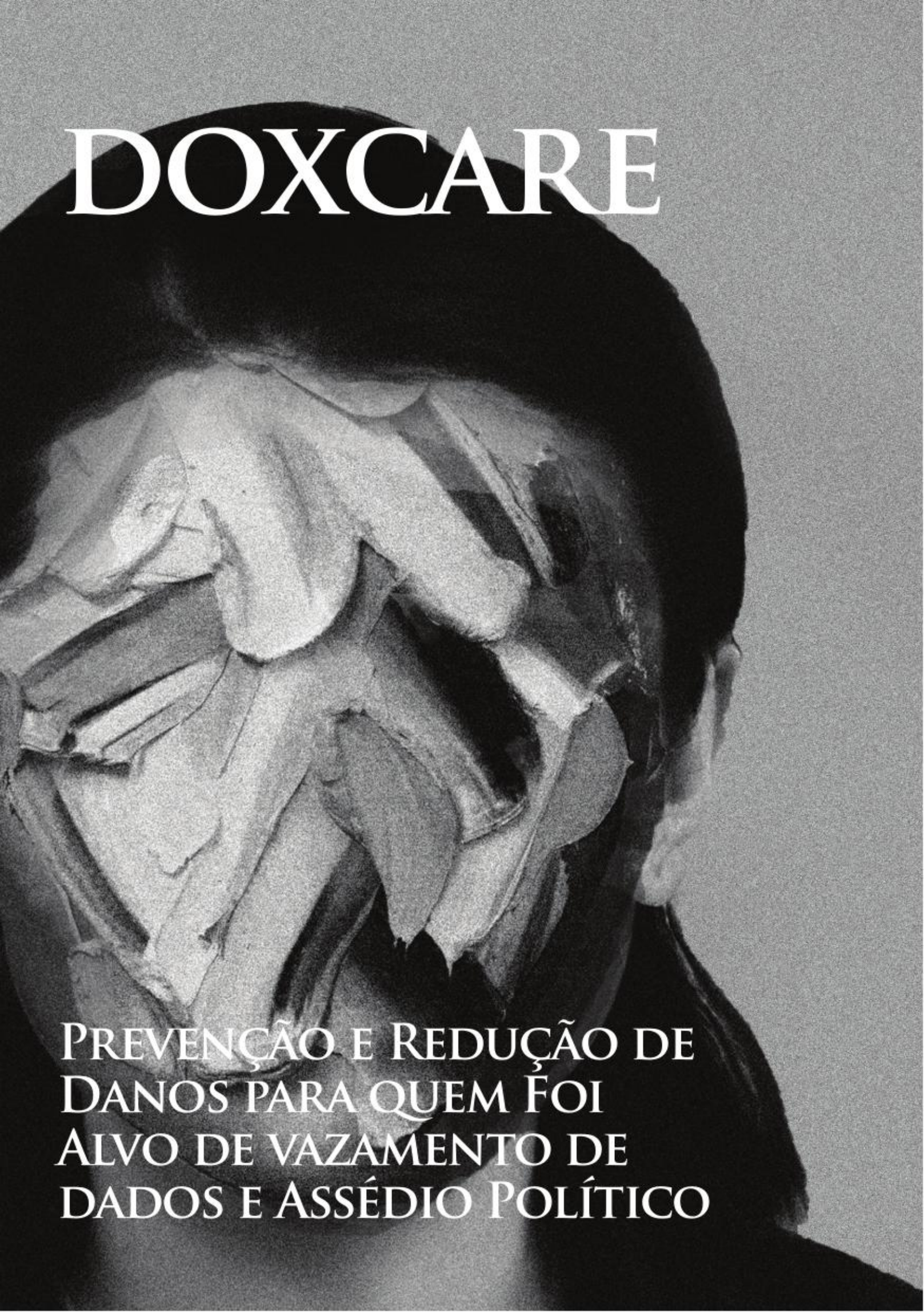

DOXCARE

Prevenção e Redução de Danos para quem Foi Alvo de vazamento de dados e Assédio Político

Este artigo está disponível em

www.cwc.im/antidoxx20

Visite para ter acesso aos links e recursos mencionados neste zine.

