COFEM



Ficha Técnica 1:
Segurança Digital

Pontos principais



A violência digital não é um problema privado. Ela é frequentemente utilizada para silenciar, intimidar e excluir mulheres da vida pública.



A segurança digital eficaz começa pela compreensão dos seus riscos. Pergunte a si mesma o que você está protegendo, de quem está protegendo e quais seriam as consequências caso essas informações fossem expostas.



Senhas fortes, autenticação em dois fatores, comunicações seguras e configurações de privacidade continuam sendo algumas das medidas mais eficazes para proteger contra a violência e os riscos no ambiente digital.



A segurança digital é uma responsabilidade coletiva. Práticas organizacionais compartilhadas, procedimentos claros de resposta e redes de apoio contribuem para proteger equipes e movimentos como um todo.



A segurança digital e o bem-estar caminham juntos. Responder às violências no ambiente online exige apoio técnico, jurídico, psicossocial e emocional.



O objetivo não é abandonar os espaços digitais, mas participar deles de forma segura, confiante e em nossos próprios termos.

A política de estar online

O extraordinário de estar online é a rapidez com que pessoas, ideias e informações podem circular. Os espaços digitais nos permitem transitar. Transitamos entre comunidades, idiomas, países e conversas. Fazemos circular ideias, evidências e histórias. Encontramos umas às outras, construímos relações, contestamos narrativas dominantes e mobilizamos ações coletivas para além das fronteiras.

Mas esse movimento não diz respeito apenas ao que conquistamos. Os mesmos espaços digitais que possibilitam conexão, visibilidade e ação coletiva também podem nos expor a novas formas de vigilância, assédio e violência. Feministas em todo o mundo vêm defendendo, há muito tempo, que a violência contra as mulheres não é uma questão privada, mas uma violação sistêmica dos direitos humanos, entendimento refletido em marcos normativos internacionais, como a Declaração sobre a Eliminação da Violência contra as Mulheres, o Protocolo de Maputo e a Recomendação Geral nº 35 da CEDAW. O movimento #MeToo foi construído sobre esse legado. Criado em 2006 pela ativista Tarana Burke como uma iniciativa liderada por sobreviventes, ganhou visibilidade mundial quando a hashtag se tornou viral nas redes sociais em 2017. Em poucas semanas, milhões de pessoas, distribuídas por cerca de 85 países, compartilharam suas histórias online, demonstrando como os espaços digitais podem conectar experiências individuais à ação coletiva e à transformação social.[1]

Na Argentina, o movimento #NiUnaMenos surgiu em 2015 após o assassinato de Chiara Páez, de 14 anos, um caso que desencadeou ampla indignação pública diante do feminicídio. Um tuíte da jornalista Marcela Ojeda conclamando as mulheres a erguerem suas vozes contra os assassinatos motivados por questões de gênero rapidamente ganhou repercussão entre ativistas e redes culturais e de comunicação. Sob a bandeira de #NiUnaMenos ("Nem Uma a Menos"), a mensagem espalhou-se rapidamente pelo Twitter e pelo Facebook, contribuindo para mobilizar centenas de milhares de pessoas no que se tornou uma das maiores manifestações feministas da história da América Latina. Assim como o #MeToo, o movimento demonstrou como os espaços digitais podem transformar experiências individuais de violência em ação coletiva e pressão política por mudanças.[2]

Esses exemplos revelam algo importante: os espaços digitais nunca são neutros. As mesmas tecnologias que possibilitam a organização feminista e a ação coletiva são moldadas por relações de poder, disputas políticas e interesses concorrentes. À medida que o mundo se torna mais conectado, circular pelos espaços digitais também nos expõe a novas formas de violência. As mesmas tecnologias que permitem a difusão de ideias feministas também podem facilitar o assédio, a vigilância, a desinformação e os abusos.[3] A mesma visibilidade que nos ajuda a fortalecer movimentos pode nos transformar em alvos. As mesmas redes que alimentam conexões também podem se tornar canais pelos quais a violência se propaga.

