ALFABETIZAÇÃO E SEGURANÇA DIGITAL

A IMPORTÂNCIA DE SE MANTER SEGURO E INFORMADO

OEA | Mais direitos para mais pessoas

SUMÁRIO

CRÉDITOS

Equipe Técnica Twitter

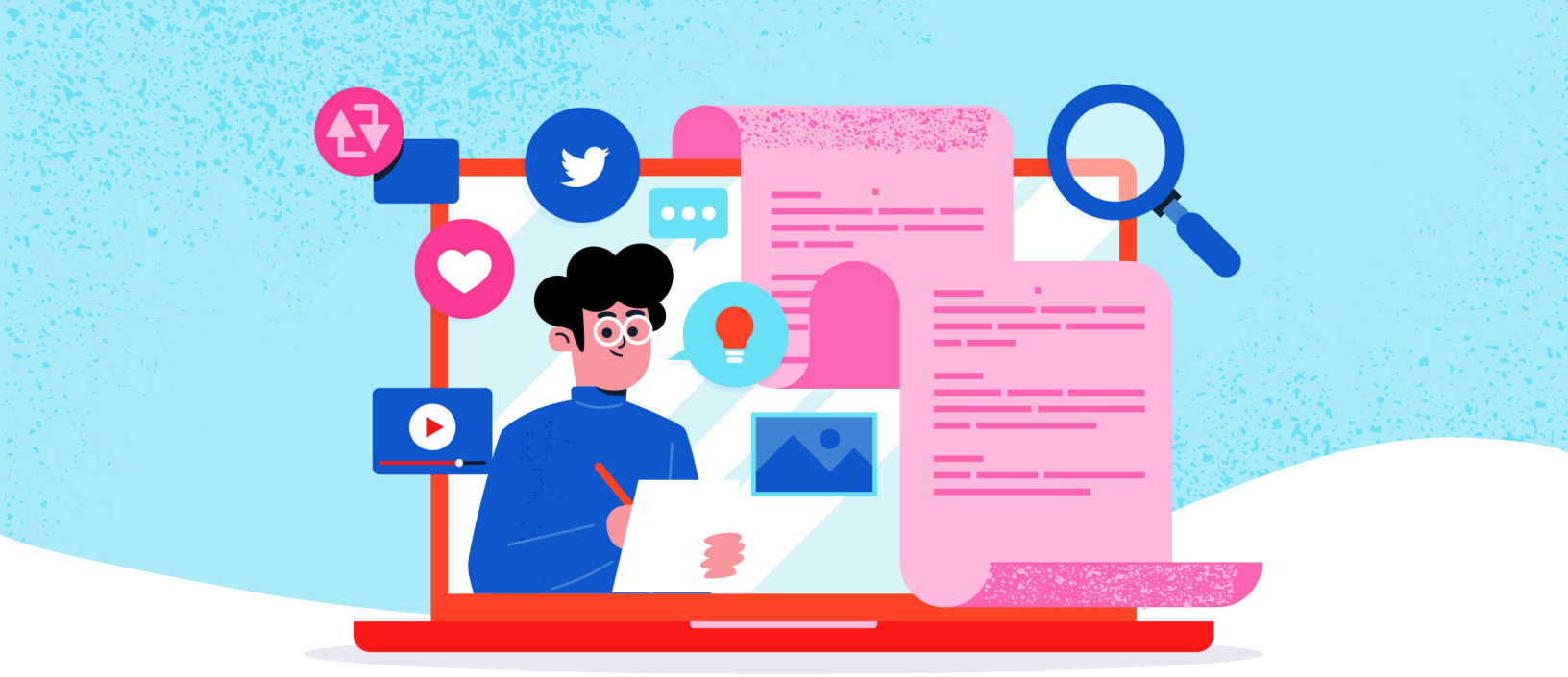
Andrea Pereira Palacios
Hugo Rodríguez Nicolat

Equipe técnica OEA

Alison August Treppel
Kerry-Ann Barrett
Gerardo De Icaza
Gonzalo Espáriz
Cristóbal Fernández
Mariana Jaramillo
Yerutí Méndez
Gabriela Montes de Oca
David Moreno
María Isabel-Rivero
Diego Subero
Katya Vera Morales

Design e Layout

Michelle Felguérez



INTRODUÇÃO

Na era digital e de redes sociais, a disponibilidade de informação imediata e abundante contribui para que as pessoas se mantenham em dia com o que ocorre no mundo de forma instantânea. Além disso, a digitalização e a transformação de processos cotidianos são dois procedimentos que acontecem de maneira rápida e imparável.

Para receber e processar informação abundante e facilmente acessível, são necessárias certas habilidades que devem ser desenvolvidas, além do entendimento dos meios nos quais ela circula. É importante conhecer não somente a origem, a intenção ou a finalidade da informação que se consome e se publica, mas também os possíveis riscos e o impacto que podem ter em nosso entorno.

Diante desse cenário, o **Twitter** e a **Organização dos Estados Americanos (OEA)** atualizaram esta publicação sobre alfabetização e segurança digital, com o objetivo de oferecer ferramentas e apresentar boas práticas no monitoramento, consumo e distribuição de informação, bem como recomendações para manter-se seguro online, com especial enfoque no Twitter. Nesta edição atualizada do guia *"Alfabetismo e Segurança Digital: melhores práticas no uso do Twitter"*[1], de setembro de 2019, somam-se à edição anterior outros fenômenos concernentes à desinformação e à importância da alfabetização em processos democráticos.

Desde o lançamento da primeira edição deste guia, o mundo experimentou um crescimento vertiginoso das atividades na Internet. De acordo com estudos da Comissão Econômica para a América Latina e o Caribe (CEPAL), das Nações Unidas, os avanços na utilização das redes e da infraestrutura de comunicações, cuja previsão de concretização era de anos, aconteceram em poucos meses a partir de 2020[2]. A CEPAL também salienta a necessidade do desenvolvimento de habilidades digitais como condicionante fundamental para o aproveitamento da Internet.

1 Organização dos Estados Americanos e Twitter. (2019). Alfabetização e Segurança Digital: melhores práticas no uso do Twitter. https://www.oas.org/es/sms/cicte/docs/20190913-DIGITAL-Alfabetismo-y-seguridad-digital-Twitter.pdf.
2 Comissão Econômica para a América Latina e o Caribe (CEPAL). Relatório Especial Covid-19.(2020). Universalizar o acesso às tecnologias digitais para enfrentar os efeitos da Covid-19. https://repositorio.cepal.org/bitstream/handle/11362/45938/4/S2000550_es.pdf.

Tanto a OEA como o Twitter puderam observar diversas mudanças nesse panorama. Na América Latina, mais de 30% das empresas perceberam um aumento do número de ataques cibernéticos em 2019, em comparação com anos anteriores, embora apenas 17% delas disponham de um seguro de risco cibernético[3]. Isso mostra a importância de ações voltadas para o aumento da conscientização sobre as ameaças digitais existentes na região e como combatê-las em todos os níveis. Por sua vez, o Twitter, por ser uma plataforma pública e aberta para o intercâmbio de perspectivas, ideias e informação, se mantém em um processo constante de atualização de suas regras, processos, ferramentas e tecnologia, o que é necessário para a adaptação da plataforma de maneira paralela às mudanças que se apresentam na sociedade e à forma mediante a qual as pessoas interagem e partilham informação em seu serviço.

A primeira seção da publicação se centra em definir o que é alfabetização digital, fazendo referência ao trabalho realizado pela Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO) e pela Comissão Interamericana de Direitos Humanos (CIDH). Esses enfoques refletem o desenvolvimento do termo "alfabetização" e sua relação com a tecnologia, além de considerações regionais sobre a alfabetização digital. Também foi incluída uma seção específica elaborada pelo Departamento de Cooperação e Observação Eleitoral (DCOE) da OEA com respeito à relação entre a alfabetização digital e a democracia.

A segunda seção focaliza boas práticas de segurança cibernética, apresentando informação relativa à natureza de novas ameaças cibernéticas que surgiram desde a primeira publicação deste guia. São igualmente incluídas recomendações específicas que respondem ao aumento das condições de teletrabalho ou trabalho remoto e ao trabalho jornalístico na região.

A terceira seção ampliou e atualizou a informação referente ao consumo de informação no Twitter e conselhos para verificar sua veracidade, além de discorrer sobre algumas das ferramentas disponíveis para melhor navegar na plataforma e encontrar e verificar informação de maneira fácil e rápida.

Finalmente, **na última seção** do guia, dada a importância do Twitter como ferramenta de comunicação, se oferece uma atualização das Regras do Twitter e sua aplicação, com o propósito de divulgar os parâmetros que regem a circulação de informação e interações na plataforma. Também são apresentadas nessa seção as ferramentas de segurança do Twitter, com uma explicação sobre como utilizá-las, com vistas a uma experiência mais personalizada e controlada na plataforma.

A tecnologia e as ferramentas disponíveis para seu uso estão em constante desenvolvimento, razão pela qual se insiste em que todas as pessoas se mantenham constantemente atentas às atualizações de produtos e políticas que afetam seu desenvolvimento e interações em meios digitais e redes sociais.

CONTAR COM HABILIDADES PARA DESENVOLVER-SE DE MANEIRA SEGURA NA INTERNET É FUNDAMENTAL PARA NEUTRALIZAR OS ATAQUES CIBERNÉTICOS E OUTROS MECANISMOS DE DESINFORMAÇÃO QUE SÃO CADA VEZ MAIS SOFISTICADOS E COMPLEXOS.

3 Marsh e Microsoft. (2020). Situação de risco cibernético na América Latina em tempos de Covid-19. https://coronavirus.marsh.com/mx/es/insights/research-and-briefings/report-cyber-risk-in-latin-america-in-times-of-covid19.html

ALFABETIZAÇÃO DIGITAL

O que é alfabetização digital?

De acordo com a UNESCO, alfabetização se define como:

> **Um meio de identificação, compreensão, interpretação, criação e comunicação em um mundo cada vez mais digital, baseado em textos, rico em informação e em rápida mutação[4].**

Essa definição, cunhada de forma oficial em anos recentes, considera que as habilidades digitais são um componente fundamental da alfabetização em geral, diferentemente de noções anteriores que somente levam em conta o conjunto de competências de leitura, escrita e cálculo.

Da mesma forma, no anuário de 2016 da UNESCO, na seção "Alfabetização Midiática e Informacional para os Objetivos de Desenvolvimento Sustentável", encontram-se as "Cinco Leis para a Alfabetização Midiática e Informacional", a saber:

4 Organização das Nações Unidas para a Educação, a Ciência e a Cultura (UNESCO). (2016). Alfabetização. https://es.unesco.org/themes/alfabetizacion

1. A informação, a comunicação, as bibliotecas, os meios de comunicação, a tecnologia, a Internet e outras fontes de informação pertencem à mesma categoria de informação. Nenhuma é mais relevante que a outra nem deve ser tratada como tal.
2. Cada cidadão é um criador de informação ou conhecimento e portador de uma mensagem. Todas as pessoas devem ter a faculdade de acessar informação nova e expressar-se livremente.
3. A informação, o conhecimento e as mensagens nem sempre são isentas de valores ou preconceitos. Qualquer conceituação, uso e aplicação de alfabetização digital deve apresentar esse fato de maneira transparente e compreensível a todos os cidadãos.
4. Todo cidadão deseja conhecer e compreender informação, conhecimentos e mensagens novos, bem como comunicar-se, e seus direitos nunca devem ser comprometidos.
5. A alfabetização digital é um processo dinâmico de experiências vividas. Considera-se completa quando inclui conhecimentos, habilidades e atitudes, quando abrange o acesso, a avaliação, o uso, a produção e a comunicação de informação, de conteúdo midiático e tecnológico.

É importante levar em conta essas noções para compreender a importância da aquisição de ferramentas digitais para o correto uso da Internet por qualquer pessoa.

Como alcançar a alfabetização digital?

Adquirir ferramentas digitais tem impacto direto em nosso nível de alfabetização. No anuário da UNESCO, citado no primeiro parágrafo desta seção, mencionam-se dez habilidades que devem ser desenvolvidas para alcançar a alfabetização digital[5]. Essas habilidades são:

1. Interagir com informação referente aos meios de comunicação e à tecnologia.
2. Ser capaz de aplicar habilidades técnicas de comunicação de informação para processar informação e produzir conteúdo midiático.
3. Utilizar a informação de maneira ética e responsável e transmitir sua compreensão ou conhecimento adquirido a uma audiência ou leitores na forma e meio apropriados.
4. Extrair e organizar informação e conteúdos.
5. Avaliar de forma crítica a informação e o conteúdo apresentado nos meios informativos e outras fontes de informação, inclusive meios *online*, em termos de autoridade, credibilidade, propósito e possíveis riscos.

5 Grizzle, A and Singh, J. (2016). In the MILID Yearbook 2016: Media and Information Literacy for the Sustainable Development Goals.

6. Localizar e acessar informação relevante.
7. Resumir as ideias extraídas do conteúdo.
8. Compreender as condições sob as quais essas ideias ou funções podem ser concretizadas.
9. Compreender o papel e as funções dos meios de comunicação, inclusive meios online, na sociedade e seu desenvolvimento.
10. Reconhecer e articular a necessidade de informação e dos meios de comunicação.

A alfabetização digital para combater a desinformação

Levando em consideração as habilidades digitais apresentadas na seção anterior, um tema de suma relevância relacionado à alfabetização digital é a presença da desinformação na Internet. De acordo com a Relatoria Especial para a Liberdade de Expressão (RELE) da CIDH, por meio de seu Guia para garantir a liberdade de expressão frente à desinformação deliberada em contextos eleitorais, a desinformação pode ser definida - em termos práticos e provisórios- como a divulgação maciça de informação falsa:

a. com a intenção de enganar o público; e
b. com conhecimento de sua inautenticidade.

Embora esse fenômeno não seja novo, os desdobramentos tecnológicos recentes tornaram possível que se replique de forma acelerada, alcançando maior número de pessoas e com consequências em diversas esferas da vida pública[6]. Da mesma forma, a existência da desinformação salienta a necessidade de que se desenvolva a habilidade de avaliar informação de forma crítica, já que, se a informação carece de autoridade, credibilidade e propósito, e se propaga da mesma forma, seus impactos podem ser consideráveis.

Nesse mesmo guia, a RELE enfatiza o impacto que a desinformação pode ter em contextos eleitorais. Por esse motivo, formula uma série de recomendações para os diferentes atores que deles participam. Essas recomendações visam principalmente a ajudar as partes envolvidas a abordar problemas de desinformação, sem esquecer possíveis efeitos secundários que poderiam afetar negativamente normas de D ireitos H umanos.