Entre julho e agosto de 2020, voltou a circular nas mídias sociais um documento de quase mil páginas com dados de milhares de pessoas supostamente ligadas ao antifascismo em todo o Brasil. O chamado "Dossiê Antifa" não é novidade, é uma versão da que circulou em 2019 com quase mil nomes. Dessa vez, ela foi ampliada e tem dados pessoais, fotos e endereços de quase 3 mil pessoas. Basicamente, o levantamento consiste em reunir informações sobre pessoas que compartilharam fotos, mensagens ou qualquer conteúdo que indique uma posição contrária ao fascismo ou outras ideologias de extrema direita. Nesse contexto e, avaliando o conteúdo em si, é possível tirar duas conclusões, sendo uma boa e outra nem tanto. A boa é que não se trata um serviço de "inteligência fascista" eficiente de fato, que mapeia a atividade de pessoas ou grupos organizados para combatê-los. Ao reunir dados de pessoas que expressaram sua opinião na internet, eles não desvendaram nem mapearam nada além de informações que as pessoas compartilharam em filtros das fotos de perfil ou postagens públicas. A má notícia é que essa é uma tática suja de intimidação e muitas dessas pessoas já estão sendo assediadas e sofrendo em saber que dados sensíveis sobre sua vida estão disponíveis para qualquer um na internet. Mesmo assim, é possível buscar formas de contornar essa situação, reparar os danos e, principalmente, evitar que novos casos de exposição e assédio aconteçam.

***

Tenho sido ativa em minha comunidade há anos. Não muito tempo atrás, trolls de extrema direita acharam contas de rede social de minhas amigas e amigos, família e local de trabalho. Eles me stalkearam e usaram as fotos que encontram de mim e membros de minha família para montar linhas do tempo da minha vida e mapear minhas redes sociais. Por conta de meus valores anti-racistas, usaram essa informação que juntaram para ameaçar a mim, minha família e pessoas minhas amigas. Em cada email de assédio e cada comentário de rede social, eles caracterizavam os projetos que eu participava como "grupos terroristas", me descrevendo como uma "líder" e membro de uma imaginária "máfia obscura de esquerdistas violentos" a qual eles querem "fazer algo sério quanto a isso". Quer essas conclusões sejam apenas trabalho investigativo duvidoso ou declarações falsas desonestas e intencionais, o comportamento deles deve preocupar qualquer pessoa que acredita em se posicionar contra opressões.

Eu desativei minhas mídias sociais quando entendi que isso estava em andamento – não porque eu tenho vergonha de ser associada com a luta por um mundo mais livre, mas porque eu quero proteger minhas amizades e redes de relacionamento. Qualquer pessoa que me conheça sabe que não é nenhum segredo que eu me oponho a todas as formas de intolerância e opressão. Eles não me tomaram como alvo especificamente por alguma coisa em particular que eu fiz, mas porque que eles são opostos a todo ativismo anti-racista, feminista e LGBTQIA+ e eles pensam que podem nos isolar e intimidar uma por uma. Esse é o motivo pelo qual precisamos permanecer juntas.

Quero que você saiba sobre esse caso se você alguma vez se encontrar na mesma situação. Você não está sozinha. Eu espero que isso lhe dê coragem para pensar seriamente sobre sua segurança pessoal online, e também sobre a segurança de seus familiares e suas amizades.

Robert Bowers, o atirador da sinagoga de Pittsburgh, conversou em um chat público com trolls da "nova direita" que fizeram doxxing de antirracistas. A campanha de perseguição contra mim mostra que eles estão dispostos a inventar mentiras para colocar as pessoas na mira dessas armas. A única maneira de nos proteger é seguirmos visíveis e nos apoiando. Não devemos permitir que eles nos intimidem.

O QUE É DOXXING

Doxxing significa catalogar e publicar as informações pessoais de alguém com a intenção de expor e intimidar a pessoa. Isso pode resultar em danos físicos, emocionais e econômicos para quem foi alvo. Tem a intenção de dissuadir o alvo para que não realize alguma ação, assim como envergonhá-lo por suas ideias e valores. É importante levar segurança a sério antes de você ter sofrido doxxing – antes mesmo de você ter motivos para temer que possa sofrer doxxing. Frequentemente, quem faz doxxing vai esperar até eles terem juntado muita informação antes de divulgá-las. É possível que você já esteja sendo observada e perseguida, "stalkeada" e não vai descobrir até ser tarde demais.