Para as feministas que trabalham para eliminar a violência contra as mulheres e meninas (VAWG), a circulação de informações, histórias e recursos é uma de nossas maiores fortalezas. Podemos documentar injustiças, apoiar sobreviventes, aprender umas com as outras e organizar ações coletivas para além das fronteiras. No entanto, essa circulação digital de conhecimento também exige que reflitamos cuidadosamente sobre segurança, privacidade e riscos. Como, então, utilizar o poder do ambiente digital de forma intencional? Como aproveitar as possibilidades que os espaços digitais oferecem, ao mesmo tempo em que minimizamos os riscos que eles apresentam? Como permanecer visíveis sem nos tornarmos vulneráveis? Como proteger a nós mesmas, nossas organizações e as pessoas com quem trabalhamos, continuando, ao mesmo tempo, a participar plenamente da vida pública?

Esta ficha técnica apresenta algumas respostas práticas para essas questões. Ela parte da compreensão da violência digital como uma questão política, passa pela avaliação de riscos, pela implementação de medidas práticas de proteção, pelo fortalecimento da segurança coletiva e pelas formas de responder aos danos quando eles ocorrem.

[1] Sweeney J 2020

[2] https://8am.media/eng/ni-una-menos/

[3] Amnesty International, May 2021 Azerbaijan: Stop the Vicious Campaign of Gendered Smears and Reprisals against Women Activists. London: Amnesty International. Disponível em: https://www.amnesty.org

Em destaque

O caso de Narmin Shahmarzadeh[4]

Em 8 de março de 2021, a ativista pelos direitos das mulheres do Azerbaijão, Narmin Shahmarzadeh, participou da organização de uma marcha pelo Dia Internacional das Mulheres em Baku. Na manhã seguinte, ela acordou e descobriu que sua conta no Facebook havia sido invadida. Os responsáveis pelo ataque utilizaram sua conta para publicar conversas forjadas e conteúdo pornográfico. Também obtiveram acesso aos seus documentos de identificação, usaram seu documento oficial de identidade para impedir que ela recuperasse o acesso à própria conta e utilizaram seu cartão bancário para pagar anúncios destinados a promover o conteúdo abusivo. No Telegram, os perpetradores criaram um canal atribuindo falsamente imagens pornográficas a Narmin. Em pouco tempo, o canal já havia atraído mais de 1.600 inscritos e acumulado milhares de visualizações.

O ataque foi digital, mas seu objetivo era político. Narmin foi alvo porque era uma figura pública e visível. Ela havia organizado mobilizações, se manifestado publicamente e desafiado estruturas de poder. Os responsáveis pelo ataque transformaram justamente as ferramentas que haviam possibilitado seu ativismo em armas contra ela. Sua experiência ilustra uma realidade cada vez mais comum para mulheres defensoras dos direitos humanos e ativistas feministas. A violência digital é frequentemente planejada não apenas para intimidar indivíduos, mas também para destruir reputações, comprometer a credibilidade, enfraquecer os esforços de organização e criar um ambiente de medo. As consequências podem começar no ambiente online, mas raramente permanecem restritas a ele.

O custo da visibilidade

A experiência de Narmin não é um caso isolado. Ela ilustra um padrão mais amplo no qual a violência digital é utilizada para punir a visibilidade, desarticular o ativismo e restringir a participação das mulheres na vida pública. Cada vez mais, os abusos cometidos no ambiente online não permanecem restritos aos espaços digitais; eles transbordam para o mundo físico, afetando a segurança, o bem-estar, os meios de subsistência e a capacidade das mulheres de participar da vida pública e política

O impacto da violência digital sobre mulheres que atuam na vida pública é amplo e está se intensificando. Um estudo da ONU Mulheres, publicado em 2025 e realizado com mais de 640 mulheres em 119 países, constatou que 70% das mulheres defensoras dos direitos humanos (WHRDs), ativistas, jornalistas e comunicadoras públicas relataram ter sofrido violência no ambiente online no exercício de seu trabalho — e as consequências não permanecem restritas ao ambiente digital. Quarenta e um por cento das participantes informaram ter sofrido violências no mundo offline, incluindo agressões físicas, perseguição (stalking) e assédio verbal, que associaram diretamente à violência iniciada nos espaços digitais. Entre as mulheres defensoras dos direitos humanos e ativistas, esse percentual chegou a 44%. A passagem da violência online para a violência offline também vem se acelerando. Entre jornalistas e profissionais da mídia, a proporção das que relacionaram a violência sofrida no ambiente online a danos vivenciados no mundo offline mais que dobrou entre 2020 e 2025, passando de 20% para 42%. Quase um quarto de todas as participantes relatou ter sido vítima de violência online assistida por inteligência artificial, enquanto 28% das mulheres defensoras dos direitos humanos (WHRDs) e ativistas afirmaram que tecnologias de inteligência artificial foram utilizadas nas violências dirigidas contra elas. O relatório é categórico ao afirmar qual é o objetivo dessa violência: trata-se de um instrumento estratégico utilizado para restringir a liberdade de expressão das mulheres, impedir sua participação democrática e enfraquecer seus direitos à igualdade de gênero, produzindo efeitos que, como destacam as autoras, estão longe de ser apenas virtuais.[5]

