MISA MOÇAMBIQUE

Guião de Segurança Digital para Jornalistas

Outubro de 2023

Nota introdutória

Não existem dúvidas sobre a importância da Internet nas sociedades contemporanêas. No contexto das liberdades de imprensa e de expressão, pode se destacar, entre vários contributos da Internet, o seu inestimável papel na democratização do acesso à informação e dos forúns de debate de ideias, fora das barreiras dos *media* tradicionais.

Contudo, ao mesmo tempo que trouxe benefícios incalculáveis para a vida em sociedade, a Internet gerou enormes desafios. A título de exemplo, alguns governos recorrem a ferramentas da Internet para criminalizar vozes críticas, da mesma forma que empresas colocam o lucro acima dos direitos humanos, não oferecendo mecanismos seguros de protecção aos seus usuários contra assédio, ódio e violência que enfrentam nas plataformas operadas por essas empresas (Geybullayeva, 2022).

Na comunicação social, as ameaças e assédio online enfrentados por jornalistas atingiram um nível sem precedentes, com uma tendência geral crescente de autoritarismo digital, tornando o trabalho dos jornalistas difícil, perigoso e, às vezes, impossível – as ameaças e assédio online enfrentados por jornalistas tornaram-se, pois, "a nova linha de frente para a segurança dos jornalistas" (Geybullayeva, 2022:3).

Se é verdade que qualquer cidadão que usa Internet deixa impressões digitais[1], a situação é, de facto, muito mais crítica para a classe jornalística, particularmente os jornalistas de investigação que, muitas vezes, não estão a fazer pesquisas banais ou normais - habitualmente, estão a cavar dados, em alguns casos informações sensíveis ou que alguém não quer que sejam do conhecimento público, e isso torna as suas peugadas digitais mais interessantes que de um simples usuário da Internet, que apenas está a usar google para compras ou ver tendências de moda.

Além de ameaçar a sua segurança, os ataques de diversa ordem que os jornalistas sofrem no espaço digital levam, até, a traumas, o que justifica a importância de massificar treinamentos e consciencialização de profissionais de comunicação social sobre a importância da segurança digital na actual era das Tecnologias de Informação e Comunicação.

É neste contexto que surge este guião sobre segurança digital, com dicas sobre como jornalistas e outros profissionais do sector se podem manter seguros no ambiente digital. Produzido pelo MISA Moçambique, no âmbito do Projecto de Promoção da Liberdade de Expressão e Direitos Digitais, em Moçambique, que conta com apoio do Canadá, este guião é uma compilação de melhores práticas sobre segurança digital, desenvolvidas por diversas organizações internacionais aqui mencionadas.

É entendimento do MISA que jornalistas devem pensar nas informações pelas quais são responsáveis e no que pode acontecer se caírem em mãos erradas, e tomar medidas para defender as suas contas, dispositivos, comunicações e actividade online.

Mas, para o MISA, a segurança de jornalistas no espaço digital não é só uma questão de protecção desta classe. Mais do que isso, proteger jornalistas no espaço digital é, também, proteger as fontes de informação e, em geral, proteger a sociedade, perante governos e corporações que não querem que seus segredos sejam expostos, conforme uma das missões vitais do jornalismo em sociedades democráticas.

1 Aqui entendidas como as peugadas ou os rastros do usuário do espaço digital. As peugadas digitais podem ser deixadas de forma activa ou passiva. Considera-se que deixamos as nossas impressões digitais de forma activa quando, deliberadamente, partilhamos informações, fazendo publicações ou participando em sites das redes sociais digitais. Se estamos numa rede com uma conta ou perfil, qualquer publicação que fazemos é parte desse ecossistema de impressões digitais de forma activa. Também deixamos nossas impressões digitais, activamente, quando subscrevemos newsletter ou aceitamos cookies nos nossos navegadores. Por sua vez, as impressões digitais passivas ocorrem quando nossas informações são recolhidas sem nós sabermos – por exemplo, os sites das redes sociais digitais e de publicidade usam nossos likes, partilhas e comentários para definir o nosso perfil e, por essa via, nos direcionarem seus produtos (AMWIK, 2021).

Dicas para segurança de jornalistas no espaço digital

- Faça pesquisa online para ter ideia de informação publicamente disponível a seu respeito. Veja o que aparece. A sua informação pessoal, como endereço de casa, número de celular ou e-mail pessoal, estão alistados online? Se sim, procure removê-los. Há algo que lhe pode colocar em risco? Caso sim, procure ver como limitar ou eliminar a informação que pode ser comprometedora.

