmo nível de recursos, experiência, conhecimento da plataforma e do sistema operacional, ou incentivo para proteger sua loja de aplicativos ou avaliar os aplicativos que hospedam, como as lojas de aplicativos nativas. Além disso, lojas de aplicativos de terceiros podem buscar se diferenciar das lojas maiores e estabelecidas sendo mais permissivas com aplicativos que, de outra forma, seriam considerados indesejáveis. Por outro lado, as lojas de aplicativos nativas dedicam recursos consideráveis para melhorar a segurança dos aplicativos em seu mercado.

## Um Roadmap para Implementação da DMA

Exigir sistemas operacionais de dispositivos móveis inevitavelmente terá efeitos negativos na privacidade e segurança de seus ecossistemas, mas há maneiras de permitir com segurança que os usuários tenham maior acesso a aplicativos e lojas de

---

[42] https://www.apple.com/legal/more-resources/docs/2022-App-Store-Transparency-Report.pdf

[43] https://security.googleblog.com/2022/12/app-defense-alliance-expansion.html

terceiros, ao mesmo tempo em que oferecem aos desenvolvedores de terceiros maior acesso à funcionalidade do sistema operacional. Como indicamos acima e como as partes interessadas de primeira linha, como a Apple, atestaram, o cumprimento da DMA é quase certo de aumentar a prevalência de "malware, fraudes e golpes, conteúdo ilícito e prejudicial, e outras ameaças à privacidade e segurança".[44] No entanto, legisladores e formuladores de políticas podem mitigar esses problemas com orientações construtivas de implementação que permitam aos “gatekeepers” proteger seus consumidores.

Os estados membros da UE devem estar dispostos a defender os proprietários de lojas de aplicativos nativas e sistemas operacionais de dispositivos móveis, bem como os usuários, apoiando:

- Os “gatekeepers” devem realizar revisões básicas de aplicativos, independentemente do canal de distribuição. Isso pode exigir novos mecanismos incorporados aos sistemas operacionais ou contratos com lojas de aplicativos. Também pode haver uma maneira de usar certificações e avaliações de terceiros para demonstrar que os aplicativos são seguros.
- Os formuladores de políticas devem considerar avisos de descrição de aplicativos sobre funcionalidades básicas e informações essenciais, para ajudar os usuários e outros a entenderem como os aplicativos funcionam e qual é o seu propósito.
- Os sistemas operacionais podem implementar proteções aprimoradas para evitar que o malware prejudique a segurança e integridade do dispositivo móvel, incluindo ferramentas adicionais para isolar e proteger aplicativos entre si e para proteger o sistema operacional, dados do usuário e hardware do dispositivo contra aplicativos maliciosos. Essas ferramentas podem incluir ferramentas de MDM para administradores de empresas.
- Os “gatekeepers” devem estabelecer controles técnicos e contratuais para lojas de aplicativos de terceiros, a fim de garantir que possam ser confiáveis. Cada “gatekeeper” provavelmente escolherá um equilíbrio diferente entre diferentes mitigadores, mas deve ter um amplo conjunto de opções para proteger o dispositivo e os usuários que podem ser usadas para proteger os usuários enquanto trabalham para cumprir a DMA.
- Empresas “gatekeepers” precisam de orientações claras de que podem proteger seus usuários e devem ser dadas tempo adequado para conceber, construir, testar e comprovar novos sistemas para garantir a segurança de seus usuários.
- Reguladores devem prestar atenção às preocupações de segurança e integridade tanto em aplicativos quanto em lojas de aplicativos e reconhecer que nem todos os aplicativos e lojas são iguais. Eles devem apoiar o desenvolvimento de mecanismos para avaliar e garantir que desenvolvedores de aplicativos e lojas de aplicativos se comportem de maneira responsável e que possam ser responsabilizados se não o fizerem.
- Os “gatekeepers” desenvolvendo sistemas operacionais precisam ter a flexibilidade para ajustar as permissões e os modelos de segurança, bem como sua operação, para garantir que os desenvolvedores não possam se aproveitar do ecossistema em evolução. Os formuladores de políticas devem proteger a capacidade das lojas de aplicativos e sistemas operacionais de dispositivos de evoluir os tipos de mecanismos de segurança e limitações que estão disponíveis para integrar em seu ecossistema.
- Políticas que abordam ecossistemas de dispositivos móveis não devem enfraquecer a segurança desses ecossistemas. Os formuladores de políticas devem garantir que a segurança e a privacidade das plataformas continuem a melhorar e que ambas sejam incorporadas desde o início às plataformas e aplicativos. Propostas que ameacem o progresso feito devem ser reconsideradas.
- Os responsáveis pela formulação de políticas devem ser realistas sobre quais responsabilidades de segurança os usuários estão dispostos e aptos a assumir. Estudos observam que a conscientização sobre segurança não se correlaciona com a tomada de boas decisões de segurança.[45]

---

[44] https://www.apple.com/newsroom/2024/01/apple-announces-changes-to-ios-safari-and-the-app-store-in-the-european-union/

[45] https://www.ncbi.nlm.nih.gov/pmc/articles/PMC5352308/

- Os responsáveis pela formulação de políticas devem apoiar práticas baseadas em riscos para dispositivos móveis, em vez de impor práticas específicas sobre como os dispositivos móveis operam e quais aplicativos podem ser instalados.

## Conclusão

Com o DMA transformado em lei e os “gatekeepers” trabalhando para garantir sua conformidade, estamos entrando em uma transição crucial para o ecossistema de dispositivos móveis. O Center for Cybersecurity Policy and Law espera que legisladores, “gatekeepers” e o restante do ecossistema de dispositivos móveis possam trabalhar juntos para manter os usuários e seus dispositivos seguros e protegidos. Os legisladores devem considerar o impacto em termos de segurança para empresas, o ecossistema e os consumidores. Embora o impacto de muitos elementos de revisão e supervisão de lojas de aplicativos existentes seja difícil de quantificar, os investimentos feitos pelos desenvolvedores de lojas de aplicativos para proteger seus usuários devem ser reconhecidos e recompensados. Quando os proprietários e desenvolvedores de lojas de aplicativos tomam medidas para aprimorar a segurança e a privacidade, os usuários se beneficiam de maneiras das quais não têm conhecimento.

Não existe um sistema perfeito que proteja os usuários de todo o malware móvel, mas sabemos como diminuir significativamente o número de atividades indesejadas ou maliciosas que os usuários precisam considerar.