No entanto, reconhecer esses riscos não deve nos levar a abandonar os espaços digitais nem a aceitar a violência como o preço da participação. Mulheres, meninas e pessoas com identidades de gênero diversas têm o direito de ser visíveis, de se expressar livremente, de construir comunidades, de se organizar, de criar e de vivenciar a alegria no ambiente online sem medo de abusos. O objetivo não é nos tornarmos menos visíveis ou menos presentes nos espaços digitais, mas transformá-los para que todas as pessoas possam participar de forma segura, em condições de igualdade e com dignidade. Assim, proteger-nos no ambiente online não significa apenas reduzir danos; significa também defender a internet como um espaço de expressão, solidariedade, criatividade e de fortalecimento das possibilidades feministas.

[4] Ibid
[5] Posetti et al., UN Women, December 2025

Avaliando seus riscos

Embora governos, empresas de tecnologia e plataformas digitais tenham a responsabilidade primordial de criar ambientes digitais mais seguros, as medidas de proteção e os mecanismos de responsabilização atualmente disponíveis ainda são desiguais e insuficientes. Nesse contexto, organizações feministas e ativistas podem optar por adotar medidas práticas para ajudar a minimizar os riscos. Essas medidas não eliminam a violência, nem devem transferir a responsabilidade daqueles que a praticam; no entanto, podem fortalecer nossa capacidade de ocupar e utilizar os espaços digitais em nossos próprios termos.

Nem toda ameaça se aplica da mesma forma a todas as ativistas, organizações ou movimentos. Uma pesquisadora feminista que trabalha com depoimentos de sobreviventes enfrenta riscos diferentes daqueles enfrentados por uma ativista que conduz campanhas nas redes sociais. Da mesma forma, uma defensora dos direitos humanos que documenta a violência praticada pelo Estado enfrenta desafios distintos dos de uma prestadora de serviços que coordena um grupo local de apoio. Em vez de perguntar: "*Qual é a opção mais segura?*", uma pergunta mais útil é: "*O que estou tentando proteger e de quem?*".

Para algumas organizações, isso pode significar proteger informações de sobreviventes, arquivos de casos ou bancos de dados de contatos. Para outras, a prioridade pode ser proteger a identidade de suas equipes, garantir a segurança das comunicações ou resguardar suas contas em redes sociais. Ativistas individuais podem estar preocupadas com doxxing, perseguição (stalking), assédio no ambiente online ou com a exposição de informações pessoais que possam colocar em risco a si mesmas ou suas famílias. Não existe uma abordagem única que seja adequada para todas as pessoas. As avaliações de risco são mais eficazes quando refletem o contexto, as prioridades e o nível de exposição pública de cada pessoa, permitindo decisões informadas sobre quais medidas de proteção são mais apropriadas. A experiência de Narmin Shahmarzadeh demonstra como um ataque digital pode se agravar rapidamente quando informações pessoais, documentos de identidade e contas em redes sociais são comprometidos. Compreender quais informações, relações e contas são mais importantes de proteger constitui, portanto, um ponto de partida essencial para reduzir vulnerabilidades e minimizar riscos.

Uma avaliação de risco simples pode começar com quatro perguntas:[6]

- Quais informações, dados ou ativos estou tentando proteger?
- Quem pode ter interesse em acessá-los?
- Quais métodos essas pessoas ou grupos podem utilizar para obter esse acesso?
- Quais seriam as consequências caso essas informações fossem expostas?

A maioria das organizações não dispõe de tempo, recursos financeiros ou conhecimento técnico ilimitados para se preparar para todas as ameaças possíveis. O objetivo, portanto, é tomar decisões informadas sobre os riscos mais relevantes para o seu contexto e priorizar seus esforços de acordo com eles. Depois de compreender quais são esses riscos, torna-se muito mais fácil identificar as medidas práticas que terão o maior impacto na sua proteção.