Algumas dessas recomendações em matéria de desinformação no contexto de processos eleitorais[7], que se centram, em grande medida, na necessidade de contribuir para a alfabetização e a segurança digital, figuram abaixo.

6 Organização dos Estados Americanos. (2019). Guia para garantir a liberdade de expressão frente à desinformação deliberada em contextos eleitorais. http://www.oas.org/es/cidh/expresion/publicaciones/Guia_Desinformacion_VF.pdf
7 A lista completa de recomendações pode ser encontrada no Guia para garantir a liberdade de expressão frente à desinformação deliberada em contextos eleitorais, páginas 30-51.

Para os Estados, inclusive os diferentes poderes públicos e autoridades eleitorais:

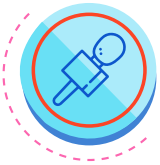
- Evitar estabelecer estruturas normativas que responsabilizem intermediários por conteúdos produzidos por terceiros.
- Fortalecer as estruturas jurídicas de proteção de dados pessoais.
- Lembrar as responsabilidades especiais dos altos funcionários públicos no exercício de sua própria liberdade de expressão.
- Realizar ações positivas de educação, capacitação e conscientização para a cidadania, a fim de fortalecer sua capacidade de desarticular campanhas de desinformação em contextos eleitorais.

Para as empresas intermediárias:

- Divulgar os critérios utilizados para moderar, detectar e priorizar conteúdos nas plataformas e garantir o devido processo na moderação de conteúdos.
- Apoiar o jornalismo de qualidade e outras ações positivas destinadas a neutralizar as campanhas de desinformação, incluindo a colaboração com autoridades eleitorais e com pesquisadores independentes.
- Respeitar e cumprir de forma proativa a proteção de dados pessoais.

Para os partidos políticos:

- Evitar campanhas que utilizem informação falsa.
- Tornar transparente a campanha eleitoral.
- Respeitar e cumprir de forma proativa a proteção de dados pessoais.



Para os meios de comunicação e jornalistas:

- Fortalecer o jornalismo de qualidade frente à desinformação.

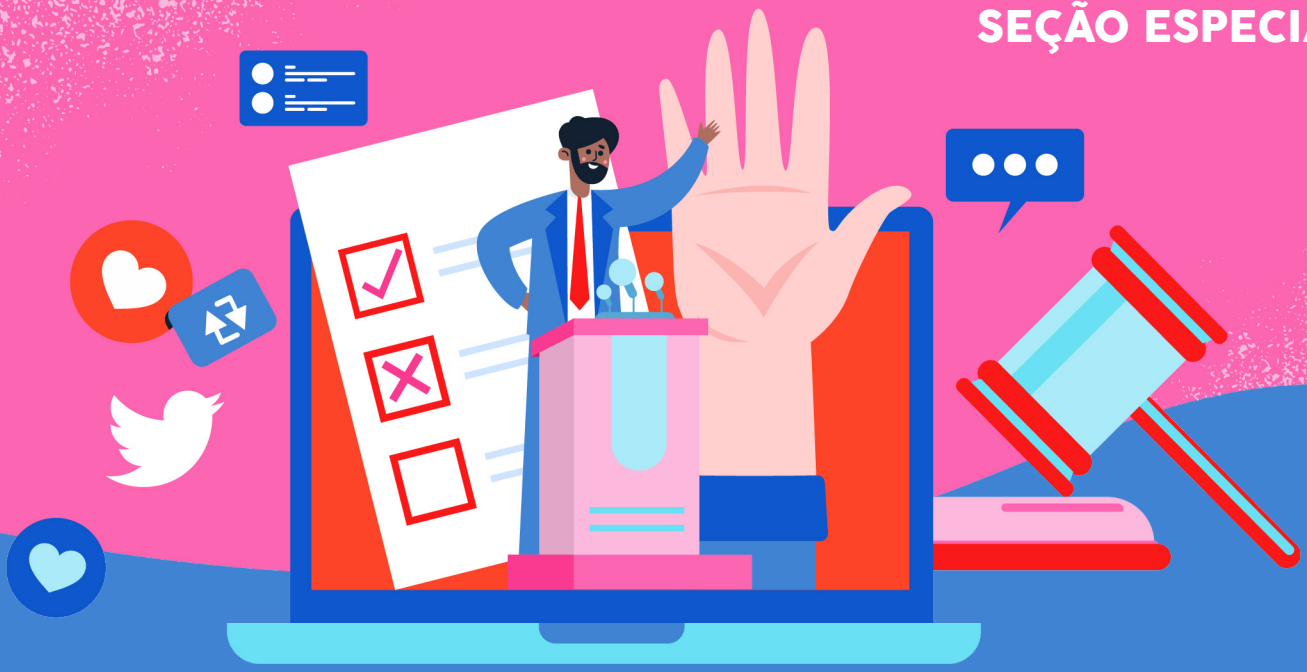
Para os verificadores ou *fact-checkers:*

- Unificar definições de desinformação e fortalecer as redes regionais.

Para institutos acadêmicos e de pesquisa:

- Expandir as pesquisas empíricas sobre a desinformação.

Ao longo deste guia, são abordadas algumas noções básicas sobre como fortalecer habilidades essenciais para alcançar a alfabetização digital e combater a desinformação e outros fenômenos que atentam contra seu desenvolvimento digital seguro.



A IMPORTÂNCIA DA ALFABETIZAÇÃO DIGITAL PARA A DEMOCRACIA
MISSÃO DE OBSERVAÇÃO ELEITORAL DA OEA (DECO)

As plataformas tecnológicas e as redes sociais ampliaram e criaram novas modalidades de comunicação que fortaleceram a interação de representantes e cidadãos, desse modo complementando as formas mais tradicionais de participação política. Isso contribuiu para o surgimento de uma cidadania ativa e envolvida no debate aberto em torno das ideias e interesses que confluem no espaço público.

Atualmente se dispõe de meios diversos para manifestar opiniões e posições próprias, bem como para se informar sobre o que ocorre no entorno, em âmbito municipal, estadual ou nacional, e em outros países e continentes. Tem-se também a oportunidade de criar conteúdos, os quais podem ser divulgados e compartilhados com uma ampla audiência. Por outro lado, existe uma interação mais direta com aqueles que exercem funções públicas, que não só redunda em acesso, mas também em fiscalização, possibilitando com isso que o exercício do poder esteja hoje mais do que nunca sujeito a um escrutínio público constante e imediato.

Já é habitual o acesso de autoridades às redes sociais, para informar-se sobre o exercício de suas funções, ou de candidatas e candidatos para conhecer suas propostas de forma direta e manter-se em dia com as atividades de campanha. Os partidos políticos se beneficiam ao poder transmitir suas mensagens e visão política diretamente ao cidadão, pelos diversos meios disponíveis, estendendo o âmbito territorial a um alcance nacional. Ao mesmo tempo, a sociedade civil dispõe hoje de plataformas com alcance maciço para divulgar suas ações e se conectar com as pessoas. E, em geral, a cidadania conta neste momento com novas formas de organização que possibilitam expressões coletivas.

Os aspectos acima mencionados permitem que o ambiente digital seja um elo importante dos processos democráticos e das eleições, contribuindo para o exercício da liberdade de expressão, para o livre acesso à informação e para a liberdade de associação, além de promover a transparência e a responsabilização, entre outros elementos. No futuro, o impacto das plataformas digitais e de outras tecnologias da informação em nossas democracias será ainda maior. A pandemia de Covid-19 aprofundou esse processo. No entanto, assim como há importantes benefícios, também existem diversos riscos. A dinâmica própria do mundo digital expõe todas as pessoas que utilizam a Internet a fenômenos como a desinformação, a violação de dados pessoais, as atividades ilegais e a influência de atores externos na política interna ou em processos eleitorais, entre outros elementos, que direta ou indiretamente minam a confiança em nossas democracias.

Para que se possa usar de maneira plena as diversas oportunidades que o mundo digital oferece, bem como para conhecer e compreender os riscos que esse ambiente no qual se está cada vez mais envolvido apresenta, e dele se proteger, é importante que a alfabetização digital alcance todas as pessoas.

Trata-se de um elemento essencial para o fortalecimento da democracia, e um processo necessário para que todos que intervêm a partir do âmbito público, atores sociais, grupos de interesse, instituições, meios de imprensa, sociedade civil, partidos políticos e a cidadania em geral, tenham a capacidade e a oportunidade de fazer uso dos instrumentos hoje disponíveis para contribuir, com base na tecnologia, para a democracia ativa e responsável.

Aprender a utilizar as ferramentas tecnológicas, acessar a informação, discernir informação de desinformação, avaliá-la, ser crítico na análise, distinguir as fontes, proteger os dados e resguardar a privacidade são algumas das condições necessárias para reduzir a lacuna digital, propiciar uma interação segura com as tecnologias e educar para uma cidadania consciente e informada.

SEGURANÇA CIBERNÉTICA E AUTOCUIDADO DIGITAL

A INTERNET FOI UMA FERRAMENTA QUE TRANSFORMOU E DEFINIU A COMUNICAÇÃO NO SÉCULO XXI.

Com suas múltiplas utilidades, permitiu que tanto indivíduos como organizações se conectem e se comuniquem. Em consequência dos diversos acontecimentos dos últimos anos, como a pandemia de Covid-19 e a aceleração dos processos de digitalização em todo o mundo, cada vez mais pessoas se valem da Internet para manter-se conectadas e compartilhar mensagens e informação de caráter pessoal, profissional e social em diferentes plataformas.

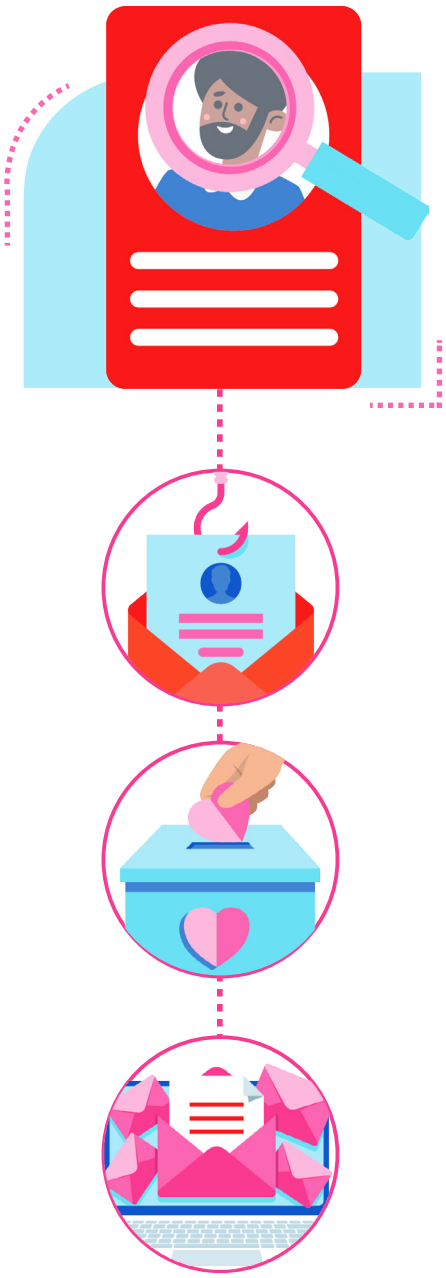
No entanto, à medida que se multiplicam esses processos, organizações e instituições de âmbito mundial registraram um crescimento considerável do nível de exposição a riscos online. Isso se deve principalmente à falta de familiaridade com o uso em grande escala das Tecnologias da Informação das Comunicações (TIC) e à carência generalizada de conhecimentos sobre ameaças cibernéticas e ferramentas de segurança digital. Esse baixo nível de competências de segurança cibernética, bem como a exposição a mais riscos online, configuraram um cenário propício para os que praticam os ataques, os quais se aproveitaram da 'nova normalidade' digital para explorar formas mais atuais de ataque e acesso a dados pessoais (UNODC, 2020)[8].

Levando em conta esse cenário, esta seção oferece uma variedade de termos e descrições para familiarizar o público geral com essas formas de ataque que mudaram ao longo do tempo. Da mesma forma, incluem-se conselhos para reduzi-los e enfrentá-los de forma proativa.

8 Trend Micro. (2020). Developing Story: COVID-19 Used in Malicious Campaigns. https://www.trendmicro.com/vinfo/fr/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains

Como reconhecer ataques cibernéticos?

Embora os ataques cibernéticos não sejam algo novo, é importante que estejamos familiarizados com eles, para que possamos denunciá-los e agir diante deles.



Engenharia social

Caracteristicas: A engenharia social consiste na utilização de métodos não tecnológicos para enganar potenciais vítimas específicas que foram previamente investigadas, para que compartilhem informação pessoal sensível, como senhas ou detalhes de contas bancárias, de forma quase voluntária, com um hacker[9].

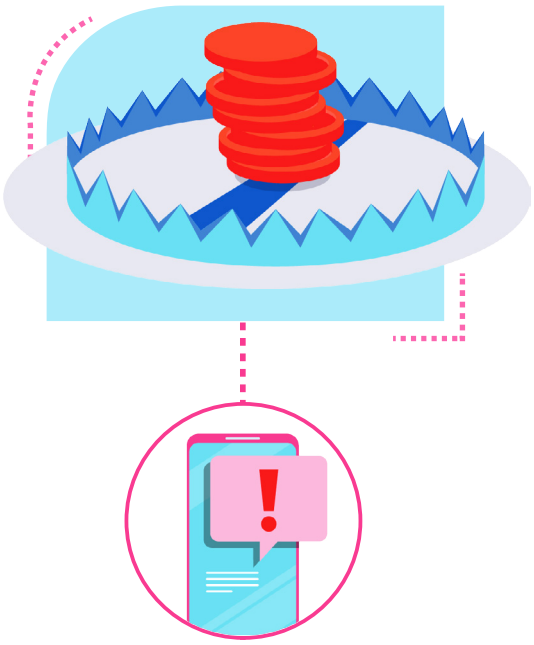
Alguns exemplos[10]:

***Spear phishing*:** mediante a personalização de e-mails, mensagens de *phishing* ou usurpando a identidade de contatos próximos, recrutadores, etc.
Exemplo: um *hacker* que falsifica a informação de um banco e pede a uma pessoa informação privada para "desbloquear sua conta", ou que se faz passar por um recrutador para solicitar informação de identidade para encaminhar uma oferta falsa.