- Qualquer informação que partilha, incluindo com instituições, expande as suas impressões digitais, aumentando a possibilidade de essa informação ser inapropriamente usada. Então, antes de submeter informação a instituições, pense nos riscos à volta e limita a quantidade de dados que partilha sobre si. Lembre-se de que seu provedor de serviços de Internet pode manter seus dados e liberar suas informações confidenciais para o governo e as autoridades policiais, se eles solicitarem. Mais ainda, o fornecedor do sítio Web pode ser obrigado ou solicitado pelas autoridades a fornecer os dados do utilizador, incluindo mensagens privadas e conteúdos «eliminados».

- Se decidir fornecer informação, então, forneça apenas a que é absolutamente necessária. Pode, inclusivamente, fornecer nomes e endereços falsos e outros detalhes não correctos, quando não é absolutamente necessário fornecer informação pessoal para obter serviços e quando tal não implicar penalização – exemplo: para aceder Wi-Fi no aeroporto, hotel, etc.

- Configure alertas do Google que irão notificá-lo se o seu nome (inclua erros ortográficos e encurtamentos comuns, por exemplo, Alexander - Alex - Lex), número de telefone, endereço residencial ou outros dados privados sobre si aparecerem online.

- Antes de se inscrever num serviço online, descubra: i) Quem é/são o (s) proprietário (s) do serviço?; ii) Que dados sobre si conservam?; iii) Partilham os dados com mais alguém?; iv) A empresa já foi hackeada antes?; v) O seu Fornecedor de Serviços de Internet tem acesso aos seus dados pessoais de inscrição, histórico de navegação, localização, conteúdo que você assiste? Redes como Facebook, Twitter, etc, coleccionam quantidades excepcionais de informação, colocando em risco os usuários.

- Certifique-se de que altera as definições de privacidade das suas contas de redes sociais digitais para garantir que as informações privadas não estão acessíveis ao público. No Facebook, por exemplo, aceda a **Definições de Privacidade > Verificação de Privacidade > Quem pode ver o que partilha** ou **as suas definições de dados no Facebook** e reveja-as. O mesmo aplica-se aos seus dispositivos electrónicos. A maioria deles, incluindo telemóveis, tem uma secção de configurações, onde você pode ver quais programas/aplicativos têm acesso a tudo – você pode desactivar permissões que não se lembra de ter concedido.

- Leia os Termos de Serviço e revisite-os sempre: as mudanças regulares nos Termos de Serviço por muitas plataformas de redes sociais digitais, muitas vezes, levam a mudanças nas configurações de privacidade disponíveis ou nos padrões, tornando as informações anteriormente consideradas "privadas" mais livremente acessíveis a outros.

- Evite ter ou usar aplicativos de redes sociais digitais em dispositivos que contêm informações confidenciais, pois eles colectam informações do seu dispositivo. Idealmente, aceda a sites de redes sociais através de um navegador que proteja a privacidade.

- Crie senhas fortes, tanto para contas de e-mail e redes sociais digitais, como para dispositivos electrónicos como telemóveis e computadores: as senhas são sua primeira linha de defesa. Senhas fortes tornam-se difíceis de quebrar e/ou invadir, incluindo por hackers.

- O que faz uma boa senha? Deve ser longa (preferencialmente acima de 16 caracteres e, pelo menos, 14 caracteres); torna-a alfanumérica, contendo letras maiúsculas e minúsculas, bem como números e símbolos. Prefira as chamadas "passphrases" ao invés de "passwords" que, além de símbolos e números, incluem frases que consistem em várias palavras, idealmente não relacionadas. Não inclua informações pessoais identificáveis, que podem ser facilmente encontradas no espaço digital, como a sua data de nascimento – estas informações podem ser facilmente encontradas e/ou advinhadas.