[6] Essas perguntas baseiam-se em abordagens consolidadas de modelagem de ameaças (threat modelling) na área de cibersegurança, adaptadas às práticas feministas de segurança digital. Consulte, por exemplo, *Participatory Threat* Modelling, 2021 de Slupska et al.



Protegendo suas contas e dispositivos

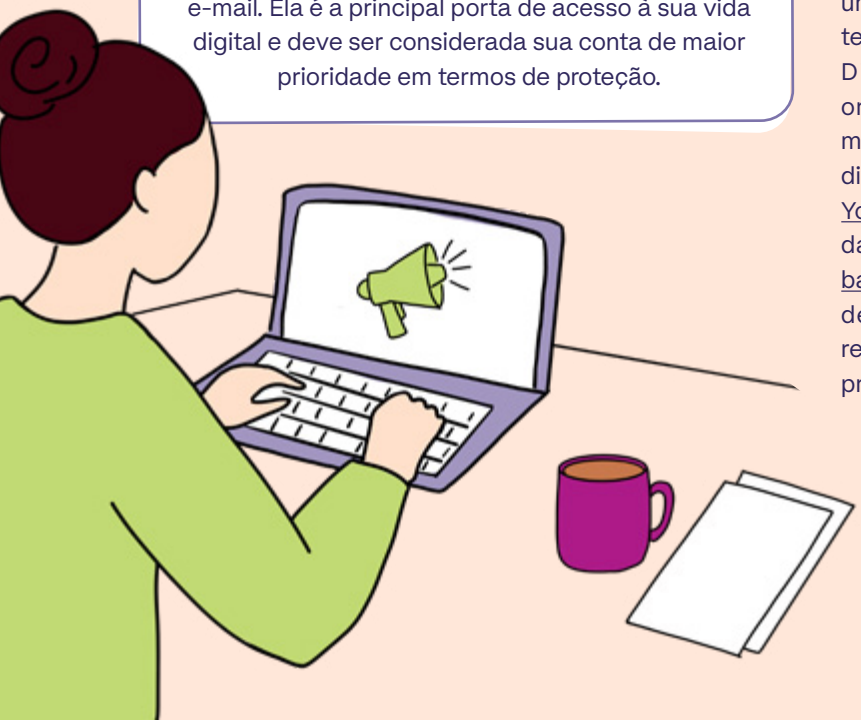
O ponto de entrada mais comum para incidentes graves de violência digital é o comprometimento de contas: quando alguém obtém acesso ao seu e-mail, às suas redes sociais ou a outras contas por meio de uma senha roubada, descoberta ou reutilizada. Uma vez comprometida a conta de e-mail, todas as demais contas vinculadas a ela também se tornam vulneráveis. Para ativistas feministas, pesquisadoras e defensoras dos direitos humanos, as consequências podem ir muito além de um simples transtorno pessoal, expondo fontes, sobreviventes, colegas e comunicações sensíveis. A experiência de Narmin Shahmarzadeh demonstra como o comprometimento de uma conta pode se agravar rapidamente. Os responsáveis pelo ataque obtiveram acesso à sua conta em uma rede social, utilizaram sua identidade para disseminar conteúdo forjado e impediram que ela recuperasse o acesso ao próprio perfil. O que começou como uma invasão digital rapidamente se transformou em um ataque à sua reputação e ao seu bem-estar psicológico.

A boa notícia é que algumas das medidas de proteção mais eficazes também são as mais simples:

Utilize senhas fortes e exclusivas para cada conta e armazene-as em um gerenciador de senhas confiável, como Bitwarden ou 1Password. Gerenciadores de senhas geram e armazenam senhas complexas, eliminando a prática comum — e arriscada — de reutilizar a mesma senha em diversas plataformas.

Combine essa medida com a autenticação em dois fatores (2FA) em todas as contas que ofereçam esse recurso. Sempre que possível, utilize um aplicativo autenticador em vez da verificação por SMS, que pode ser vulnerável a ataques de troca de chip (*SIM swapping*). Dê atenção especial à sua conta de e-mail. Ela é a principal porta de acesso à sua vida digital e deve ser considerada sua conta de maior prioridade em termos de proteção.