Quer você seja uma ativista publicamente muito conhecida ou quase nada envolvida, você deve proteger suas redes sociais e outras esferas de sua vida – mesmo que você ache que não está fazendo nada que vai chamar atenção. Manter boas práticas de segurança protege suas amizades, sua família e sua comunidade. É comum que pessoas sejam incluidas em teorias da conspiração da direita sobre "membros Antifa" apenas porque elas são queer ou trans, "parece esquerdista", toquem em bandas, compareçam a um evento ou frequentem espaços radicais. A informação não precisa ser correta ou justificada para alguém tomar você como alvo. Tudo que um assediador precisa é um pedaço de informação para começar a procurar mais detalhes online.

Estar ciente de quais rastros de informação você deixa online pode proteger você tanto das autoridades bem como de perseguidores stalkers. Agora que a vigilância imposta pelo Estado está cada vez mais sofisticada e transmissões ao vivo se tornaram normais em manifestações, o simples uso de uma máscara muitas vezes não é suficiente. Em Junho de 2020 na Filadélfia, investigadores identificaram uma mulher começando com nada mais que apenas uma foto borrada dela. Eles seguiram um rastro de migalhas incluindo uma compra online no site Etsy, contas do twitter e sua página profissional de trabalho. A polícia de alfândega e de fronteiras começou a passar um pente fino em mídias sociais públicas. Tornar mais segura sua presença online pode fazer você se sentir mais segura ao agir offline.

Uma Grama de Prevenção Vale mais que Um Kilo de Cura

Não há nenhum momento melhor para começar do que agora. Depois de você ter sofrido doxxing, você pode não ser capaz de eliminar a informação que está lá fora mesmo que você tente que ela seja retirada do ar.

Existem muitas maneiras diferentes de lidar com isso. Obviamente, a melhor maneira de garantir que ninguém possa descobrir nenhuma informação sobre você é não ter nada disponível – mas algumas pessoas simplesmente não podem eliminar suas presenças online, seja por conta de trabalho, família ou outras responsabilidades. Em alguns casos, existem razões estratégicas para manter alguma espécie de persona online; por exemplo, ter uma mídia social de longa data, que passe confiança mas seja inofensiva pode ajudar pessoas estrangeiras a cruzarem a fronteira para entrar nos EUA. Felizmente, existem formas de criar barreiras entre esferas distintas de sua vida, manter um perfil público se você precisa de um e adotar práticas que podem ajudar você e suas amigas a se sentir empoderadas para continuar agindo em sua comunidade. Esse processo pode ser entediante. Vai tomar tempo e energia. Eu recomendo que você o faça junto com pessoas amigas, colegas que dividem a mesma moradia ou membros da sua família… para que seja mais fácil vocês passarem por aspectos mais difíceis ou entendiantes.

Mantendo Esferas Separadas

Se você não pode deletar-se completamente da internet, você ainda pode preservar uma privacidade relativa ao manter esferas distintas de atividade online e limpar contas esquecidas ou que sejam raramente usadas.

É provável que você tenha mais de uma presença online. Isso pode incluir redes sociais, quadro de recados, sites de emprego, contas de email — qualquer coisa que você precise usar um login para entrar. No doxxing, frequentemente a informação é triangulada de muitas fontes diferentes. Uma forma de reduzir a quantidade de informação disponível pra quem faz doxxing é particionar essas esferas para que elas não estejam conectadas umas às outras. Isso é um processo altamente individualizado; tome um tempo para considerar as seguintes questões e mapear as suas próprias esferas online.

Você passa seu tempo em fóruns de internet ou no mural de contatos no Facebook debatendo? Você frequentemente curte ou reposta status de contas radicais no Instagram ou Twitter? Você tem fotos ou informações pessoais em páginas de trabalho? Você compra coisas em sites na internet? Alguma pessoa amiga posta fotos suas nas contas delas no Instagram? Você precisa se promover online por conta da sua carreira ou tipo de trabalho que exerce? Você se conecta com colegas de trabalho, familiares e amigas ativistas usando a mesma conta? Você usa partes do seu nome verdadeiro ou aniversário para nomes de usuário ou emails?

Cada uma dessas situações pode não ser um problema em si mesmo, mas juntas elas podem criar links entre diferentes esferas a sua vida.