***Pretexting*:** mediante um pretexto ou uma história cativante, os *hackers* atraem a atenção de uma pessoa a quem se busca atacar e a envolvem, para que pratique alguma ação específica, como doar a uma campanha falsa, ou prestar informação pessoal sensível.
Exemplo: *e-mails* nos quais se promete dinheiro de uma suposta herança, buscando obter detalhes de uma conta bancária.

***Spam* de contatos:** consiste no envio maciço de *e-mails* a uma lista de contatos de uma conta que foi hackeada. Esses *e-mails* são enviados de uma caixa de correio conhecida para não levantar suspeitas, mas seu conteúdo aparecerá para os destinatários com *links* abreviados ou assuntos informais como "Olha isso". Caso a pessoa clique, um *software* malicioso será instalado, que dará continuação a essa cadeia de *spam* e poderá acarretar consequências negativas para seus dados pessoais.

9 NortonLifeLock. O que é engenharia social? https://lam.norton.com/Internetsecurity-emerging-threats-what-is-social-engineering.html
10 SoftwareLab.org. O que é engenharia social? A definição e os cinco exemplos principais.https://softwarelab.org/es/que-es-ingenieria-social/



Fraudes, crimes informáticos e campanhas de *phishing*

Caracteristicas: Esses ataques são realizados de forma maciça por meio de publicações ou mensagens em redes sociais, nas quais informação não verificada sobre temas que estão no ciclo de notícias é utilizada como isca, persuadindo os destinatários a acessar *sites* falsos, facilitar dados pessoais ou bancários ou infectar sistemas informáticos e dispositivos eletrônicos[11].

Exemplo: são comuns as campanhas de *phishing* em que os criminosos cibernéticos falsificam a identidade de organismos internacionais e autoridades governamentais e sanitárias, oferecendo informação ou o apoio de supostos programas sociais[12], convidando a fazer doações para atender a emergências sanitárias ou, ante o aumento exponencial das compras *online*, nas quais se fazem passar por serviços de remessa ou entrega a domicílio.

As fraudes também circulam por meio de campanhas de *smishing*, que oferecem alimentos gratuitos, bônus, produtos médicos, descontos, serviços gratuitos de recargas e assinaturas em plataformas de entretenimento.

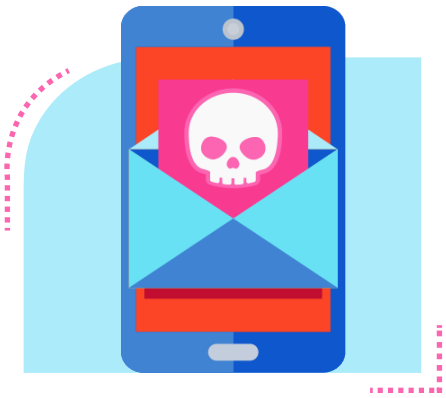
Malware ou instalação de *software* malicioso

Caracteristicas: O *malware* ou infiltração de conteúdo malicioso usa como isca informação relacionada a temas relevantes no ciclo de notícias para infiltrar-se em dispositivos eletrônicos. No caso da América Latina, uma ameaça recorrente nos últimos anos foram os ataques de *ransomware* contra computadores pessoais e telefones móveis, mediante os quais os criminosos cibernéticos codificam e 'sequestram' informação e dados pessoais das vítimas, exigindo um resgate para desbloquear o equipamento ou liberar a informação[13]. Às vezes, os *hackers* também podem recorrer a ameaças contra as vítimas, caso estes se neguem a pagar a recompensa esperada.

11 Porter, Taryn. (2020). COVID-19 Scam Alters. Cybercrime Support Network. https://cybercrimesupport.org/covid-19-scam-alerts/
12 Organização Mundial da Saúde (2020). WHO reports a fivefold increase in cyber attacks, urges vigilance. https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance; BBC News Mundo. (2020). Coronavírus: a advertência da OMS sobre os fraudadores que estão usando o nome da organização para roubar dinheiro e dados. https://www.bbc.com/mundo/noticias-52009138
13 We Live Security e eset. (2020). Relatório de Ameaças. Segundo Trimestre de 2020. https://www.welivesecurity.com/wp-content/uploads/2020/08/Q2-2020_Threat_Report-ESP.pdf

Criação de *sites* falsos *(spoofed domains)*

Caracteristicas: Nesse caso, os criminosos cibernéticos registram nomes de domínio com palavras-chave que geralmente são associadas a temas inovadores ou de interesse público, para confundir as pessoas. Isso é feito para que as pessoas acessem essas páginas nas quais se oferecem produtos que prometem solucionar algum problema pontual com soluções "milagrosas" ou rápidas, mas na realidade instalam *softwares* maliciosos ou coletam algum tipo de informação.



Mensagens de sextorsão falsas

Caracteristicas: Por meio desse tipo de ataque, os *hackers* enviam às pessoas mensagens nas quais ameaçam enviar a seus contatos vídeos íntimos e comprometedores que obtiveram ao infiltrar-se em seus dispositivos[14] ou gravaram enquanto navegavam em páginas de conteúdo sexual. Esse ataque vem, em geral, acompanhado de uma notificação de pagamento de uma quantia exigida em uma carteira digital, em troca de evitar que as ameaças feitas pelo hacker sejam cumpridas[15].

Ataques por meio das ferramentas de trabalho remoto

Caracteristicas: A pandemia de Covid-19 fez com que muitas empresas mantenham uma sucursal em cada domicílio de seus empregados, os quais se expõem a mais riscos *online* e, por sua vez, expõem os sistemas informáticos de seus centros de trabalho. Nesse ambiente, os criminosos cibernéticos identificaram vulnerabilidades de *software*, redes e ferramentas de trabalho remoto, dirigindo ataques para infiltrar-se nos sistemas corporativos por meio dos computadores pessoais dos funcionários.

14 Ducikin, Paul. (2020). Dirty little secret extortion email threatens to give your family coronavirus. Sophos https://nakedsecurity.sophos.com/2020/03/19/dirty-little-secret-extortion-email-threatens-to-give-your-family-coronavirus/
15 INCIBE y OSI. (2020). Detectada onda de falsos e-mails de sextorsão ou infecção de Covid-19. https://www.osi.es/es/actualidad/avisos/2020/04/detectada-oleada-de-falsos-correos-de-sextorsion-o-infeccion-de-covid19

Divulgação de informação falsa e desinformação

Caracteristicas: A circulação de informação falsa não verificada ou de teorias da conspiração na Internet facilita a execução de fraudes e ataques informáticos e outros ataques cibernéticos[16]. Essa informação pode ter origem em diversas fontes, não só de contas falsas, *trolls* ou *bots*, mas também de contas oficiais e contatos próximos, e sua circulação na Internet se deve a que, em grande medida, a população a compartilha de forma irrefletida[17].

Uso da *Dark Web* para atividades criminosas

Caracteristicas: Cresceu o uso da *Dark Web* para a venda de informação e dados pessoais ou corporativos obtidos via *ransomware* e outras atividades maliciosas, incluindo a exploração sexual infantil, a venda de dados pessoais ou endereços de correio, entre outras atividades ilícitas.

Medidas práticas para fazer frente aos ataques cibernéticos

Ante as ameaças expostas, esta seção pretende compartilhar passos simples e fáceis para proteger informação, contas e dados pessoais e corporativos de ataques cibernéticos. É importante destacar que essas recomendações se dirigem ao público geral e algumas podem não ser aplicáveis a figuras públicas, como políticos, ativistas ou outros atores, cujas práticas de redes sociais estejam sujeitas a um maior escrutínio. Do mesmo modo, o exercício dos direitos de expressão, reunião e protesto deve ser respeitado no âmbito digital, garantindo, ao mesmo tempo, práticas mais seguras de Internet.

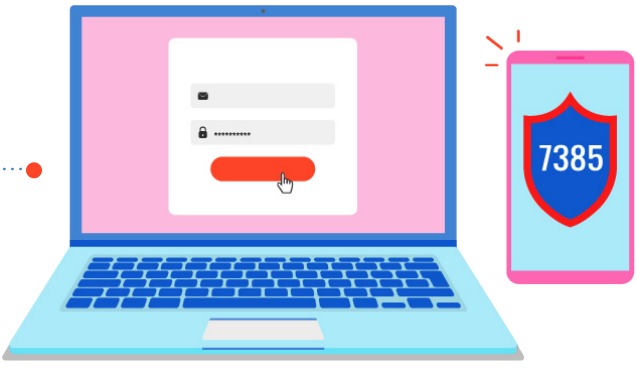
16 Stone, Jeff. (2020). How scammers use fake news articles to promote coronavirus 'cures' that only defraud victims.Cyberscoop. https://www.cyberscoop.com/coronavirus-cure-scam-social-media-riskiq/
17 NewsGuard. https://www.newsguardtech.com/

1. Revisar a configuração de privacidade

Administrar a configuração de privacidade em redes sociais e demais contas pessoais é uma das formas mais simples por meio das quais as pessoas pode m controlar a segurança e a privacidade de seus dispositivos e dados. A seguir, apresentam-se uma série de recomendações:

- Revisar regularmente a seção de "Privacidade" dentro das configurações de suas contas de redes sociais, *e-mail* e dispositivos conectados à Internet.
- Selecionar quem pode ver sua atividade nas redes sociais (por exemplo: seus Tuítes e interações).
- Verificar se seu perfil se encontra facilmente acessível ou público a outras pessoas e como é possível se conectar com esse perfil, seja mediante solicitações de amizade, seja começando a "segui-lo" no Twitter.
- Revisar, compreender e determinar o volume de informação pessoal que publica *online*. Lembrar-se de não colocar números de telefone, senhas pessoais ou informação sensível em publicações de suas redes sociais.
- Monitorar periodicamente a segurança e a informação de início de sessão de suas contas e verificar se não há nenhuma atividade suspeita ou acesso de aplicativos de terceiros a seus dados pessoais.
- Revisar a política de privacidade da plataforma para saber que dados os serviços compilam e com quem são compartilhados, e selecionar suas preferências nesses dois temas.

2. Configurar uma autenticação de dois fatores para iniciar sessão em suas contas pessoais



A autenticação de dois fatores proporciona às pessoas uma capa adicional de segurança, uma vez que exige que as pessoas verifiquem sua identidade com um segundo fator de verificação, como a biometria (tomada de impressão digital ou facial), ou proporcionando um código, desse modo protegendo o risco de credenciais fracas ou comprometidas.

A seguir, são apresentadas as duas mais conhecidas formas para adicionar essa capa de segurança adicional, bem como os prós e os contras de cada uma delas.

2 8 5 _ **Método de dupla autenticação**	**Prós**	**Contras**
 **Mensagem de texto** Cada vez que a pessoa inicie uma sessão em uma conta, por meio de um novo dispositivo, se exigirá que forneça um código de vários números que lhe será enviado por mensagem de texto para seu telefone ou por chamada telefônica.	• É uma forma fácil de autenticar a identidade do usuário, já que é necessário apenas um telefone que possa receber mensagens de texto. • É acessível, uma vez que, em alguns casos, o código também pode ser enviado em forma de chamada.	• Em casos de falsificação de identidade ou perda ou roubo de seu dispositivo móvel, outra pessoa poderia ter acesso a sua informação pessoal e iniciar sessões em suas contas. • Existe uma prática, chamada "portabilidade" ou "*SIM swapping*", que permite que um criminoso troque o cartão SIM do usuário por um infectado, para interceptar os códigos de dupla autenticação e acessar suas contas pessoais.
 **Aplicativo de autenticação de duplo fator** Um aplicativo de autenticação é um aplicativo de *software* independente que se baixa em um dispositivo móvel inteligente (*tablet*, iPad, etc.) ou em um computador. Esse aplicativo gera um código aleatório que se insere depois das credenciais ou envia uma notificação *push* (mensagens ou alertas que se enviam de um servidor remoto até o dispositivo que tem um aplicativo instalado) para autenticar a identidade da pessoa.	• Essa funcionalidade está disponível sem conexão à Internet. • Não é suscetível à portabilidade, uma vez que não depende de um *chip* telefônico. • A versão de notificação automática oferece o benefício adicional de ser mais rápida e fácil de usar. Caso apareça na notificação que a localização aproximada está distante do domicílio ou do escritório da pessoa, é mais provável que notificações como essas chamem sua atenção e o estimulem a tomar as medidas necessárias.	• Caso o aplicativo envie notificações *push* como método de autenticação, será exigida a conexão à Internet. • Caso o telefone de uma seja extraviado ou apagado, e não haja cópias do código salvas em outro lugar, não será possível acessar o aplicativo.

3. Gerir a informação pessoal incluída no perfil

Ao criar uma conta nas redes sociais, como regra geral, toda a informação divulgada em um perfil é pública, o que significa que qualquer pessoa pode acessar o conteúdo publicado nessa conta. No entanto, as necessidades e preferências de privacidade variam de pessoa para pessoa. Enquanto algumas pessoas preferem uma exposição maior, podendo, desse modo, promover seu conteúdo nas redes sociais, outras preferem incluir informação limitada ou nenhuma informação. Para maior proteção, é importante avaliar em que medida se está disposto a incluir informação pessoal em um perfil. Por conseguinte, é importante levar em conta as seguintes configurações nas redes sociais:

Escolha de nome de usuário: o nome de usuário é o "nome digital" que uma pessoa escolhe para ser identificada online como indivíduo ou organização. Caso a pessoa prefira não ser facilmente identificada, pode usar um pseudônimo que esteja relacionado ou não a ela. Esse nome não tem de ser o mesmo em todas as redes sociais e é possível mudá-lo em qualquer momento ao inserir a configuração da (s) conta(s).

Imagens de conta: as pessoas têm a opção de personalizar uma conta com a inserção de uma foto do perfil. Quando as pessoas preferem não ser identificadas, sugere-se escolher uma imagem na qual não possa ser reconhecida e mudá-la quando considere necessário. A utilização da mesma imagem em todas as redes sociais facilita a identificação do usuário nas plataformas.

Inclusão de localização: quando os serviços de localização são ativados em uma plataforma das redes sociais, é possível rastrear a origem de qualquer atividade de mídia online. É importante levar em conta que, uma vez que se ative essa função, ela permanecerá ativa até que seja desabilitada na configuração de privacidade. Mesmo que uma pessoa ative ou desative a função de compartilhar sua localização, persiste a possibilidade de ela ser descoberta por meio do conteúdo ou das imagens que compartilhe.

Publicação de fotos: as fotografias e outros arquivos multimídia contêm informação, chamada dados Exif, que detalha a localização, o dispositivo, a data e a hora de captura, etc. Por esse motivo, é importante conhecer as políticas de privacidade de conteúdo multimídia dos sites que visita e onde compartilha fotos, bem como estar em constante alerta quanto a com quem compartilha suas publicações e conteúdo multimídia[18].