- Mude a senha frequentemente e não a reutilize em várias plataformas.
- Escrever suas senhas em um pedaço de papel que você guarda em sua gaveta ou carteira ou colar no monitor do seu computador nunca é uma boa ideia. Grave-as na mente ou em gestores de password (como KeePassXC ou KeePassDroid para androind) e MiniKeePass (para iOS).
- Não compartilhe senhas com ninguém e não deixa que alguém veja a senha sendo inserida na sua tela.
- Não confie no seu navegador para guardar palavras-passe, através de opções como "Save My Password" ou "Remember Me", configurações salvas em sites através de um navegador. A segurança subjacente a estes serviços é, muitas vezes, indocumentada.
- Se possível, evite usar computadores públicos ou partilhados, como em Internet-Café ou salas de imprensa. Se tiver de utilizar um computador público, evite iniciar sessão nas suas contas pessoais. Se tiver de usar contas pessoais, certifique-se de que, imediatamente a seguir, termina todas as sessões e limpa o seu histórico de navegação – além de riscos de se aceder à sua informação, computadores públicos podem estar infectados por vírus.
- Cuidado com o Wi-Fi público: Quando você está em uma rede Wi-Fi (mesmo que seja uma rede protegida por senha), o seu tráfego da Web pode ser facilmente interceptado. A melhor protecção é usar uma Rede Privada Virtual (VPN, na sigla em inglês) para criptografar seu tráfego da Web para que ele não possa ser interceptado.
- Preferencialmente, conecte-se à sua rede móvel, criando um hotspot do seu telefone e evite se conectar à rede fornecida quando estiver em locais públicos, porque pode haver uma probabilidade de monitoramento de rede pelas autoridades ou até mesmo um risco de infecção por vírus.
- Em adicção a passwords longos, habilite o chamado Two-Factor Authentication (2FA), que é uma camada extra de segurança para as suas contas. Depois de introduzir a sua palavra-passe para iniciar sessão, ser-lhe-á pedido um código adicional que é frequentemente gerado numa aplicação ou enviado para o seu telemóvel através de um serviço de mensagens (exemplo de FreeOTP i).
- Desenvolva obsessão por códigos: introduza códigos em discos rígidos de computadores, telefones, tablets e dispositivos de armazenamento externos, para garantir que outras pessoas não possam acessar essas informações sem uma senha.
- Bloqueie toda e qualquer aplicação com um PIN ou código de acesso sempre que possível para melhor se proteger contra alguém que abra a aplicação se tiver acesso físico ao seu telemóvel.
- Configure um bloqueio de registo para exigir que alguém que queira instalar uma aplicação com o seu telemóvel tenha de introduzir o seu número PIN.
- Use, preferencialmente, aplicativos que fornecem comunicação criptografada, como o Signal, para se comunicar: a encriptação envolve a conversão de texto simples legível por humanos em texto incompreensível, conhecido como texto cifrado. É a maneira mais simples e importante de garantir que as informações de um sistema de computador não possam ser roubadas e lidas por alguém que queira usá-las para fins maliciosos.
- Evite chamadas e SMS normais: utilize-as para trocar informações sensíveis apenas em circunstâncias excepcionais, como em situações de emergência.
- Aplicativos como o WhatsApp ou Signal oferecem a possibilidade de definir fotos e vídeos para excluir depois de visualizá-los. Pode ser útil activá-lo se você estiver enviando imagens confidenciais. O WhatsApp e o Signal também oferecem criptografia de ponta a ponta para chamadas de vídeo.
- Se estiver preocupado com a possibilidade de o seu telemóvel ser tomado e de as suas mensagens serem acedidas, considere activar eliminação automática de mensagens após um certo tempo.
- Faça logout das contas nas redes sociais digitais, sobretudo quando usa dispositivos partilhados. Se a aplicação oferecer a opção "permancer conectado", trate de desabilitá-la.
- Desactive os aplicativos de rastreamento de localização ou, pelo menos, limite seu uso o máximo possível. Um telemóvel é como um dispositivo de rastreio: a sua localização é constantemente comunicada à empresa que gere a rede. Mesmo esses dados básicos de localização têm sido usados pelas autoridades para identificar e assediar participantes em protestos, bem como para vigilância geral.
- Use VPN (Virtual Private Network), que é um serviço de segurança da Internet que permite, aos usuários, acessar a Internet como se estivessem conectados a uma rede privada. Isso criptografa a comunicação na Internet e fornece um grau substancial de anonimato. Isso significa que seu endereço IP será mascarado, garantindo que ninguém possa rastrear seus dispositivos e geolocalização, e você pode pesquisar e navegar na Internet sem nada ou ninguém mantendo registros digitais de sua actividade e histórico. Um usuário que se conecta à Internet usando um serviço VPN tem um nível mais alto de segurança e

privacidade. No entanto, você deve estar ciente de que sua VPN tem acesso ao seguinte: i) Dados pessoais de inscrição; ii) Endereço IP e localização; iii) Histórico de navegação; iv) Conteúdo que você assiste e; v) Quanto tempo você gasta olhando para as coisas na Internet.

- Use HTTPS: HTTPS é oficialmente conhecido como "protocolo de transferência de hipertexto seguro". É semelhante ao HTTP, que é usado para inserir endereços de Internet. No entanto, o HTTPS adiciona uma camada extra de segurança e criptografia enquanto estiver online. A comunicação entre usuários e sites que suportam HTTPS é criptografada e autenticada. Isso significa que o HTTPS pode determinar se um site é genuíno ou não.

- Descarregue programas/aplicativos apenas de fontes fidedignas. Se você quiser baixar qualquer aplicativo, obtenha-o na Play Store (para Android) ou na App Store (iOS). As lojas de aplicativos oficiais examinam aplicativos para possíveis problemas de segurança ou privacidade. Descarregar aplicações de sites inseguros torna-o presa fácil para vírus e potenciais abusos online.