Pergunte-se:

- O quão separadas são cada uma dessas contas/identidades?
- O que é público? O que é privado?
- O que público e privado significam no contexto de cada site
- O que se consegue achar ao pesquisar seu nome?
- Você usa o mesmo nome de usuário ou email para diversas contas? Essas se cruzam em esferas distintas da sua vida? Tome um tempo para pensar sobre a maneira pela qual todas essas esferas se sobrepõem offline.
- O seu trabalho lhe permite ser aberta quanto às suas políticas?
- O quão público é o seu ativismo? Você fala com jornalistas? Você trabalha em um centro social ou infoshop?
- Você filtra algum ou todo o conteúdo de suas mídias sociais que seus parentes podem ter acesso?
- Existe alguma referência a atividades ilegais ou controversas em um determinado perfil?

Aqui estão alguns exemplos de como sua presença online pode se sobrepor entre diferentes sites:

PARENTES Quão aberta é a relação entre você e seus parentes de sangue/legais? Se uma pessoa estranha tivesse informação de apenas uma pessoa dessa rede, o que ela poderia descobrir sobre as demais?

POLÍTICA Você discute ou posta sobre seus valores políticos online? Caso sim, em quais plataformas?

AMIZADES E COMUNIDADE Se você tem mídia social, quem são suas amigas? As pessoas que te seguem? De que maneiras suas comunidades online refletem suas comunidades na vida real?

HOBBIES Quais hobbies você tem? Você tem amigas e comunidade a partir deles? Você faz parte de alguma comunidade na internet dedicada à essas atividades?

LEGAL Quem é você no papel? Quais nomes, números de telefone e endereços você está ligada? Alguma de suas contas inclui esse tipo de informação? Algum outro site faz isso (provavelmente sem a sua permissão)?

CARREIRA O seu trabalho envolve uma presença online, em sites ou em mídias sociais? Existiria algum problema se a sua política se sobrepusesse à sua carreira? Ou sua carrerira de alguma maneira é ligada à sua identidade política?

Tome um tempo para considerar essa sobreposição, quais são seus objetivos online e onde você pode separar essas duas esferas..

Tácticas

Vamos falar sobre como descobrir quais informações estão disponíveis sobre você, como identificar e eliminar rastros e quais recursos online existem para removê-las.

Comece com o que está disponível publicamente. Busque no Google mesmo e faça uma lista de todas as suas contas de mídia social. Exclua contas antigas de coisas que você não usa mais. Este também é um bom momento para baixar um gerenciador de senhas como o LastPass ou KeePass para te ajudar a gerenciar nomes de usuário, e-mails e senhas exclusivos e seguros..

Delete sites de Rastreadores/Corretores de Dados

Descubra quais informações as pessoas podem descobrir sobre você simplesmente usando um mecanismo de pesquisa. Pesquise você mesmo no DuckDuckGo e no Google. Tente fazer esta pesquisa no modo de nave-

gação anônima. Experimente diferentes versões do seu nome, com e sem o nome do meio e entre aspas. Você pode configurar os Alertas do Google para enviar e-mails quando seu nome for publicado na internet. Isso lhe dará uma noção de quantos dados sobre você estão disponíveis online para pessoas que não estão em sua rede.

Após esta pesquisa inicial, dê uma olhada em todos os sites compiladores de dados (corretores de dados/data brokers) que lucram com a negociação de dados pessoais. Aconselhamos remover também seus familiares mais próximos desses bancos de dados. Este processo pode ser árduo; esses sites tentam dificultar ao máximo a exclusão de informações sobre você. Existem algumas coisas das quais você não pode remover quando quiser, por exemplo, se você passou uma conta de água para seu nome ou se registrou recentemente para votar e ainda vive no mesmo endereço (este é outro motivo pelo qual algumas pessoas optam por não votar).

Os sites de host mais trafegados incluem: Been-Verified, CheckPeople, Instant Checkmate, Intelius, PeekYou, PeopleFinders, PeopleSmart, Pipl, PrivateEye, PublicRecords360, Radaris, Spokeo, USA People Search, TruthFinder.com, Nuwber, OneRep e FamilyTreeNow. Recomendamos começar com eles pesquisando cada um neste site, que contém um guia para desativar praticamente todos os corretores de dados. Se você tem mais dinheiro do que tempo, pode pagar por um serviço chamado Just Delete Me para que suas informações sejam removidas, mas geralmente só recomendo esse serviço se você já tiver sido alvo de doxxing..

delete contas antigas

Quando você pesquisa seu nome em uma ferramenta de busca online, também pode encontrar contas antigas. Pode ser bom fazer uma pesquisa reversa usando todos os nomes de usuário e apelidos (nicknames) antigos de que você se lembrar. Contas que você não usa há muito tempo podem ser uma vulnerabilidade porque, se tiverem usando uma senha mais antiga, alguém pode tentar o suporte técnico dessa conta para obter mais dados sobre você e tentar usá-los para acessar outras contas. Baixe qualquer material de valor sentimental para você e feche permanentemente todas as contas que você não usa mais. Elas podem estar cheias de pistas sobre sua vida.