A segurança dos dispositivos também é fundamental. Mantenha o sistema operacional, os navegadores e os aplicativos sempre atualizados, pois essas atualizações frequentemente corrigem vulnerabilidades exploradas por pessoas mal-intencionadas. Ative a criptografia completa do disco (*full-disk encryption*) em computadores e utilize um software antivírus confiável, quando apropriado. Tenha cautela ao abrir links, anexos ou solicitações de login inesperados. Ataques de phishing continuam sendo uma das formas mais eficazes de roubo de credenciais e de instalação de programas maliciosos (*malware*).



As recomendações acima constituem um ponto de partida prático, mas a segurança digital não é uma lista de verificação a ser cumprida apenas uma vez. Trata-se de uma prática contínua, que precisa evoluir à medida que as tecnologias e as ameaças se transformam.

Diversas organizações feministas desenvolveram orientações acessíveis e adaptadas às experiências de mulheres, meninas e pessoas com identidades de gênero diversas. Entre elas estão os Digital Security Resources for Young Women, da FRIDA; o GitBook; o Online Safety Guide, da ONU Mulheres; e o Youth Guide to End Online Gender-based Violence. Esses recursos oferecem orientações mais detalhadas sobre como fortalecer o bem-estar digital, responder aos abusos no ambiente online e desenvolver práticas mais seguras de segurança digital.

Gerenciando sua pegada digital e sua privacidade

Cada fotografia, marcação de localização, atualização de perfil e publicação nas redes sociais contribui para a sua pegada digital. Para ativistas feministas e mulheres defensoras dos direitos humanos (WHRDs), esses elementos aparentemente insignificantes podem revelar muito mais informações do que o pretendido. Gerenciar sua pegada digital não significa tornar-se invisível. Significa agir de forma intencional. Comece revisando quais informações você disponibiliza publicamente. Configure as opções de privacidade em suas redes sociais, prestando especial atenção a quem pode marcar você em publicações, encontrá-la por meio de buscas ou visualizar seu conteúdo. Revise essas configurações regularmente, pois as plataformas frequentemente alteram suas configurações padrão de privacidade sem aviso prévio.

Pense com atenção sobre as informações de localização. Check-ins em tempo real, fotografias com geolocalização e publicações que revelem onde você e sua família moram, trabalham ou passam períodos significativos podem facilitar o rastreamento de seus deslocamentos por outras pessoas. Fotografias tiradas com smartphones frequentemente contêm metadados de localização por padrão, que devem ser removidos antes do compartilhamento público de imagens sensíveis.

Para comunicações sensíveis, utilize ferramentas desenvolvidas com foco na privacidade:

- O Signal continua sendo uma das opções mais confiáveis para mensagens e chamadas com criptografia de ponta a ponta.
- Para e-mails, provedores voltados à proteção da privacidade, como o Proton Mail, oferecem camadas adicionais de segurança em comparação com os serviços convencionais.
- Revise regularmente as permissões concedidas aos aplicativos e remova acessos desnecessários à sua localização, ao microfone, à câmera e aos seus contatos.
- Ao trabalhar em espaços públicos, evite acessar informações sensíveis por meio de redes Wi-Fi não seguras. Caso isso seja inevitável, considere utilizar uma VPN confiável para proteger sua conexão.

Nenhuma dessas medidas é particularmente complexa. No entanto, quando adotadas de forma consistente, podem reduzir significativamente a exposição aos riscos.

Proteção coletiva e organizacional

A segurança digital costuma ser apresentada como uma responsabilidade individual. No entanto, no contexto das organizações e dos movimentos feministas, o comprometimento de uma única conta pode expor as comunicações, os contatos e o trabalho de toda uma equipe. Uma única senha fraca em uma plataforma compartilhada pode criar vulnerabilidades para todas as pessoas colaboradoras. Por isso, a segurança digital deve ser compreendida como uma prática de cuidado coletivo, e não como uma questão individual de competência. Esse processo começa com o estabelecimento de práticas compartilhadas. Definam quais ferramentas serão utilizadas para comunicações sensíveis, estabeleçam requisitos mínimos para o uso de senhas fortes e autenticação em dois fatores e assegurem que as contas institucionais não dependam exclusivamente do dispositivo ou do perfil de uma única pessoa.