18 Germain, Thomas.(2019). How a Photo's Hidden 'Exif' Data Exposes Your Personal Information.Consumer Reports.https://www.consumerreports.org/privacy/what-can-you-tell-from-photo-exif-data/

4. Recomendações gerais

O trabalho remoto ou teletrabalho aumenta os riscos associados ao manejo de informação sensível em ambientes corporativos e pessoais. Por esse motivo, recomenda-se levar em conta alguns conselhos adaptados à "nova normalidade" do teletrabalho e da vida digital[19]:

Mantenha seus softwares atualizados: recomenda-se que o *software* de todo dispositivo e aplicativo seja atualizado com a maior frequência possível. Isso proporciona ao usuário maior segurança e velocidade de resposta do dispositivo, além de poder oferecer proteção contra fraudes, vírus, cavalos de Tróia e ataques de *phishing* (falsificação de identidade), entre outras ameaças. É provável que, com essas atualizações, as preferências de privacidade se restabeleçam, razão pela qual se recomenda que, ao introduzir essas atualizações, se faça uma revisão da informação que se compartilha com aplicativos e dispositivos móveis.

Utilize um antivírus: o uso de *software* antivírus para dispositivos portáteis conectados à Internet serve como um escâner inicial de qualquer atividade suspeita ou maliciosa à qual todo usuário está exposto. Isso pode ajudar a supervisionar a entrega de notificações e oferecer um nível adicional de proteção, caso uma pessoa clique por engano em *links* suspeitos que podem conter *spam* e diferentes tipos de vírus.

Bloqueie e filtre: o uso das funções de bloquear e denunciar, bem como a utilização de filtros para correios, mensagens e notificações, permite que os serviços das plataformas permaneçam seguros e resistentes. Cada vez que se bloqueia uma conta ou uma publicação, um sinal importante é transmitido às plataformas sobre conteúdo ou interações não desejadas para a pessoa, razão pela qual se limita ou bloqueia esse tipo de conteúdo. É recomendável não ignorar um conteúdo suspeito ou que viole as políticas de uso de uma plataforma: é melhor denunciá-lo de maneira contínua. Caso seja necessário, deve também denunciar, a agentes da ordem pública, ameaças que atentem contra sua segurança física[20].

Utilize um computador portátil da empresa para o trabalho remoto, caso seja possível, e não compartilhe informação com outros membros do seu domicílio: não utilize sua máquina pessoal, já que pode ter menos controles de segurança que o *hardware* de sua empresa. Caso não possa evitar o uso de equipamentos pessoais e tenha de utilizar seu próprio dispositivo, mantenha-o o mais próximo possível das normas de segurança de sua organização. Utilize o *software* de segurança proporcionado por sua empresa, siga as medidas de proteção de dados da empresa e não misture seu uso pessoal com o do trabalho.

Utilize VPN designadas e evite as redes Wi-Fi públicas e gratuitas: a utilização de redes Wi-Fi públicas pode colocar em risco informação sensível, como senhas e dados bancários, entre outros. Do mesmo modo, caso trabalhe em um ambiente corporativo, é recomendável fazer uso da VPN (*Virtual Private Network*, em inglês) designada, para que seus ativos laborais se mantenham seguros quando se trabalha de um lugar remoto.

Utilize redes divididas: ao trabalhar em casa, é recomendável que a rede pessoal seja de acesso próprio e que se crie uma rede específica para o uso de convidados. Caso tenha um roteador ou comutador (*router*) com uma funcionalidade (VLAN), coloque-o em atividade e dedique uma VLAN somente a temas de trabalho.

19 Roesler, Martin.(2020). Working From Home? Here's What You Need for a Secure Setup.Trend Micro. https://www.trendmicro.com/vinfo/ph/security/news/cybercrime-and-digital-threats/working-from-home-here-s-what-you-need-for-a-secure-setup

20 U.S. Department of Homeland Security. (2019). Social Media Plan Guide: Science and Technology Directorate. https://www.dhs.gov/sites/default/files/publications/social_media_plan_guide_09_20_2019.pdf

Prepare uma solução de respaldo em casa: ter opções de respaldo (por exemplo, *hardware*, como discos duros externos ou USB) é uma medida preventiva fundamental, no caso de experimentar alguma falha no armazenamento de informação, como perda de conectividade ou falha do servidor.

Reconheça os ataques de engenharia social: há vários sinais de alerta que podem indicar um ataque de engenharia social. Os mais comuns figuram abaixo[21]:

Linguagem genérica e com falhas: Scaso o *e-mail* tenha origem em uma fonte segura e confiável, o corpo estará escrito de maneira correta, segundo as regras de ortografia e gramática. Do contrário, é possível que se trate de um ataque. Outro elemento linguístico que pode indicar uma tentativa de ataque são as saudações e as formulações genéricas. Caso, portanto, um *e-mail* comece com "Prezado destinatário" ou "Prezado usuário", tenha cuidado.

Remetente desconhecido ou com identificação suspeita: caso um *e-mail* venha de um endereço que seja uma combinação de números e caracteres aleatórios, ou desconhecido do destinatário, deve ser enviado diretamente para a pasta de *e-mail* não desejado. No entanto, em alguns casos, os hackers também podem ter um endereço de *e-mail* legítimo, razão pela qual é importante, de todo modo, revisar os demais sinais de alerta incluídos nesta seção.

Sentido de urgência: os criminosos por trás das campanhas de engenharia social, frequentemente, tentam assustar as vítimas e fazer com que ajam, utilizando frases que provocam ansiedade como "envie-nos seus dados de imediato ou sua encomenda será descartada" ou "caso não atualize seu perfil agora, encerraremos sua conta". Os bancos, as empresas de remessas, as instituições públicas e, inclusive, os departamentos internos costumam comunicar-se de forma neutra e objetiva. Portanto, caso a mensagem tente pressionar o destinatário para que aja rapidamente, é provável que seja uma fraude maliciosa e possivelmente perigosa.

21 Eset. Social Engineering (in cybersecurity). https://www.eset.com/int/social-engineering-business/

Solicitação de informação pessoal e privada: As instituições e, inclusive, outros departamentos de sua própria empresa normalmente não solicitam informação confidencial por *e-mail* ou por telefone, a menos que o contato tenha sido iniciado pelo empregado.

As recomendações acima são apenas algumas mediante as quais uma pessoa ou organização pode ser proativa para garantir altos níveis de segurança cibernética nas redes sociais e nos dispositivos eletrônicos. No entanto, assim como com a alfabetização, é responsabilidade de cada pessoa manter-se informada e revisar a configuração de privacidade, bem como continuamente atualizar suas medidas de segurança cibernética, a fim de assegurar que seus dados e informação importante estejam protegidos em todo momento.

Adquirir e colocar em prática esse conhecimento e essas medidas de segurança ajudam as pessoas a se preparar melhor para que, quando estejam *online*, pesquisem, consumam e distribuam informação de forma responsável. A seção seguinte examina em maior profundidade essas áreas ao usar o Twitter como ferramenta para manter-se informado.

RECOMENDAÇÕES GERAIS PARA JORNALISTAS

Embora as seções acima contenham informação fundamental para todas as pessoas, aquelas que se dedicam a tarefas jornalísticas, assim como as demais pessoas que utilizam a Internet para diferentes atividades, não estão isentas de praticar bons hábitos de segurança digital para proteger-se no momento de executar seu trabalho. Para essas pessoas, a Internet também se converteu em uma ferramenta crucial para desempenhar seu papel, sobretudo em momentos decisivos de alto interesse, como os processos eleitorais, em que a informação de um fato noticioso se desloca em rápida velocidade. Nesse sentido, se apresenta a seguir uma série de recomendações de segurança cibernética para momentos específicos, extraídas do Cobrindo eleições: kit de segurança para jornalistas, desenvolvido pelo Comitê para a Proteção de Jornalistas (CPJ na sigla em inglês)[22]:

I. Preparação básica de dispositivos

Antes de sair para cobrir os acontecimentos, são boas práticas:

- ☑ Fazer cópias dos dados dos dispositivos em um disco rígido e apagar qualquer dado sensível do dispositivo que leve.
- ☑ Encerrar as sessões de todas as contas, aplicativos e navegadores, bem como apagar o histórico de navegação.
- ☑ Proteger todos os dispositivos com senhas e configurá-los para que possa apagar os dados de maneira remota.
- ☑ Levar o menor número possível de dispositivos. Caso possua dispositivos que não usa, levá-los em lugar de seus dispositivos pessoais ou de trabalho.

22 Forbes, Jack. (2019). Cobrindo eleições: kit de segurança para jornalistas. Comitê para a Proteção de Jornalistas. https://cpj.org/es/2019/10/guia-de-seguridad-periodistica-para-elecciones/#harassed

II. Como proteger e armazenar materiais informativos

Durante os períodos eleitorais, é importante dispor de bons protocolos para armazenar e proteger materiais informativos. Caso as autoridades detenham um jornalista na cobertura de uma campanha eleitoral, poderiam confiscar e inspecionar seus dispositivos, o que poderia ter graves consequências para ele e para suas fontes de informação. As seguintes medidas podem ajudar a se proteger e proteger a informação em seu poder:

- Revisar a informação armazenada em seus dispositivos, especialmente telefones e computadores. Isso é feito salvando adequadamente a informação que possa ser colocada em risco, ou que contenha dado sensível, e posteriormente apagar essa informação do dispositivo.
- Revisar o conteúdo de seus telefones, inclusive a informação que nele tenha sido salva (o hardware), bem como a informação salva na nuvem (Google Photos ou iCloud).
- Revisar o conteúdo dos aplicativos de mensagem, como o WhatsApp. Salvar e, em seguida, apagar toda informação que acarrete risco. Os trabalhadores da mídia devem levar em conta que o WhatsApp faz uma cópia de apoio de todo o conteúdo no serviço na nuvem vinculado à conta, por exemplo, iCloud ou Google Drive.
- Retirar material informativo de seus dispositivos periodicamente e salvá-lo na opção para cópias de respaldo de sua preferência. Isso assegurará que, caso o dispositivo seja confiscado ou roubado, ainda seja conservada uma cópia da informação.
- Criptografar toda a informação salva é benéfico para manter dados sensíveis seguros. Isso pode ser feito criptografando o disco rígido externo ou USB. Também se pode ativar a criptografia de dispositivos. Os jornalistas devem estudar a lei vigente no país onde trabalham, para assegurar-se de que conhecem os aspectos legais que regem o uso da criptografia.
- Armazenar os dispositivos e discos rígidos externos em lugar físico diferente do domicílio, em casos de ameaça ou risco de roubo.
- Bloquear todos os dispositivos com um PIN: quanto maior seja o PIN, mais difícil será decifrá-lo.
- Configurar o telefone ou o computador para poder apagá-los de maneira remota. Essa é uma função que permite apagar os dispositivos a distância, por exemplo, caso as autoridades ou outros atores os confisquem.

DISTRIBUIÇÃO E CONSUMO DE INFORMAÇÃO NO TWITTER

Manter-se seguro *online* é uma prática tão fundamental para uma experiência positiva e saudável na Internet quanto o pensamento crítico e o uso de ferramentas para a verificação de informação. O funcionamento do Twitter se baseia no que está acontecendo e naquilo que as pessoas estão falando no momento, razão pela qual se transformou na principal plataforma de informação para muitas pessoas. No entanto, com tanta informação disponível, às vezes pode ser complicado acompanhar o ritmo da conversa e verificar a veracidade da informação que se consome. A seção seguinte oferece recomendações, ferramentas e melhores práticas para buscar, organizar, compartilhar e publicar informação no Twitter.

Verificação de informação no Twitter

No Twitter, as pessoas podem encontrar informação e verificar sua exatidão de maneira rápida. Por ser uma plataforma aberta e pública, há diversas formas e ferramentas para iniciar conversas com outras pessoas ou fazer uma busca rápida de uma *hashtag*[23] ou palavras-chave, a fim de avaliar a veracidade do conteúdo que se consome na plataforma.

Quando se lê algo, é importante levar em conta os preconceitos próprios e opiniões, assim como as reações pessoais. Com frequência, quando se recebe informação com a qual não se está de acordo, naturalmente as pessoas se fazem certas perguntas ou comentários que ajudam a desmentir essa informação. No entanto, em geral, esse exame minucioso deixa de ser feito quando o que se lê confirma ideias preconcebidas. Diante desse cenário, é importante adquirir o costume de sempre se perguntar quem, o quê, onde, quando, como e o porquê de uma informação antes de compartilhá-la, fazer um Retuíte[24], um Tuíte com comentário ou dar um *Curtir*.

23 Hashtags ou etiquetas (escritos com o sinal "#" anteposto) são usadas para indexar palavras-chave ou temas no Twitter. Essa função é uma invenção do Twitter e permite que as pessoas possam encontrar facilmente conteúdo sobre os temas que lhes interessam.
24 Retuíte é a ação de compartilhar um Tuíte já existente.

- Quem é a fonte? É do seu conhecimento?
- É uma conta verificada?
- A quem segue essa conta e quem a segue?
- Quem escreve o artigo e qual o seu nível de conhecimento da área?

- O que disseram?
- Que motivos têm para compartilhar essa informação?
- Que tipo de artigo é: informação ou opinião?
- Que tom utiliza? É, talvez, intencionalmente falsa ou uma brincadeira?
- Que respostas esse conteúdo vem recebendo, ou seja, o que dizem as pessoas no Twitter?

- Onde ocorreu?
- Onde o disseram ou publicaram?
- É uma fonte confiável?
- Qual a URL ou *link* do *site*? É legítimo?
- Que outros meios ou pessoas cobriram esse evento?

- Quando o disseram?
- Quando se publicou? Tem data?

- Por que se publicou a notícia?
- É para gerar tráfego no *site* ou conta?
- É para provocar uma ação? Em caso afirmativo, de quem e para quê?

- Como está escrito?
- Há um excesso de sinais de pontuação e letras maiúsculas para torná-lo sensacionalista?
- Tem um titular falso?
- Está utilizando *hashtags* não relacionadas ao tema para chamar a atenção?
- Tem um tom conspiratório?

À primeira vista parecem ser muitas perguntas, mas podem ser respondidas em questão de segundos e há ferramentas do Twitter que facilitam essa tarefa e favorecem em grande medida o consumo seguro e informado de informação no Twitter. A seção seguinte aborda essas ferramentas e apresenta conselhos para seu uso.