Primeiro, visite o site **namechk.com**, que busca centenas de plataformas por nomes de usuário específicos e pesquise todos os nomes de usuário

e e-mails possíveis que você usou. Isso lhe dirá quais plataformas têm contas usando esse identificador.

Em seguida, entre neste outro site **backgroundchecks.org/justdeleteme** e digite o domínio do site. Este site arquiva uma grande variedade de páginas existentes, categoriza o quão fácil ou difícil eles tornam a exclusão de uma conta e fornece o link para a página "excluir perfil" para cada respectivo site.

Haveibeenpwned.com te ajudará a descobrir se há alguma violação de dados envolvendo qualquer conta que você possui. Se houver, tome medidas imediatas para alterar as senhas.

Troque Nomes de Usuária, Endereços de E-mail e Senhas

A maneira mais fácil de alguém encontrar mais informações sobre você é pesquisar seu nome, apelidos e nomes de usuária. Para manter suas esferas de atividade na Internet separadas, sempre use um novo nome de usuário ao criar uma conta. Se você tiver um site profissional para trabalhar e precisar usar seu nome legal, certifique-se de que o e-mail que você usa para essa conta seja usado exclusivamente para esse fim. Pode ser que você precise ter um punhado de contas de e-mail e nomes de usuária. Tenho uma para todas as minhas contas médicas e governamentais, uma para minhas compras online, uma para minha vida política e uma para minhas mídias sociais, outra para sites de namoro e assim por diante. Uso pseudônimos e informações falsas para todos os sites e aplicativos que me representam ou exibem fotos minhas.

Um gerenciador de senhas (chaveiro) é de grande ajuda para isso, pois irá armazenar logins para todas as suas contas. Eu recomendo o LastPass, que você pode baixar para o seu telefone e navegador da web. Pode ser tentador deixar tudo conectado permanentemente, mas sempre certifique-se de sair quando terminar de usá-lo. Primeiro, para que você não esqueça a senha mestra — e também para garantir que mesmo se alguém conseguir acessar seu telefone ou computador, não poderá acessar todos os seus dados pessoais. Aproveite para criar novos e-mails e alterar nomes de usuário para todas as contas que você não vai excluir. Você pode facilmente criar novos e-mails usando Protonmail. Tanto o 1Password quanto o LastPass podem ajudar a gerar senhas aleatórias, que são as mais seguras.

Organize o Que Está Disponível e Altere Suas Configurações de Privacidades

Depois de eliminar todas as pontas soltas, observe o que você escolheu manter e o que pode ser encontrado lá. Se você mantém alguma conta de mídia social, vá até seu perfil e observe o que as pessoas podem descobrir sobre você. Você pode escolher entre uma variedade de estratégias sobre como abordar isso, dependendo de quão cauteloso você deseja ser e quão certo está de que é possível manter distintas as suas diferentes esferas de atividade na Internet.

Algumas de suas opções incluem:

- Excluir todas as fotos do seu rosto, de seus animais de estimação, de seu carro, de sua caixa de correio, de tatuagens e de qualquer coisa que inclua informações de identificação desnecessárias — especialmente sua foto de perfil público.
- Eliminar ou falsificar quaisquer dados pessoais em seu perfil — forneça um aniversário incorreto ou nenhum aniversário, escolha respostas aleatórias para sua cidade natal, escolas que você frequentou e outras informações.
- Excluir seguidores e "amizades" duvidosas. Se você alterar todas as suas configurações de mídia social para privadas e se sentir confiante sobre sua lista de seguidores, pode haver menos razão para esconder seu rosto. Ainda recomendo manter os detalhes sobre sua localização e vida pessoal íntima offline. Lembre-se de que sua segurança é determinada por quão seguras são as pessoas com quem você se relaciona. Se você optar por ser mais público, mantenha suas amizades e familiares separados, não poste fotos das pessoas ou de suas informações pessoais sem seu consentimento explícito e lembre-se de que as conexões sociais são visíveis por meio de redes sociais e sites de coleta de dados.