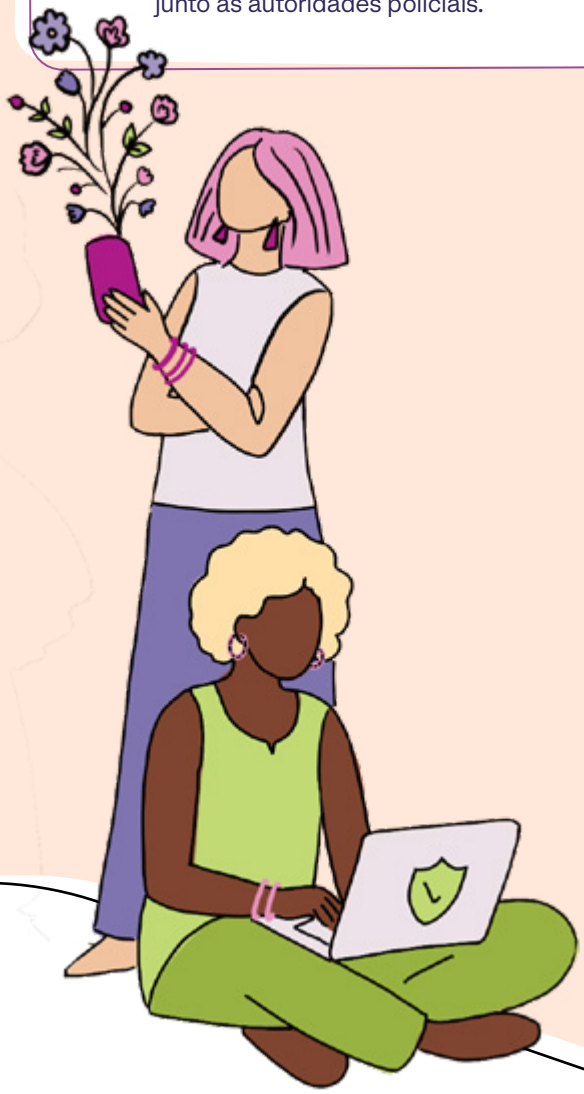
Quando integrantes deixam a organização, seu acesso às contas compartilhadas deve ser removido de forma imediata e sistemática. Igualmente importante é criar estruturas de apoio antes que elas sejam necessárias. Identifiquem pessoas de confiança em suas redes que possam oferecer suporte técnico, orientação jurídica ou apoio psicossocial caso você ou alguém da organização seja alvo de um ataque. Desenvolvam procedimentos internos simples para responder a incidentes como invasão de contas, doxxing ou comprometimento de contas. Saber antecipadamente quem será responsável por cada ação durante uma situação de crise pode reduzir significativamente a confusão e os danos. As organizações feministas investem regularmente na segurança física e no bem-estar de suas equipes e comunidades. A segurança digital merece a mesma atenção.

Como responder a incidentes e priorizar o bem-estar

Ataques digitais e o assédio no ambiente online costumam causar impactos ainda maiores quando as pessoas não dispõem de um plano para responder a essas situações. Estabelecer um protocolo básico de resposta antes que um incidente ocorra pode fazer toda a diferença.

Documente

Quando ocorrer um episódio de assédio ou o comprometimento de uma conta, documente a situação antes de qualquer outra ação. Faça capturas de tela, salve os URLs, registre os nomes de usuário e preserve todas as evidências antes que o conteúdo seja excluído ou removido. Essa documentação pode ser essencial para denúncias às plataformas, medidas judiciais ou registros de ocorrência junto às autoridades policiais.



Denuncie

Saiba onde buscar apoio. Embora os mecanismos de denúncia das plataformas apresentem limitações, eles continuam sendo um primeiro passo importante, especialmente em casos que envolvam ameaças de violência, falsificação de identidade, perseguição (stalking) ou abuso baseado em imagens. Muitos países contam com organizações que oferecem apoio jurídico, psicossocial ou técnico a ativistas que enfrentam violência no ambiente digital. Familiarize-se com esses recursos antes que uma situação de crise ocorra e mantenha seus contatos sempre facilmente acessíveis.