Ferramentas do Twitter para melhorar o consumo de informação

O Twitter continua desenvolvendo atualizações de produto para ajudar as pessoas a encontrar informação e conhecer o contexto em que ocorre, de maneira fácil e rápida. Por exemplo, para ajudar as pessoas a se manter informadas sobre importantes eventos nacionais e globais, algumas vezes se mostra na cronologia informação confiável e de alta qualidade sobre eventos que são de grande interesse público como eleições, desastres naturais ou crises globais, como a Covid-19, permitindo-se às pessoas decidir se querem continuar vendo essa informação ou se não é de seu interesse.

Por outro lado, para ajudar as pessoas a conhecer o contexto em torno de uma informação, quando as pessoas querem retuitar (compartilhar) um Tuíte que contém um *link* que não foi aberto pela pessoa a partir da plataforma, o Twitter lança um aviso que recomenda às pessoas abrir esse *link* para conhecer toda a informação antes de compartilhá-lo. Isso incentiva as pessoas a se indagar criticamente sobre a informação que estão compartilhando.

Os exemplos acima mostram produtos que ajudam as pessoas a estar mais bem informadas de forma reativa. Além disso, há ferramentas de Twitter e outros elementos no desenho da plataforma que ajudam as pessoas a explorar e organizar de maneira proativa a grande quantidade de informação disponível na plataforma e a ela acrescentam mais contexto para análise e verificação. Algumas delas são descritas abaixo.

As Tendências existem para ajudar as pessoas a descobrir conversas que estão acontecendo ao seu redor. Essas conversas são determinadas automaticamente, levando em conta diferentes fatores para identificar temas que gozam de popularidade em um dado momento, em lugar de temas que foram populares durante um tempo ou diariamente.

As Tendências estão disponíveis no aplicativo do Twitter, na seção ***Explorar*** , e no twitter.com em diferentes lugares, como na cronologia de início, nas Notificações, nos resultados de busca e nas páginas de perfil. Ao pressionar ou clicar em qualquer tendência, aparecerão os resultados de busca do Twitter relacionados a essa tendência, ou seja, todos os Tuítes que incluam essa frase ou *hashtag*.

Tendências para o usuário vs. Tendências de uma localização geográfica

De forma predeterminada, no Twitter se mostram as Tendências Para você, as quais são determinadas automaticamente, considerando as contas que segue, seus interesses e sua localização. Para ver as Tendências segundo uma área geográfica, no twitter.com ou do aplicativo, é possível clicar no ícone de ***configuração*** e escolher Tendências de localizações específicas. Caso não encontre a cidade ou o país que busca, isso significa que ainda não há suficientes Tuítes nessa zona geográfica que justifique a criação de uma lista de Tendências. Nesses casos, podem-se buscar Tuítes locais sobre qualquer tema utilizando a Busca Avançada do Twitter.

Contexto nas Tendências

Juntamente com algumas Tendências, podem-se ver:

- O número aproximado de Tuítes associados a essa tendência. É importante entender que o número de Tuítes relacionados às Tendências é somente um dos fatores levados em conta na hora de classificar e determinar as Tendências. Por esse motivo, às vezes, é possível ver que o número de Tuítes das primeiras Tendências é menor do que o número de Tuítes das seguintes.
- Informação contextual personalizada, por exemplo, quem em sua rede de contatos está tuitando sobre a tendência.
- Uma categoria, como "Política", "Música" ou "Entretenimento", pode ser selecionada automaticamente em função do que tratam os Tuítes da tendência.
- Artigos que se anexam automaticamente em função da conversa sobre a tendência.

Resultados de busca

Cada vez que se faz uma busca no Twitter, seja a partir do twitter.com ou do aplicativo, os resultados podem ser visualizados de acordo com a data em que foram compartilhados ou o tipo de conteúdo, ou seja, cada busca é organizada de forma automática em diferentes abas que oferecem a opção de ver os Tuítes:

Destacados

Resultados mais relevantes de acordo com os interesses da conta que realiza a busca.

Mais recentes

Resultados de busca em ordem cronológica.

Pessoas

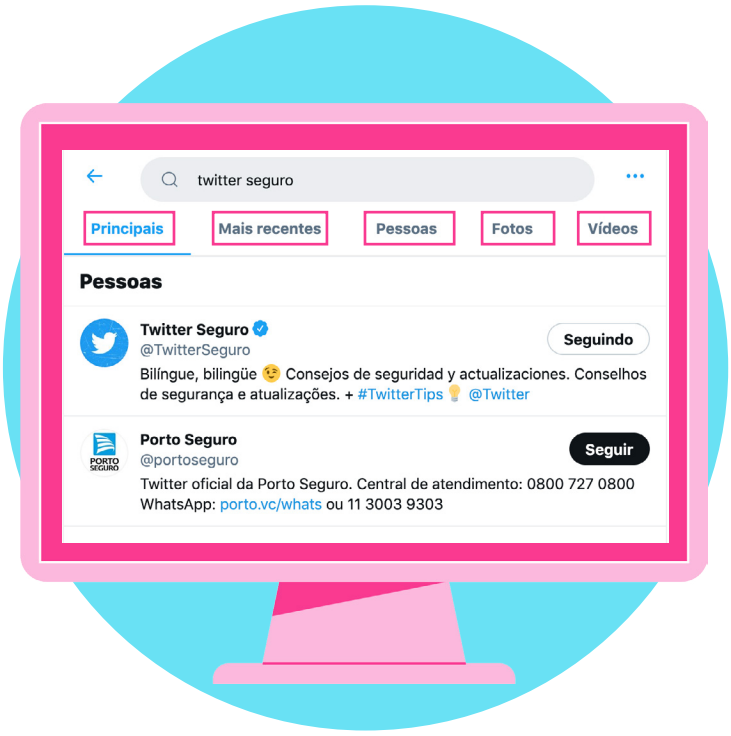
Resultados das contas que coincidem com a consulta.

Fotos

Resultados de busca que contêm fotos.

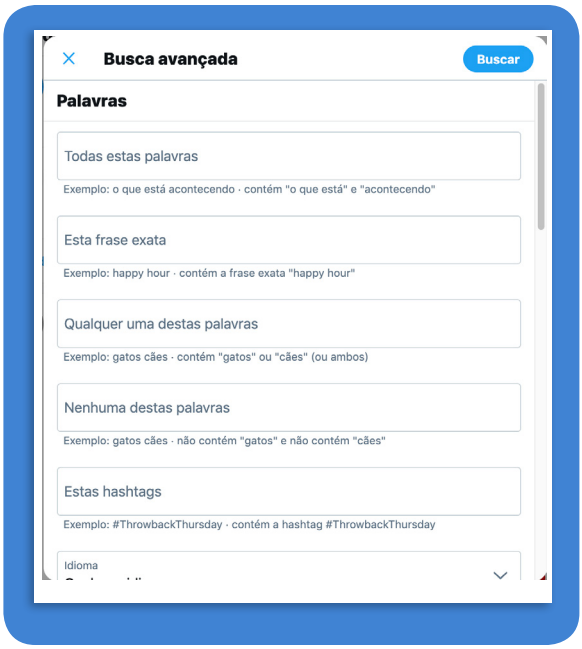
Vídeos

Resultados de busca que contêm vídeo.



Busca avançada

Caso se queira buscar alguma informação precisa no twitter.com, existe a opção de realizar uma busca avançada. Essa opção está disponível no menu suspenso para mais ***opções*** , na parte superior da página, clicando em *Busca avançada*. Ali é apresentada uma série de campos mediante os quais se pode refinar a busca para encontrar conteúdo específico de maneira mais direta e rápida.



No aplicativo, as opções de busca são mais limitadas, mas, com determinadas fórmulas de busca, também se pode refinar a informação dos resultados. Utilizando a frase *Twitter app*, o seguinte exemplo ilustra como é possível utilizar algumas nomenclaturas de acordo com o conteúdo que se busca.

Twitter app

para buscar conteúdos que contenham todos os termos de busca, sejam eles palavras, @nomes de contas ou *hashtags*. Nesse caso, a palavra *Twitter* e a palavra *app*.

Twitter -app

utilizando um travessão, ou símbolo de subtração, para buscar conteúdos que contenham a palavra *Twitter*, mas não a palavra *app*, ou seja, que excluam o que se coloca depois do travessão.

"Twitter app"

para buscar conteúdos que contenham exatamente a frase entre aspas, ou seja, *"Twitter app"*.

from:TwitterSeguro

para buscar conteúdos publicados a partir de uma conta específica de Twitter. Nesse caso, *TwitterSeguro*.

Twitter OU app

para buscar conteúdos que contenham um ou outro termo. Nesse caso, os termos *Twitter* ou *app*, ou ambos.

Cronologia de Início: "Tuítes destacados" vs. "Tuítes mais recentes"

A página principal do twitter.com ou do aplicativo mostra, de forma predeterminada, os Tuítes mais relevantes na parte superior da cronologia. No entanto, às vezes, é melhor ver os Tuítes em ordem cronológica, ou seja, ver primeiro os Tuítes mais recentes, o que depende não só das preferências de cada pessoa, mas também da informação que se busca. Por exemplo, durante um evento esportivo ou em situações de emergência, é mais útil ver primeiro a informação mais atual.

Por isso, existe no Twitter a possibilidade de mudar, de forma fácil e rápida, a configuração da cronologia de início entre Tuítes destacados e Tuítes mais recentes. Para fazer essa mudança, a partir do twitter.com ou do aplicativo, pressione o ícone no canto superior direito e escolha a opção de preferência.

A opção predeterminada no Twitter é a de Tuítes destacados. Por isso, quando se muda a configuração para Tuítes mais recentes e se deixa de usar o Twitter por um tempo, a configuração voltará automaticamente para os Tuítes destacados.

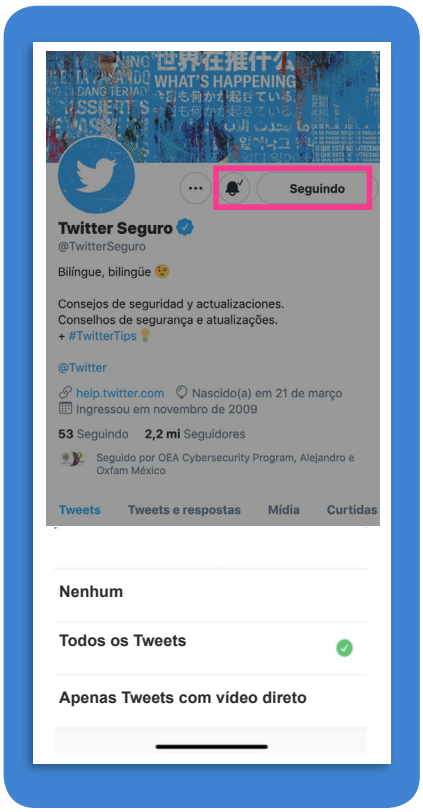
Notificações de conta

Há momentos em que é necessário ou se quer estar a par do conteúdo publicado por contas específicas, e para isso existem as notificações de conta ou notificações *push*. Esses mecanismos enviam ao usuário uma notificação ou alerta quando certas contas publicam Tuítes. Existe a opção de escolher ou ativar essas notificações para todos os Tuítes de uma conta ou somente para os Tuítes que contenham transmissões ao vivo, sendo que as últimas podem ser ativadas ou desativadas em qualquer momento.

Para ativar as notificações:

1. Assegure-se de estar seguindo a conta na qual quer receber notificações em tempo real.
2. No perfil da conta, seja no twitter.com ou no aplicativo, pressione o ícone ***Notificação*** (ícono).
3. Caso isso seja feito do twitter.com, ambas as notificações serão ativadas: para todos os Tuítes e para transmissões ao vivo. Do aplicativo, existe a possibilidade de escolher entre dois tipos de notificação: *Todos os Tuítes* ou *Somente Tuítes com vídeo ao vivo*.

Para **cancelar as Notificações**, volte ao perfil da conta, pressione o ícone ***Notificação ressaltada*** e escolha *Nenhuma*.



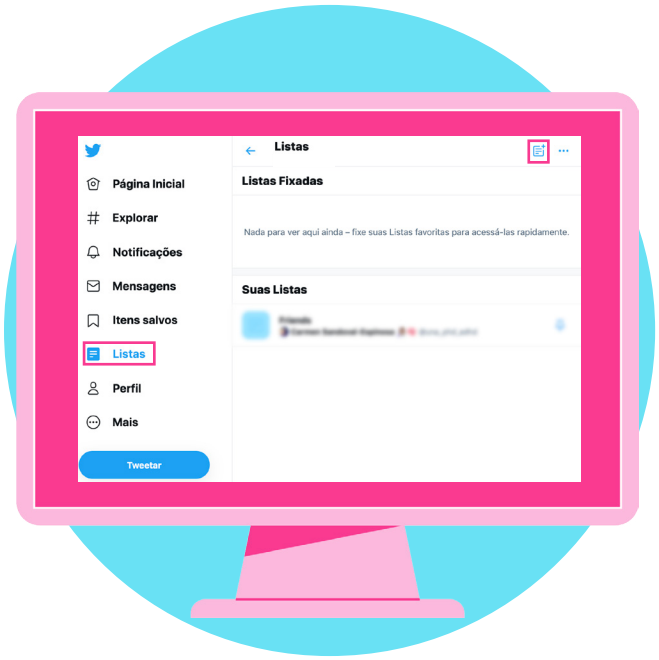
Caso seja necessário revisar que Notificações estão ativas, isso pode ser feito do aplicativo:

1. No menu da conta.
2. Escolhendo *Configuração e privacidade*.
3. Pressionando *Notificações* e, em seguida, *Notificações push*.
4. Pressionando *Tuítes*.

Listas

Uma lista é um filtro que mostra uma cronologia de início personalizada, na qual aparecem unicamente os Tuítes das contas incluídas nessa lista. Por exemplo, é possível filtrar a cronologia de início criando listas específicas de especialistas, jornalistas, comediantes, autoridades, serviços, etc. Algumas características importantes das listas:

- A possibilidade de criar listas próprias ou aderir a listas criadas por outras pessoas.
- Não ser necessário seguir uma conta para poder adicioná-la a uma lista.
- O fato de as listas poderem ser privadas, para monitoramento pessoal, ou públicas, para compartilhar informação com outras pessoas.
- Na hipótese de serem públicas, as contas que a elas se adicionem receberem uma notificação a esse respeito.
- A possibilidade de fixar, no aplicativo, até cinco listas na tela de início, para acessá-las de forma rápida.