The Coach, ou "O Guia" da Crash Override Network é um guia passo a passo útil que o vincula diretamente à página de configurações de privacidade de muitas redes sociais comumente usadas. Clique em "Let's Get Started"("Vamos começar") e "Strengthen the security of my online accounts…"("Fortaleça a segurança de minhas contas online para que as pessoas não possam invadi-las tão facilmente") e siga seus guias para todas as principais empresas de mídia social. Este guia também pode ajudar com outros

aspectos da segurança online, então, depois que você fizer isso, recomendo terminar o auxiliar do Guia e verificar quais outros recursos eles oferecem.

Quando você achar que acabou, peça a um amigo que tente criar um perfil com base nas informações que ele pode encontrar sobre você enquanto finge ser um "doxxer" para ver se alguma coisa em que você não pensou escapou pelas rachaduras. Pode ser importante verificar periodicamente o que pode ser encontrado pesquisando seu nome a cada dois meses ou algo do tipo, por exemplo.

Se Você foi Alvo de Doxxing

Não recomendamos acionar a polícia quando você sofrer doxxing (ou em qualquer outro caso). A polícia pode usar as informações que você fornece sobre os assediadores, mas também usará as informações que obtiverem sobre você e outros indivíduos e grupos aos quais você possa ter estado publicamente associado. Uma vez arquivado, tudo isso está permanentemente nas mãos deles e não há garantia de que não usarão isso contra você ou outras pessoas através da repressão estatal.

Se você decidiu envolver a polícia, por favor, seja transparente e não peça a nenhum grupo radical para te apoiar. Certifique-se de informar todos os grupos com os quais você está conectado sobre sua decisão. Normalmente, a polícia não fará nada ou tornará a situação muito pior. A ideia deste guia é fornecer alternativas baseadas no empoderamento e apoio comunitário.

Devo tornar isso público?

Resposta curta: Não reaja de forma pública imediatamente. Tome um tempo para se proteger e alertar suas redes de uma maneira privada antes de reagir publicamente.

O seu primeiro impulso pode ser de alertar o máximo de pessoas que você conseguir de forma imediata com uma declaração pública ou desativar tudo. Ir a público dessa forma pode lhe proporcionar um apoio imediato se você tem uma audiência que é simpática, mas carrega o risco de maior agressão por parte dos assediadores. Existem bons argumentos para ser cuidadosa com informação no começo. A coisa mais importante a fazer primeiro é tomar medidas para proteger você e suas redes contra novos danos.

Declarações imediatas podem atrapalhar seus esforços de segurança. Caso a informação postada sobre você seja exata ou não, provavelmente ninguém irá usá-la para causar algum dano sério a você sem antes confirmar ao menos parte dela. Postar em contas de rede social sobre ter sofrido doxxing imediatamente confirma que a informação sobre você é exata; isso também sugere que você viu onde ela foi postada e está apavorada. Isso atua no mesmo sentido do objetivo de seus assediadores. Eles querem intimidar e isolar você. Não confirme ou negue qualquer das informações que eles desenterraram sobre você, não importa se ela é falsa ou constrangedora. Eles estão procurando uma reação. Se você os deixar sabendo que a informação que eles postaram é incorreta, eles podem concluir que estão no caminho certo e apenas precisam continuar cavando. Algumas vezes, uma das respostas públicas mais efetivas é nenhuma reposta sequer — não faça nenhuma mudança grande dos seus hábitos de postagem ou mostre qualquer medo. Isso pode passar a mensagem de que a pessoa que fez o doxxing em você errou e que o ataque foi um fracasso.

Depois de você ter tido tempo para processar seus sentimentos e garantir sua posição, pode ser estratégico ir a público e talvez se juntar com outras pessoas que estão na mesma situação. Vocês podem ser capazes de alavancar a indignação pública em relação à racistas e fascistas de modo a criar uma campanha para dissuadir novos doxxings — por exemplo, fazer um projeto de financiamento com promessas de doação de dinheiro para cada e-mail assediador que você ou outras pessoas em sua comunidade recebem! Uma vez que seus assediadores querem te isolar do apoio público como esse pode dissuadir novas intimidações. Tente ser criativa, resiliente e estratégica. Tome cuidado para não por em perigo qualquer outra pessoa nesse processo.