Cuide de si

O impacto emocional da violência no ambiente digital é significativo. Abusos de natureza sexual, conteúdos forjados, campanhas coordenadas de assédio e ameaças persistentes são estratégias utilizadas para esgotar, isolar e intimidar. Seus efeitos são reais, cumulativos e, muitas vezes, invisíveis para as outras pessoas. Por isso, o planejamento da segurança digital deve sempre incluir o cuidado com o bem-estar. Converse com colegas de confiança. Afaste-se das redes sociais quando necessário. Utilize, sem receio, as funções de silenciar, bloquear e restringir. Procure apoio profissional caso os impactos se tornem excessivos. Segurança digital e bem-estar não são preocupações distintas. São duas dimensões de um mesmo compromisso: garantir que ativistas feministas, organizações e movimentos possam continuar desenvolvendo seu trabalho de forma segura, sustentável e em seus próprios termos.

Visibilidade, segurança e poder

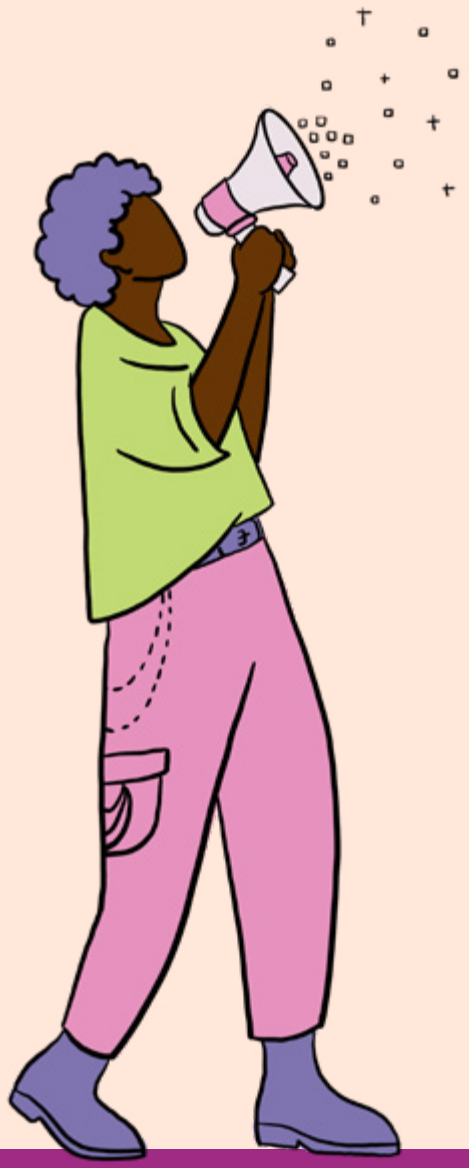
Segurança digital diz respeito à possibilidade de participar da vida pública em nossos próprios termos. Os movimentos feministas sempre precisaram se adaptar a cenários políticos em constante transformação, encontrando novas formas de organização, comunicação e construção de poder. Hoje, os espaços digitais fazem parte desse cenário. Eles nos permitem compartilhar conhecimentos, apoiar sobreviventes, enfrentar injustiças e estabelecer conexões para além das fronteiras de maneiras que seriam inimagináveis há apenas uma geração. Ao mesmo tempo, também criam novos riscos que exigem atenção, preparação e cuidado.

O objetivo é possibilitar escolhas informadas sobre os riscos, fortalecer a proteção coletiva e desenvolver a confiança necessária para continuar participando dos espaços digitais de forma segura e estratégica. Nesse sentido, a segurança digital é, ao mesmo tempo, uma questão técnica e uma questão relacionada aos movimentos sociais. Quando ativistas feministas, organizações e comunidades conseguem se comunicar com segurança, proteger umas às outras e responder de maneira eficaz às situações de violência, tornam-se mais capazes de sustentar o trabalho de promoção de direitos, apoio às sobreviventes e transformação social. Nossos movimentos dependem da conexão entre as pessoas. A segurança digital contribui para que essas conexões permaneçam uma fonte de fortalecimento, e não de vulnerabilidade.