Para criar uma lista:

1. Clique no ícone de seu perfil para abrir o menu suspenso.
2. Clique em *Listas.*
3. Clique em *Criar nova Lista.*
4. Escolha um nome para sua Lista e descreva-a brevemente. Nesse passo, informe se a Lista deve ser privada (só o dono da conta poderá vê-la e acessá-la) ou pública (qualquer pessoa pode ver e assinar a Lista).
5. Clique em *Salvar Lista.*

Para adicionar pessoas a uma Lista:
Para isso não é necessário seguir as contas que se quer adicionar à Lista.

1. Clique no ícone de ***conteúdo adicional*** no perfil da conta que deseja adicionar à Lista.
2. Escolha *Adicionar ou excluir das Listas.* Uma nova janela se abrirá, mostrando as Listas já criadas ou oferecendo a opção de criar uma nova.
3. Clique na(s) Lista(s) a que deseja adicionar a conta ou retire a marca das Listas das quais deseja excluir a conta.

Editar ou excluir uma Lista:

1. Clique no ícone de seu perfil para abrir o menu suspenso.
2. Clique em *Listas.*
3. Clique ou pressione a Lista que deseja editar ou excluir das Listas que criou.
4. Clique ou pressione o botão *Editar* para atualizar os detalhes da Lista ou para excluir a Lista por completo.

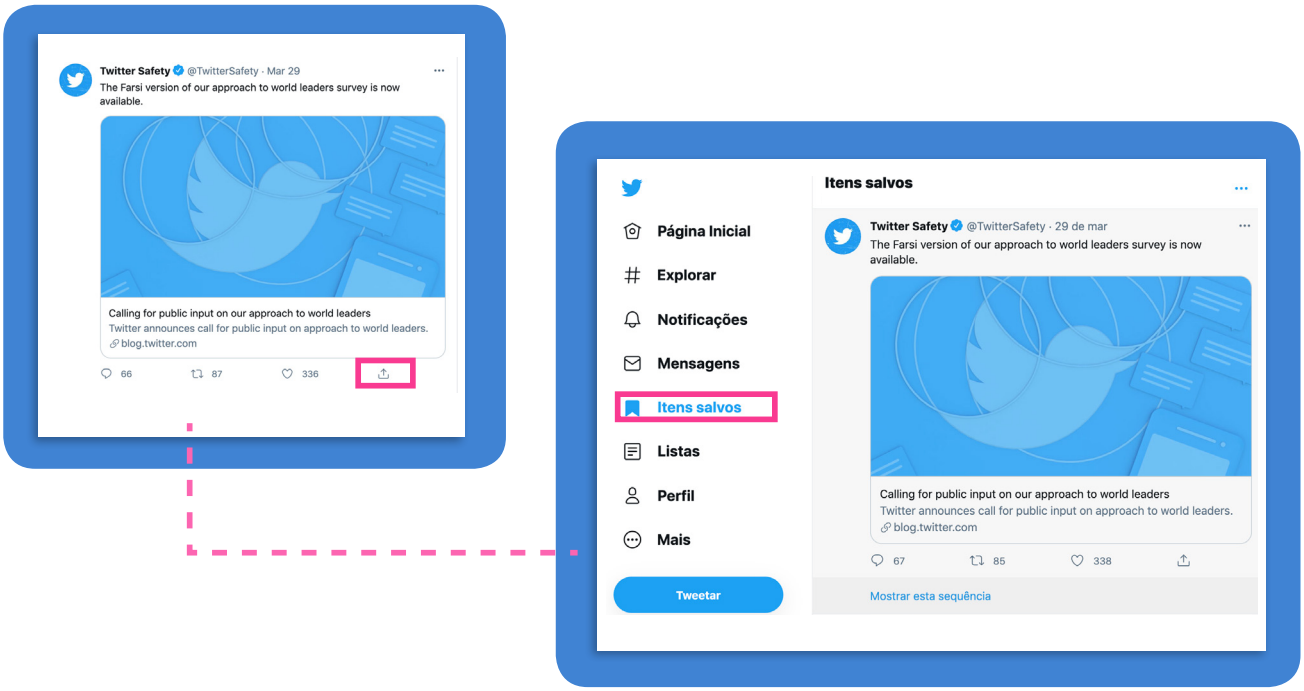
Inscrever-se nas Listas de outras contas:

1. Clique no ícone de ***conteúdo adicional*** no perfil de uma conta.
2. Clique ou pressione a opção *Listas.*
3. Escolha a Lista na qual deseja se inscrever.
4. Na página da Lista, caso seja possível, clique ou pressione a opção *Inscrever-se* para seguir a Lista. É possível seguir a Lista sem ter de seguir a conta que a criou ou ter de seguir cada uma das contas que dela fazem parte.

Tuítes salvos (*Bookmarks*)

De artigos e Fios a vídeos e GIFs, a cronologia de início está repleta de conteúdo que nem sempre há tempo de explorar nesse momento inicial ou que se quer salvar para poder revisar ou usar como referência mais adiante. Para esses casos, existem os *Bookmarks* ou Itens salvos de Twitter.

Para marcar um Tuíte como um Item salvo, pressione o ícone ***compartilhar*** que se encontra abaixo do Tuíte que se deseja salvar e selecione *Adicionar Tuíte a Itens Salvos*. Quando quiser localizá-lo, pressione *Itens* salvos no menu de seu perfil para encontrá-lo. Os Tuítes podem ser excluídos do marcador em qualquer momento e somente o dono da conta pode ver seus marcadores.



O uso adequado dessas ferramentas é fundamental para a verificação da informação que se encontra no Twitter, mas estar na plataforma implica muito mais do que consumir informação. Também se trata de compartilhar informação e interagir com outras pessoas. Para garantir que o Twitter seja um espaço no qual as pessoas possam participar de maneira livre e segura, há regras sobre o que é ou não é permitido no Twitter, além de ferramentas para ajudar as pessoas a controlar sua experiência na plataforma. Essas diretrizes figuram na seção seguinte.

MELHORES PRÁTICAS NO TWITTER PARA AUTORIDADES E ORGANIZAÇÕES

O Twitter é uma das plataformas de redes sociais mais rápidas de que as organizações, autoridades e especialistas dispõem para compartilhar informação relevante e confiável com o maior número de pessoas e com um mínimo esforço.

Para usar o Twitter de maneira efetiva, aumentar a credibilidade de sua presença *online* e se posicionar como fontes de informação confiável, as organizações, entidades ou autoridades devem apresentar um plano de conteúdo constante e interativo, que reflita sua credibilidade e relevância. Alguns conselhos para tornar isso possível.

- O perfil da conta é sua carta de apresentação no Twitter, e por isso deve refletir a informação mais atualizada: nome, biografia, localização e *site*. Do mesmo modo, as fotos do cabeçalho e do perfil ajudam as pessoas a identificar facilmente a identidade da conta.

- As mensagens devem ser sempre concisas, fáceis de digerir e apresentar um tom de conversa, em lugar de pretender iniciar um discurso. As pessoas vão ao Twitter para interagir, fazer perguntas e compartilhar reações. Interações básicas como *Curtir*, Retuítes, menções e respostas podem ajudar a desenvolver conversas sobre seus temas de interesse.

- O conteúdo multimídia é sumamente interativo e efetivo, mas apenas quando compartilhado de forma nativa e não de outras plataformas. Também é importante que o conteúdo multimídia seja claramente relacionado à mensagem que se quer compartilhar e, no caso dos vídeos, que sejam curtos – 16 segundos é o ideal.

- A relevância do momento é fundamental no Twitter. Participar do momento em que ocorrem os fatos, dividir reações e proporcionar informação de primeira mão aumentam a relevância e a credibilidade de sua presença no Twitter.

- Manter-se conectado, motivar conversas, fazer sessões de perguntas e respostas – agrupadas em torno de um *hashtag* – e transmissões ao vivo são importantes para compartilhar com seus seguidores, de forma direta, seu ponto de vista único sobre o momento, para ajudá-los a estar mais bem informados.

SEGURANÇA NO TWITTER

O Twitter é um espaço aberto de livre expressão, do qual todas as pessoas podem participar livremente. Isso permite que seja uma ferramenta útil e relevante para compartilhar e encontrar, de forma rápida, informação atual. Para garantir que as pessoas se sintam seguras ao expressar diversas opiniões e crenças, há regras para o uso da plataforma, a fim de cuidar da saúde da conversa pública e evitar que vozes sejam silenciadas. Nesta seção, são explicadas as Regras do Twitter, que constituem importantes diretrizes para saber o que é e o que não é permitido na plataforma. Também são descritas as ferramentas disponíveis para personalizar e controlar a experiência de cada pessoa na plataforma, para que seja o mais agradável e frutífera possível.

Regras do Twitter

O Twitter reflete as conversas reais que acontecem no mundo, o que inclui, às vezes, perspectivas que para alguns podem ser ofensivas, controversas ou intolerantes. Embora o Twitter seja um espaço participativo onde se podem expressar opiniões diversas, na plataforma não são tolerados comportamentos que utilizem o assédio, a intimidação ou o medo para silenciar a voz de outras pessoas. As regras da plataforma têm por objetivo garantir que todas as pessoas possam participar da conversa pública de maneira livre e segura. Essas regras são divididas em três categorias principais: **segurança, privacidade e autenticidade.**

Segurança

- Violência: não é permitido fazer ameaças violentas contra uma pessoa ou um grupo de pessoas. Também é proibida a glorificação da violência.
- Terrorismo ou extremismo violento: não é permitido fazer ameaças terroristas ou fomentar o terrorismo ou o extremismo violento.
- Exploração sexual infantil: no Twitter existe tolerância zero com respeito à exploração sexual infantil.
- Abuso/assédio: não é permitido participar de situações de assédio dirigidas a uma pessoa ou incitar outros a fazê-lo, o que inclui desejar ou esperar que alguém sofra danos físicos.
- Comportamentos de incitação ao ódio: não é permitido fomentar a violência contra outras pessoas ou ameaçá-las ou assediá-las por motivo de raça, origem étnica, origem nacional, pertencimento a uma casta, orientação sexual, gênero, identidade de gênero, filiação religiosa, idade, deficiência ou doença grave.
- Suicídio e autolesões: não é permitido fomentar ou promover o suicídio ou as autolesões.
- Conteúdo multimídia de caráter delicado, inclusive a violência gráfica e o conteúdo para adultos: não é permitido publicar conteúdo multimídia que seja excessivamente mórbido, ou compartilhar conteúdo violento ou para adultos em vídeos ao vivo ou em imagens de perfil ou de cabeçalho. O conteúdo multimídia em que se representam violência ou abusos sexuais tampouco é permitido.
- Bens ou serviços ilegais ou regulamentados: não é permitido utilizar o Twitter para nenhum propósito ilegal ou para promover atividades ilegais. Isso inclui a venda, compra ou facilitação de transações de bens ou serviços ilegais, além de determinados tipos de bens ou serviços regulamentados.

Privacidade

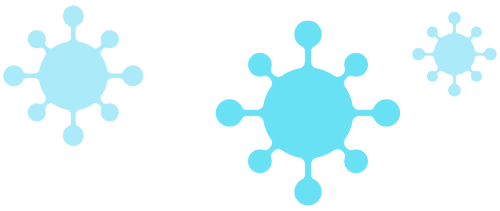
- Informação privada: não é permitido publicar a informação privada de outras pessoas (como o número de telefone e o endereço do domicílio) sem sua autorização e consentimento. Também é proibido ameaçar divulgar informação privada ou incentivar outros a fazê-lo.
- Nudez não consensual: não é permitido publicar ou compartilhar fotos ou vídeos íntimos de outra pessoa que tenham sido produzidos ou distribuídos sem o consentimento dessa pessoa.

Autenticidade

- *Spam* e manipulação da plataforma: não é permitido usar os serviços do Twitter com o propósito de ampliar ou suprimir informação de forma artificial, nem levar a cabo ações que manipulem ou dificultem a experiência das pessoas no Twitter.
- Integridade eleitoral: não é permitido utilizar os serviços do Twitter com a finalidade de manipular eleições ou nelas interferir, o que inclui publicar ou compartilhar conteúdo que possa dissuadir a participação dos votantes ou enganar as pessoas sobre quando, onde ou como votar.
- Falsificação de identidade: não é permitido falsificar a identidade de outras pessoas, grupos ou organizações de maneira a tentar, ou conseguir, confundir ou enganar essas pessoas, ou a elas comunicar uma ideia equivocada.
- Conteúdos multimídia falsos e alterados: é proibido compartilhar, com a intenção de enganar, conteúdo multimídia falso ou alterado que possa provocar danos graves. Do mesmo modo, é possível que se etiquetem Tuítes que incluam conteúdo multimídia falso e alterado para ajudar as pessoas a compreender sua autenticidade e para oferecer mais contexto.
- Direitos de autor e de marca: não é permitido infringir os direitos de propriedade intelectual de outros, inclusive os direitos de autor e de marca.

Informações mais detalhadas sobre as Regras do Twitter, bem como sua versão mais atualizada, estão disponíveis na Central de Ajuda do Twitter ou por meio de: https://twitter.com/rules.

Deve-se levar em conta que as Regras do Twitter estão em constante evolução e é possível que mudem ocasionalmente, a fim de apoiar o objetivo de fomentar uma conversa pública saudável e construtiva. Foi esse o caso após a pandemia de Covid-19, que provocou uma mudança nas regras, com vistas a ampliar a definição de dano e abordar conteúdo diretamente contrário às instruções de fontes autorizadas de informação de saúde pública global e local. Esses processos de atualização são feitos de forma transparente e comunicativa. Por exemplo, durante as mudanças realizadas em consequência da Covid-19, o Twitter manteve as pessoas informadas por meio do blog Coronavírus: Mantenha-se seguro e informado no Twitter.



Aplicação das Regras do Twitter

Quando o Twitter toma medidas de aplicação de suas regras, pode fazê-lo em relação a um conteúdo específico (por exemplo, um Tuíte ou mensagem direta), a uma conta ou combinando essas opções. Na aplicação das regras, o Twitter parte do pressuposto de que as pessoas não descumprem as regras intencionalmente. Por isso, a menos que um descumprimento seja tão flagrante que obrigue a plataforma a suspender uma conta de imediato, primeiro se procura educar as pessoas sobre as Regras do Twitter. Ao fazer isso, o Twitter oferece às pessoas que usam a plataforma a oportunidade de corrigir seu comportamento, mostrando-lhes o Tuíte ou os Tuítes que violam as regras, explicando que regra deixou de ser cumprida e solicitando que se exclua o conteúdo para que a pessoa possa poder voltar a tuitar. Caso uma pessoa descumpra as regras de forma reiterada, as medidas de aplicação dessas regras se tornam mais sérias.