- Baixe apenas os aplicativos necessários. Desligue as aplicações que não está a utilizar e elimine as que não precisa. Elas podem estar a funcionar em background, colectando seus dados.

- Suspeite documentos e/ou links enviados para o seu telemóvel por e-mail, SMS ou redes sociais digitais: para estar seguro, se você receber um e-mail que inclui um link para um site, certifique-se de que o site é legítimo antes de clicar no link. Por exemplo, em vez de clicar no site, a partir do e-mail, abra um navegador da Web diferente e visite o site da empresa directamente para executar as acções necessárias. Tenha extrema cautela em relação a quaisquer links que sejam compartilhados em páginas ou em grupos relacionados a movimentos políticos ou sociais, especialmente em tempos de agitação civil, pois estes podem ser maliciosos.

- Limpe o histórico do navegador - Os navegadores mantêm registros de cada site que você visita. Certifique-se de limpar o histórico do navegador para todos os dispositivos que você usa em um dia - seus computadores de casa e do trabalho, ou o seu próprio iPad ou de amigos. Os navegadores de Internet como o Firefox ou o Chrome registam onde esteve e o que fez online. Eles mantêm registros de cada site que você visita. As informações sobre o que você enviou ou salvou no seu computador podem ser mantidas por dias ou semanas. Para estar seguro, limpe sempre o seu histórico de navegação.

- Actualize seu sistema operacional, aplicativos e navegadores quando solicitado. O software antigo tem vulnerabilidades que podem ser exploradas para instalar vírus nos seus dispositivos. Isso é especialmente importante se você sentir que pode ser alvo de ataques sofisticados.

- No geral, não use redes sociais digitais para entrevistar as suas fontes. Em vez disso, faça por meio de plataformas mais seguras.

- Nas redes sociais digitais, tenha cuidado com quem você adiciona como amigo ou escolhe seguir. Bloqueie/desfaça amizade com qualquer pessoa que sinta ser uma ameaça ou com quem se sinta desconfortável; caso contrário, você estará se tornando mais um alvo de violência digital.

- Reveja os comentários que os outros deixam nas suas redes sociais. Alguns deles são ameaçadores ou assediadores? Não se envolva em discussões com as pessoas que te atacam, virtualmente. Pelo contrário, certifique-se de bloqueá-las e denuncia-las à plataforma.

- Sem se auto-censurar, mas por precaução, pense antes de fazer publicações controversas no espaço digital como forma de reduzir suas chances de ser violado online.

- Separe o seu trabalho e vida privada online, evitando misturar informações profissionais e pessoais nas contas - isso poderá ajudar a limitar o acesso aos dados se um deles for atacado.

- Algum membro da sua família aparece nas pesquisas relacionadas consigo? Por exemplo, seus filhos são marcados em uma foto sua no Facebook ou Instagram? Toma as medidas necessárias para torná-los anónimos.

- Diga aos seus amigos e familiares para não o marcarem em quaisquer fotos que tenham consigo ou em comentários online. Não se preocupe, ainda não há problema em tirar uma foto com seus amigos.

- Verifique as suas fotos online. Alguma delas pode ser usada para descredibilizá-lo? Certifique-se de removê-la.

- Percorra as suas redes sociais regularmente (entre 3 a 6 meses) e remova qualquer conteúdo que possa violar a sua privacidade e segurança e a da sua família ou amigos.

Referências Bibliográficas

AMWIK (2021). **Handbook on Digital Safety & Security.** Acedido a 11 de Outubro de 2023, em https://amwik.org/wp-content/uploads/2022/04/Digital-security-handbook-A6-Editted-1.pdf

CPJ (2019). **Digital Safety Kity.** Acedido a 15 de Outubro de 2023, em https://cpj.org/2019/07/digital-safety-kit-journalists/

Ctemplar (2023). Best Practices and Tips for Digital Security and Privacy for Journalists. Acedido a 13 de Agosto de 2023, em https://ctemplar.com/best-practices-and-tips-for-digital-security-and-privacy-for-journalists/

Geybullayeva, Arzu (2022). **Online Safety and Digital Security for all Journalists: a prerequisite for media freedom.** Organization for Security and Co-operation in Europe (OSCE) Representative on Freedom of the Media (RFoM). Vienna, Austria. Acedido a 10 de Outubro de 2023, em https://www.osce.org/files/f/documents/7/d/522169.pdf

Digital Safety Manual (s.d.). **Welcome to the Digital Safety Manual.** Acedido a 15 de outubro de 2023, em https://digitalsafetymanual.org/

Com apoio:

CFLI/FCIL
Fundo Canadá para Iniciativas Locais

Canada