Recursos

As organizações e os recursos a seguir oferecem apoio gratuito e prático em segurança digital:

Recurso	O que oferece
Linha direta de segurança Digital da Access Now(Access Now Digital Security Helpline)	Suporte gratuito e confidencial em segurança digital para ativistas, jornalistas e defensoras(es) de direitos humanos em todo o mundo, incluindo a África do Sul.
Coalizão contra a violência Online (Coalition Against Online Violence (CAOV))	Recursos e apoio específicos para mulheres jornalistas e para casos de assédio online baseado em gênero.
Manual prático sobre assédio online da PEN America (PEN America Online Harassment Field Manual)	Orientações práticas e abrangentes sobre como responder ao assédio online, disponíveis gratuitamente.
Iniciativa pelos direitos civis no ambiente digital (Cyber Civil Rights Initiative)	Apoio a sobreviventes de abuso relacionado ao compartilhamento não consensual de imagens íntimas, além de recursos jurídicos e orientações para denúncias às plataformas.
Electronic Frontier Foundation — Autodefesa contra a vigilância (Electronic Frontier Foundation (EFF) — Surveillance Self-Defence)	Guias gratuitos e práticos de segurança digital para ativistas e jornalistas, organizados de acordo com o nível de risco.
Front Line Defenders	Apoio em segurança digital e proteção para defensoras(es) de direitos humanos em todo o mundo.
Feminist Tech Exchange	Recursos sobre tecnologia e segurança digital desenvolvidos especificamente para organizações feministas.



Agradecimentos

Este material foi elaborado por Joy Watson e revisado por Jennifer Chinoye Amadi, Leah Goldmann, Lauren Messina e integrantes da equipe de Eliminação da Violência contra as Mulheres (EVAW) da ONU Mulheres. O projeto gráfico foi desenvolvido por Mara Ayuningtyas e Léa Drougard, e as ilustrações são de Sarah Imran. Esta publicação foi produzida pela COFEM no âmbito do Programa ACT para Acabar com a Violência contra as Mulheres e Meninas, da ONU Mulheres, financiado pela União Europeia. Seu conteúdo é de exclusiva responsabilidade da COFEM e não reflete necessariamente as opiniões da União Europeia ou da ONU Mulheres.

Citação sugerida

Coalition of Feminists for Social Change. Ficha Técnica 2: Segurança Digital. Bytes de Resistência: Enfrentando a Violência Baseada em Gênero Facilitada pela Tecnologia (2026).

Referências

Amnesty International (2021) Azerbaijan: Stop the vicious campaign of gendered smears and reprisals against women activists. London: Amnesty International. Disponível em: https://www.amnesty.org

Andreasen, M.B. (2020) 'Feminist/activist responses to online abuse', in The International Encyclopaedia of Gender, Media, and Communication. Hoboken: Wiley.

Andreasen, M.B. (2024) 'Evidentiary activism in the digital age: on the rise of feminist struggles against gender-based online violence', in Edited volume title. London: Routledge.

Bansal, V., Eruyar, S., Wang, S. & Wessells, M. (2024) 'A scoping review of technology-facilitated gender-based violence in low- and middle-income countries across Asia', Trauma, Violence, & Abuse, online.

Bennett, L. and Livingston, S. (2020) 'The #MeToo movement, digital media and the public sphere', in Digital Media and the Public Sphere. London: Routledge.

Koch, L., Russo Riva, M.P. & Steinert, J.I. (2025) 'Technology-facilitated gender-based violence against politically active women: A systematic review of psychological and political consequences and women's coping behaviours', Trauma, Violence, & Abuse, online.

Loney-Howes, R. and Mendes, K. (2023) 'It's a global #MeToo: A cross-national comparison of social media responses to sexual violence', Feminist Media Studies, 24(7), pp. 1032–1050.

Posetti J, Hellmueller L, Williams K, Renaud P, Aboulez N and Shabbir N 2025 *Tipping Point: The Chilling Escalation of Online Violence Against Women in the Public Sphere*, UN Women, New York.

UN Women (2025) AI and anonymity: Digital violence against women in the age of online backlash. New York: UN Women.

VAWG Helpdesk (2017) Cyber VAWG: Violence against women and girls and information and communications technology. VAWG Helpdesk Research Report No. 211. London: UK Aid.

Slupska J, Dawson S, Ma L and Neff G (2021) Participatory Threat Modelling: Exploring Paths to Reconfigure Cybersecurity. Proceedings of the ACM on Human-Computer Interaction.

Sweeney J 2020 The *#Me Too Movement in Comparative Perspective, Journal of Gender, Social Policy and the Law, Volume 29*, Issue 1, 2020

Organized Crime and Corruption Reporting Project (OCCRP) (2023) 'How revenge porn is used to silence dissidents in Azerbaijan', OCCRP, 3 April. Disponível em: https://www.occrp.org/en/feature/how-revenge-porn-is-used-to-silence-dissidents-in-azerbaijan