Medidas no âmbito do Tuíte

No âmbito do Tuíte, são tomadas medidas para evitar o excesso de rigor com uma conta que cometeu um erro e descumpriu as regras, mas que, em geral, não apresenta problemas. Entre essas medidas se incluem as que se seguem:

Limitar a visibilidade do Tuíte

Essa medida reduz a visibilidade do conteúdo no Twitter, nos resultados de busca, nas respostas e nas cronologias.

Solicitar a exclusão do Tuíte

Caso se determine que o Tuíte descumpriu as Regras do Twitter, solicita-se à pessoa que cometeu a infração que o exclua para poder voltar a tuitar. Nesses casos, a pessoa recebe uma notificação por *e-mail*, na qual são identificados o Tuíte ou os Tuítes que violam as regras. O Tuíte em questão deverá ser excluído ou a pessoa deve recorrer da decisão, caso considere que se cometeu um erro.

Ocultar um Tuíte infrator enquanto se exclui

No período transcorrido entre uma medida de cumprimento tomada pelo Twitter e a exclusão do Tuíte em questão pela pessoa, para que o público geral não possa vê-lo, o Tuíte é ocultado e substituído por um aviso que indica que o Tuíte já não está disponível porque descumpre as Regras do Twitter. Essa notificação é mantida durante 14 dias depois da exclusão do Tuíte.

Aviso de exceção de interesse público

Em casos muito específicos nos quais se determina que é de interesse público que um Tuíte que descumpre as Regras do Twitter continue acessível na plataforma, coloca-se o Tuíte atrás de um aviso que explica essa exceção e oferece a opção de ver o Tuíte, caso a pessoa queira.

Ao publicar esse aviso, também se tomam medidas para reduzir a visibilidade do Tuíte:

- ✔ Desativar as interações com o Tuíte (respostas, Retuítes e *Curtir*).
- ✔ Não mostrar nenhuma contagem de interações do Tuíte (por exemplo, número de *Curtir* ou respostas).
- ✔ Não expor as respostas anteriores que o Tuíte tenha recebido.
- ✔ Tornar o Tuíte indisponível:
  - Na cronologia de início, em Tuítes destacados.
  - Nos resultados de busca.
  - Nas Recomendações e Notificações.
  - Na aba Explora.

A seção seguinte explica mais detalhadamente os avisos no Twitter e seu significado.

Medidas no âmbito da mensagem direta

Interromper as conversas entre uma pessoa denunciada e a conta do denunciante

Quando um dos participantes de uma conversa privada, ou seja, por Mensagem Direta denuncia o outro participante, o Twitter impede que a pessoa denunciada continue enviando mensagens a quem a denunciou. Além disso, a conversa é excluída da bandeja de entrada do denunciante e só pode ser retomada se o denunciante decidir continuar enviando Mensagens Diretas a essa pessoa.

Colocar uma Mensagem Direta atrás de um aviso

No caso de uma conversa de grupo por Mensagem Direta, é possível que a mensagem infratora seja colocada atrás de um aviso para que ninguém mais no grupo possa voltar a vê-la.

Medidas no âmbito da conta

O Twitter toma medidas no âmbito da conta quando se determina que uma pessoa descumpriu as Regras do Twitter de forma flagrante o que las incumplió reiteradamente incluso después de haber recibido notificaciones al respecto.

Solicitar a modificação da informação ou do conteúdo multimídia do perfil

Caso o perfil ou o conteúdo multimídia de uma conta não cumpram as regras, a conta pode ser suspensa temporariamente e o Twitter, além de comunicar esse fato ao dono da conta, pode solicitar que a pessoa modifique o conteúdo ou a informação de seu perfil para que cumpram as regras.

Configurar uma conta para que seja só de leitura

Caso uma conta que, em geral, não apresenta problemas, apresente um episódio de comportamento abusivo, o Twitter pode modificar temporariamente sua configuração para que seja apenas de leitura, limitando sua capacidade de tuitar, retuitar ou usar a função Curtir por um tempo determinado. A pessoa afetada ainda poderá ver sua cronologia de início e enviar Mensagens Diretas a seus seguidores.

Quando uma conta está em modo só de leitura, os demais podem continuar a vê-la e a interagir com ela. A duração dessa medida de controle do cumprimento pode variar entre 12 horas e sete dias, segundo o tipo de descumprimento.

Verificar a titularidade da conta

Para assegurar que as pessoas não abusem do anonimato que o Twitter oferece, em algumas oportunidades, o Twitter solicita ao titular de uma conta que verifique seu número de telefone ou seu endereço de e-mail para comprovar sua autenticidade. Isso, entre outras coisas, ajuda a identificar e a tomar medidas com respeito a contas que são administradas por uma mesma pessoa para fins abusivos.

Suspensão permanente

Essa é a medida mais séria para garantir a aplicação das regras. A suspensão permanente de uma conta faz com que ela deixe de ser vista em âmbito global, e a pessoa que cometeu a infração não poderá criar contas novas. Quando se suspende uma conta de forma permanente, a pessoa é informada sobre a suspensão por descumprimentos relativos ao abuso e recebe explicações quanto à política ou políticas que descumpriu e ao conteúdo infrator.

Recursos contra essas medidas

Diante de qualquer das ações mencionadas, as pessoas denunciadas ou infratoras podem recorrer dessas medidas, caso considerem que o Twitter cometeu um erro. Podem fazê-lo por meio da interface da plataforma ou mediante o envio de um relatório usando o formulário de recurso.

Informar violações das Regras do Twitter

Caso encontre no Twitter conteúdo que considera que viola alguma das regras da plataforma, o melhor que se pode fazer é comunicar o fato. Ao comunicar, lembre-se de que o contexto que possa proporcionar é muito importante. Do mesmo modo, leve em conta que nem todo o conteúdo que alguns consideram ofensivo ou intolerante viola necessariamente as Regras do Twitter.

No momento de determinar se serão tomadas medidas a respeito de um comunicado, as equipes do Twitter consideram uma série de fatores, entre os quais se incluem:

- Se o comportamento é dirigido a um indivíduo, a um grupo ou a uma categoria protegida de pessoas.
- Se o denunciante é o objeto do abuso ou uma testemunha.
- Se a pessoa denunciada tem antecedentes de descumprimento das regras da plataforma.
- A gravidade do descumprimento.
- Se o conteúdo é um tema de legítimo interesse público.

EM help.twitter.com/forms podem ser encontrados os formulários diretos para qualquer tipo de comunicação sobre violações das Regras do Twitter. Também há opções diretas a partir do twitter.com e do aplicativo para informar sobre Tuítes, contas ou Mensagens Diretas.

Denunciar uma conta:

1. Abra o perfil que deseja denunciar.
2. Escolha o ícone de ***conteúdo adicional*** .
3. Escolha *Denunciar @nome deusuario* e, em seguida, o tipo de violação que deseja denunciar.
4. Dependendo da sua escolha, a plataforma pedirá informação adicional sobre o problema que está denunciando.

Denunciar um Tuíte:

1. Dirija-se ao Tuíte que deseja denunciar.
2. Pressione o ícone de *conteúdo adicional* situado na parte superior do Tuíte.
3. Escolha *Denunciar Tuíte.*
4. Dependendo da sua escolha, a plataforma pedirá informação adicional sobre o problema que está denunciando.

Denunciar uma Mensagem Direta:

1. Clique na conversa de Mensagens Diretas que quer denunciar.
2. Clique no ícone de *conteúdo adicional* .
3. Escolha *Denunciar @nome deusuario.*
4. Dependendo da sua escolha, a plataforma pedirá informação adicional sobre o problema que está denunciando.

Avisos no Twitter e seu Significado

Levando em conta algumas das medidas citadas anteriormente, o Twitter coloca um aviso na conta ou no Tuíte para oferecer mais contexto às pessoas sobre as medidas de cumprimento tomadas. É importante entender o significado desses anúncios para saber a diferença entre, por exemplo, uma conta que foi desativada pela pessoa ou uma conta que foi suspensa temporariamente; ou entre um Tuíte que foi excluído pelo autor original e um Tuíte que violou as regras da plataforma. Figuram abaixo alguns dos avisos que podem ser encontrados no Twitter:

> Este Tweet pode incluir conteúdo sensível.

> A mídia a seguir inclui conteúdo possivelmente sensível. **Alterar configurações**

Aviso de conteúdo multimídia sensível, não adequado para menores ou que inclui violência gráfica. Nesse caso, as pessoas são informadas de que, caso decidam clicar no aviso, verão conteúdo multimídia sensível.

Aviso de conteúdo de interesse público. Corresponde a casos muito específicos nos quais se determina que um Tuíte que descumpre as regras do Twitter é de interesse público, e por isso continuará acessível na plataforma. Esse Tuíte é colocado atrás de um aviso que explica a exceção e oferece a opção de ver o Tuíte caso a pessoa queira.

> Este Tweet violou as Regras do Twitter sobre [regra específica]. No entanto, o Twitter determinou que pode ser do interesse público que esse Tweet continue acessível. **Saiba mais**

> Este Tweet violou as Regras do Twitter. **Saiba mais**

Aviso em relação a um Tuíte excluído que descumpriu as regras. O Tuíte que descumpra as regras e ainda não tenha sido eliminado pela pessoa que o tuitou será colocado atrás de um aviso e a conta permanecerá bloqueada até que o autor o exclua. Uma vez excluído o Tuíte, o aviso permanecerá na plataforma por 14 dias mais.

Aviso em relação a um Tuíte de uma conta suspensa. Tuítes de uma conta suspensa por violações das Regras do Twitter aparecem ocultos atrás de um aviso com essa informação.

> Este Tweet pertence a uma conta suspensa. **Saiba mais**

> Você denunciou este Tweet. **Ver**

Aviso em relação a um Tuíte denunciado. Ao denunciar um Tuíte, a conta que faz a denúncia verá o Tuíte atrás de um aviso com essa indicação e terá a opção de escolher se deseja ou não voltar a ver esse conteúdo.

Aviso em relação a um Tuíte de uma conta bloqueada ou silenciada. Caso tenha silenciado ou bloqueado uma ou várias contas e outra pessoa compartilhe seus Tuítes, o conteúdo desses Tuítes aparecerá oculto atrás de um aviso, mas haverá a opção de clicar para vê-lo.

> Este Tweet pertence a uma conta que você colocou no mudo. **Ver**

Caso tenha silenciado palavras ou hashtags, receberá um aviso similar:

> Este Tweet inclui uma palavra que você silenciou. **Ver**

O proprietário desta conta limita quem pode ver seus Tweets. **Saiba mais**

Aviso em relação a um Tuíte com visibilidade limitada. Esse aviso aparece nos casos em que um Tuíte não está disponível, e tem por objetivo verificar se, por exemplo, é um Tuíte de uma conta protegida, ou seja, só as pessoas que o seguem podem ver seu conteúdo ou se é um Tuíte de uma conta que o tenha bloqueado.

Este Tweet não está disponível. **Saiba mais**

O Tuíte foi eliminado pelo próprio autor.

Este Tweet pertence a uma conta que não existe mais. **Saiba mais**

O Tuíte é de uma conta que foi desativada.

Aviso em relação a uma conta que deve verificar sua autenticidade. Quando se solicita ao titular de uma conta que verifique sua autenticidade com um número de telefone ou um endereço de e-mail, essa conta é temporariamente restrita, até que se preste a informação solicitada.

Cuidado: esta conta está temporariamente restrita. **Sim, ver perfil**

Essa conta não existe. Tente buscar outro(a).

Aviso de conta desativada. Os titulares de contas têm a escolha de desativar sua conta a qualquer momento. Quando o titular de uma conta a desativa, a página se mostra como não disponível.

Aviso de suspensão permanente. Caso uma conta tenha sido suspensa por violar as Regras do Twitter, essa informação figura na conta em questão.

O Twitter suspende as contas que violam as Regras do Twitter.

Relatório de transparência do Twitter

Seguindo o princípio de transparência e no entendimento de que o intercâmbio livre de informações pode ter impacto positivo, desde 2012, o Twitter vem publicando um relatório semestral de transparência. Esse relatório divulga informação sobre as solicitações de informação e de exclusão que o Twitter recebe das autoridades, notificações de infração de direitos de autor e de marcas comerciais, aplicação das Regras do Twitter, e instâncias de manipulação da plataforma, inclusive operações de informação que a plataforma determinou que contam com o apoio de Estados.

Controle sua experiência no Twitter

O Twitter é um lugar pensado para compartilhar ideias e informações, conectar-se com a comunidade e conhecer o ambiente em que se vive. Com o propósito de proteger essa experiência, o Twitter oferece ferramentas que permitem personalizar e controlá-la, o que se vê e o que se permite que outros vejam de si mesmo, de forma que todas as pessoas possam expressar-se no Twitter com segurança.

Filtro de Notificações

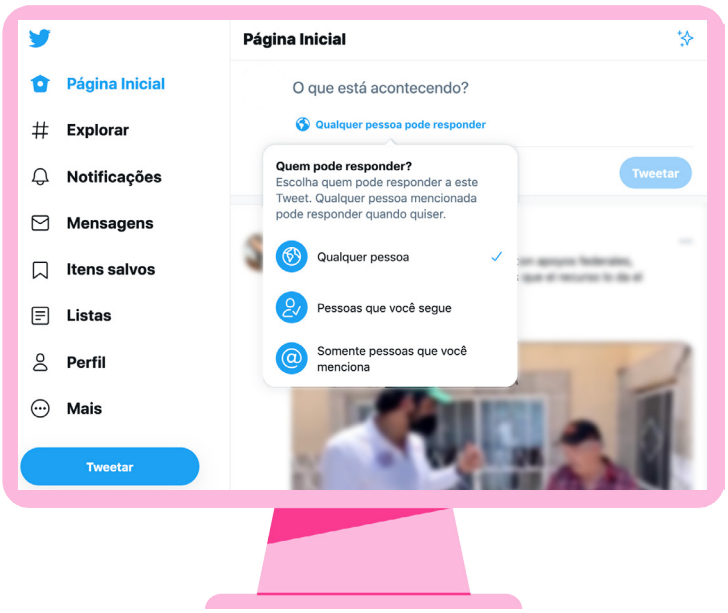
A cronologia de Notificações mostra as interações com outras contas de Twitter, como as menções, os *Curtir*, os Retuítes e quem começou a segui-lo. Caso se recebam respostas ou menções não desejadas, é possível filtrar os tipos de notificações recebidas. Na configuração das Notificações, há três opções para filtrar as notificações recebidas: filtro de qualidade, palavras silenciadas e filtros avançados.

- **Filtro de qualidade:** filtra o conteúdo de menor qualidade para que não apareça em suas notificações (por exemplo, os Tuítes duplicados ou conteúdo que pareça automatizado), mas não se filtram as notificações das pessoas seguidas ou das contas com as quais interagiu recentemente.
- **Palavras silenciadas:** silencia as notificações que incluam palavras e frases específicas que não se quer ver nas notificações.
- **Filtros avançados:** permitem desativar as notificações de certos tipos de conta, por exemplo, contas que não se seguem entre elas, ou que usam a foto de perfil predeterminada do Twitter, ou que não tenham um e-mail ou número de telefone registrado para confirmar sua autenticidade.

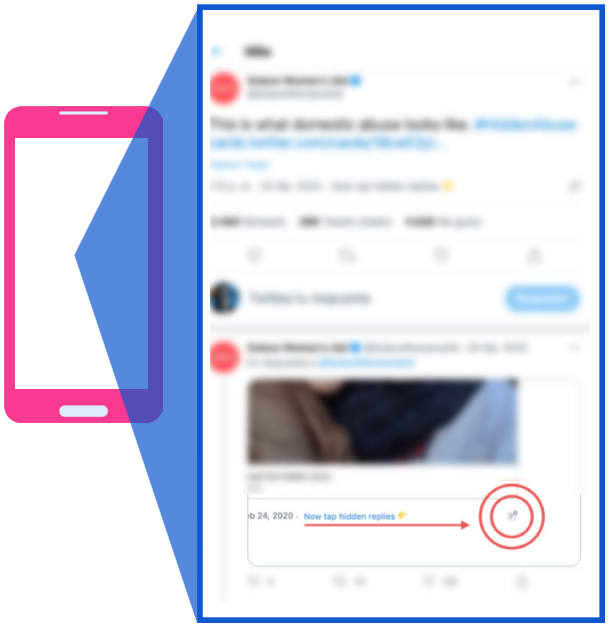
Controle de respostas

Quando se escreve um Tuíte, é possível escolher quem pode respondê-lo. De forma predeterminada, está selecionada a opção *Qualquer pessoa pode responder* na parte inferior esquerda no compositor do Tuíte. Ao clicar ou pressionar essa opção antes de publicar um Tuíte, pode-se escolher quem pode responder a esse Tuíte especificamente. As opções são: *Todos, Pessoas que segue* ou *Só as pessoas mencionadas nesse Tuíte.*

As pessoas verão se foi estabelecido um limite em relação a quem pode responder a um Tuíte, e não é possível mudar as restrições uma vez que se tenha publicado um Tuíte.



Respostas ocultas



Para ajudar as pessoas a manter o controle das conversas que iniciaram, o Twitter dispõe de uma ferramenta que permite ao autor do Tuíte ocultar respostas específicas que seu conteúdo recebe. Todas as pessoas podem continuar acessando as respostas ocultas, por meio do ícone ***resposta oculta*** , que aparece no Tuíte original quando há respostas ocultas. O autor do Tuíte pode ocultar ou deixar de ocultar uma resposta em qualquer momento e o autor dessa resposta não receberá notificação a esse respeito.

Para ocultar uma resposta, clique ou pressione o ícone de ***conteúdo adicional*** do Tuíte que quer ocultar, escolha *Ocultar resposta* e confirme. Para ver as respostas ocultas, clique ou pressione o ícone ***resposta oculta*** que estará disponível no canto inferior direito do Tuíte inicial.

Silenciar

É possível silenciar contas, palavras ou conversas:

Silenciar uma conta no Twitter significa que os Tuítes dessa conta não aparecerão em sua cronologia de início. As contas silenciadas não recebem nenhum tipo de aviso para informar que foram silenciadas. Além disso, as notificações de menções dessas contas continuarão ativas, bem como o intercâmbio de Mensagens Diretas. Também é possível silenciar contas que não são seguidas para ocultar seus Tuítes da cronologia de notificações.

Para silenciar uma conta, pressione o ícone de ***conteúdo adicional*** em um Tuíte e clique em *Silenciar*. Para deixar de silenciar uma conta, visite o perfil de Twitter da conta silenciada e clique no ícone de ***conteúdo adicional*** da conta e, em seguida, em *Deixar de silenciar @nome deusuario* para deixar de silenciar.

Silenciar palavras, frases, nomes de usuário, emojis ou *hashtags.* A opção de silenciar fará com que esses Tuítes não apareçam na aba de Notificações, notificações *push*, notificações de e-mail, cronologia de início e respostas, embora esses Tuítes ainda fiquem visíveis em resultados de buscas. Para adicionar ou excluir itens em sua lista de silenciados:

1. Clique em *Configuração e privacidade* no menu suspenso de sua imagem de perfil.
2. Clique em *Preferências de conteúdo*.
3. Clique em *Silenciado*.
4. Clique em *Palavras silenciadas* e, em seguida, em *Adicionar*.
5. Insira a palavra ou o *hashtag* que deseja silenciar, um de cada vez.
6. Escolha *Cronologia de início*, caso deseje silenciar a palavra ou a frase em sua Cronologia de início, ou *Notificações*, caso deseje silenciar a palavra ou a frase em suas Notificações.
7. Escolha a opção *De qualquer usuário* ou *Somente de pessoas que não sigo*.
8. Na seção Por quanto tempo?, escolha entre as opções *Para sempre, 24 horas a partir de agora, 7 dias a partir de agora* ou *30 dias a partir de agora*.
9. Clique em *Aceitar*.

Silenciar conversas faz com que não sejam recebidas as notificações de uma conversa. Quando se silencia uma conversa, não se recebe nenhuma notificação relacionada, mas os Tuítes da conversa ainda são visíveis na cronologia e também ao clicar no Tuíte original. Para silenciar uma conversa:

1. Clique no ícone de ***conteúdo adicional*** de qualquer Tuíte ou resposta da conversa que deseja silenciar.
2. Clique ou pressione Silenciar esta conversa.
3. Pressione ou clique para confirmar.

Bloquear

O bloqueio de uma conta no Twitter impede que essa conta interaja com a conta que a bloqueou. O bloqueio pode ser útil para controlar as interações não desejadas provenientes de contas com as quais a pessoa não tem interesse em se relacionar. As contas bloqueadas não podem ver os Tuítes, as interações, a quem segue ou quem segue a conta que a bloqueou, desde que tenham uma sessão aberta no Twitter. Tampouco serão recebidas notificações de contas bloqueadas ou seus Tuítes serão vistos na cronologia. É possível que a pessoa que administra uma conta que tenha sido bloqueada note que foi bloqueada, caso tente visitar o perfil ou seguir a conta que a bloqueou, mas não receberá notificações que a avisem do bloqueio.

Para acessar essa opção, pressione o ícone de ***conteúdo adicional*** em um Tuíte dessa conta, ou a partir de seu perfil, e clique em *Bloquear*. Para desbloquear uma conta, no perfil da conta do Twitter, clique no botão *Bloqueado* e confirme que deseja desbloquear a conta.

CONSIDERAÇÕES FINAIS

O conteúdo apresentado neste documento, desenvolvido pela **OEA** e pelo **Twitter**, pretende informar e conscientizar as pessoas sobre o manejo, o consumo e a distribuição de informação *online*, com enfoque nas redes sociais, especialmente no Twitter. Este guia tem por objetivo contribuir para que todas as pessoas, inclusive jornalistas, autoridades governamentais e organizações, compreendam melhor a importância da alfabetização e da segurança cibernética.

O aumento das atividades digitais mostrou vulnerabilidades preexistentes do espaço digital. O crescimento do número de ataques cibernéticos e da digitalização de inumeráveis processos cotidianos reafirma a necessidade do aumento da alfabetização e da conscientização quanto a boas práticas de segurança cibernética. Esta edição do guia oferece uma visão renovada sobre ferramentas e boas práticas para consumir informação e conteúdo de maneira segura e responsável.

As plataformas tecnológicas e as redes sociais criaram novas modalidades de comunicação, ampliando as possibilidades de participação política, ao permitir que o ambiente digital esteja envolvido nos processos democráticos. A alfabetização digital é essencial para o fortalecimento da democracia, dado que é um instrumento que contribui para uma participação maciça que facilita uma participação cidadã ativa e responsável. Do mesmo modo, a alfabetização neutraliza fenômenos como a desinformação, a ingerência de atores externos na política interna, entre outros elementos, que direta ou indiretamente impactam e influenciam os processos democráticos.

As diferentes seções compilam informação relacionada à segurança cibernética e ao autocuidado digital, a qual foi atualizada para apresentar as novas ameaças e ferramentas surgidas em função das mudanças no ambiente e no aumento do teletrabalho. Do mesmo modo, o guia inclui recomendações específicas em relação ao consumo de informação do Twitter e à atualização de suas regras de uso, além de ferramentas fundamentais para a experiência das pessoas na plataforma.

DADO QUE A ALFABETIZAÇÃO E A SEGURANÇA DIGITAL, BEM COMO A COMPLEXIDADE DOS DELITOS ONLINE, ESTÃO, POR SUA PRÓPRIA NATUREZA, SE DESENVOLVENDO DE MANEIRA CONSTANTE, É VITAL PERMANECER INFORMADOS E ATUALIZADOS QUANTO AOS PRODUTOS E POLÍTICAS QUE AFETAM O DESENVOLVIMENTO E AS INTERAÇÕES EM MEIOS DIGITAIS E REDES SOCIAIS.

O uso intenso das tecnologias digitais no mundo permanecerá na vida cotidiana, e, por esse motivo, a segurança cibernética e a alfabetização, aplicadas por parte de cada indivíduo, são sumamente importantes para garantir e capitalizar o benefício da conectividade e da disponibilidade de informação de maneira segura, a fim de propiciar um ambiente de maiores possibilidades de desenvolvimento, bem como de bem-estar social e fortalecimento da democracia.

Referencias

BBC News Mundo. (2020). *Coronavírus: a advertência da OMS sobre os fraudadores que estão usando o nome da organização para roubar dinheiro e dados.* https://www.bbc.com/mundo/noticias-52009138

Duclkin, Paul. (2020). *Dirty little secret extortion email threatens to give your family coronavirus. Sophos* https://nakedsecurity.sophos.com/2020/03/19/dirty-little-secret-extortion-email-threatens-to-give-your-family-coronavirus/

Eset. *Social Engineering (in cybersecurity).* https://www.eset.com/int/social-engineering-business/

CPJ. (2019). Cobrindo eleições: kit de segurança para jornalistas. https://cpj.org/pt/2020/10/cobrindo-eleicoes-kit-de-seguranca-para-jornalistas/

Germain, Thomas. (2019). *How a Photo's Hidden 'Exif' Data Exposes Your Personal Information.* Consumer Reports. https://www.consumerreports.org/privacy/what-can-you-tell-from-photo-exif-data/

INCIBE y OSI. (2020). *Detectada onda de falsos e-mails de sextorsão ou infecção de Covid-19.* https://www.osi.es/es/actualidad/avisos/2020/04/detectada-oleada-de-falsos-correos-de-sextorsion-o-infeccion-de-covid19

Marsh y Microsoft. (2020). *Situação de risco cibernético na América Latina em tempos de Covid-19.* https://coronavirus.marsh.com/mx/es/insights/research-and-briefings/report-cyber-risk-in-latin-america-in-times-of-covid19.html

Media and Information Literacy for the Sustainable Development Goals. Grizzle, A and Singh, J. (2016). In the MILID Yearbook 2016.

News and Media Literacy: What is Media Literacy, Common Sense Media: https://www.commonsensemedia.org/news-and-media-literacy/what-is-digital-literacy (consultado el 18 de agosto de 2019).

NortonLifeLock. *O que é engenharia social?.* https://lam.norton.com/Internetsecurity-emerging-threats-what-is-social-engineering.html

Organização Mundial da Saúde. (2020). *WHO reports a fivefold increase in cyber attacks, urges vigilance.* https://www.who.int/news/item/23-04-2020-who-reports-fivefold-increase-in-cyber-attacks-urges-vigilance

Organização das Nações Unidas. Comissão Econômica para a América Latina e o Caribe. Relatório Especial Covid-19 (2020). *Universalizar o acesso às tecnologias digitais para enfrentar os efeitos da Covid-19.* https://repositorio.cepal.org/bitstream/handle/11362/45938/4/S2000550_es.pdf

Organização das Nações Unidas para a Educação, a Ciência e a Cultura. (2016). *Alfabetização.* https://es.unesco.org/themes/alfabetizacion

Organização dos Estados Americanos e Twitter. (2019). *Alfabetismo e Segurança Digital: melhores práticas no uso do Twitter.* https://www.oas.org/es/sms/cicte/docs/20190913-DIGITAL-Alfabetismo-y-segurança-digital-Twitter.pdf

Organização dos Estados Americanos. (2019). *Guia para garantir a liberdade de expressão frente à desinformação deliberada em contextos eleitorais.* http://www.oas.org/es/cidh/expresion/publicações/Guia_Desinformacion_VF.pdf

Porter, Taryn. (2020). COVID-19 *Scam Alters. Cybercrime Support Network.* https://cybercrimesupport.org/covid-19-scam-alerts/

Roesler, Martin.(2020). *Working From Home? Here's What You Need for a Secure Setup.* Trend Micro. https://www.trendmicro.com/vinfo/ph/security/news/cybercrime-and-digital-threats/working-from-home-here-s-what-you-need-for-a-secure-setup

Software Lab.org. *O que é engenharia social? A definição e os cinco exemplos principais Qué es engenharia social.* https://softwarelab.org/es/que-es-ingenieria-social/

Stone, Jeff. (2020). *How scammers use fake news articles to promote coronavirus 'cures' that only defraud victims.* Cyberscoop. https://www.cyberscoop.com/coronavirus-cure-scam-social-media-riskiq/

Trend Micro.(2020). *Developing Story: COVID-19 Used in Malicious Campaigns.* https://www.trendmicro.com/vinfo/fr/security/news/cybercrime-and-digital-threats/coronavirus-used-in-spam-malware-file-names-and-malicious-domains

U.S. Department of Homeland Security. (2019). *Social Media Plan Guide: Science and Technology Directorate.* https://www.dhs.gov/sites/default/files/publications/social_media_plan_guide_09_20_2019.pdf

We Live Security y eset. (2020). *Relatório de Ameaças. Segundo Trimestre de 2020.* https://www.welivesecurity.com/wp-content/uploads/2020/08/Q2-2020_Threat_Report-ESP.pdf

ALFABETIZAÇÃO E SEGURANÇA DIGITAL

A IMPORTÂNCIA DE SE MANTER SEGURO E INFORMADO

OEA | Mais direitos para mais pessoas