Ao fazer declarações públicas, se você se posiciona ou se vangloria sobre suas habilidades, sua capacidade de empregar violência, armas com as quais você pode se defender ou exagerar em sua ferocidade, você pode estar mordendo mais do que consegue mastigar. Geralmente não é uma boa ideia dar uma impressão falsa sobre si. Falar diretamente ou indiretamente com o assediador não costuma melhorar a situação. Recomendo fazer uma declaração postitiva afirmando sua ética e valores, descrevendo sobre como a sua identidade e seus ideais serviram para que você fosse tomada como alvo mas mantendo que enquanto essas campanhas de assédio tem como objetivo fazer você se acovardar, você não vai fazer isso, porque não tem nenhum motivo para esconder sua política. Evite falar sobre ações específicas ou grupos, caso você esteja envolvida com elas ou não.

Imediatamente Depois de Ter Sofrido Doxxing

1. **Não entre em pânico.** Chame uma pessoa amiga e próxima para te encontrar e te ajudar.
2. **Crie um diário de acontecimentos.** Mantenha registros tanto de provocações online quanto offline. Isso é crucial para identificar os padrões dos ataques. Pode ser útil comparar isso com outras organizadoras de modo a identificar padrões mais amplos com fins de identificar seus oponentes e suas organizações.
3. **Avise suas amizades, família e redes políticas sensíveis de uma maneira privada.** Deixe alguns amigos que você pode confiar com suas informações pessoais encarregados para ajudar a relatar postagens em blogs e redes sociais que estão catalogando e identificando você, classificando elas como assédio. Faça isso repetidamente. Algumas plataformas carecem de polítias que vão te proteger, mesmo se essas postagens incluem informações pessoais exatas, mesmo se elas te colocam em perigo. Algumas vezes quem faz doxxing usará suas fotos e informações pessoais para fazer contas falsas. Geralmente é mais fácil denunciá-las como falsas; tente fazer isso rapidamente a fim de prevenir que eles possam obter mais informação de suas redes ao se passarem como se fossem você. Você, sua família e seu chefe no trabalho podem começar a receber ameaças ou ligações de assédio. Deixe-os a par do que está acontecendo tão rapidamente quanto conseguir e instrua-os a não interagir com os assediadores.
4. **Corte o fluxo de informação.** Se você está lendo essa sessão e não executou a sessão de cuidados preventivos, comece esse processo. Baixe um gerenciador de senhas como o 1Password ou o LastPass e mude todas as suas senhas imediatamente. Você também pode pagar por um serviço chamado Delete Me que tirará grande parte de seus rastros online dos sites espiões que coletam e exibem sua informação pessoal. Esse serviço vai cuidar da informação agregada a partir dos corretores de dados mas não de qualquer mídia social, contas de internet, artigos novos ou registros jurídicos que você possa ter: esses você terá que tratar por você mesma. É importante tentar balancear a hemorragia de informação também enquanto não alerta aos seus assediadores que o dox foi eficaz ou "acertou no alvo". Tente escorar suas contas de mídia social fazendo listas de amizades e tornando as

informações privadas de modo a proteger suas redes até você ter certeza de que elas não oferecem informações pessoais vulneráveis para aqueles que estão querendo levantá-las. A forma como você reage publicamente é uma situação muito delicada e deve ser tratada cuidadosamente durante todo este processo.

5. **Elabore um plano de proteção.** Recrute pessoas amigas e família para lhe dar apoio. Informe-as sobre o que está acontecendo; doxxing pode ser traumático e você precisa priorizar sua saúde mental e física para que você consiga superar esses ataques. Essas conversas podem ser difíceis — especialmente se elas não ententem as nuances desse momento político, se é a primeira vez que estão ouvindo falar sobre um tipo de grupo de ódio específico, ou se suas relações são manchadas por diferenças políticas ou pessoais. Se você não se sentir em condições, pode pedir a alguma amizade que tenha um bom entendimento da situação para realizar as conversas mais difíceis por você.

Se o seu endereço estiver incluido no doxx, ache algum lugar novo que você possa ficar, se for possível para você. Se você não pode sair de casa, convide pessoas amigas ou um grupo de segurança local para ficar com você. Monte uma mochila do tipo "pronta para sair" com tudo que você precisa se você tiver que fazer as malas e sair sem chamar muita atenção..

Avaliando Ameaças

Se você acha que não está correndo um grande risco, especialmente se o seu vazamento de dados é composto de informações disponíveis abertamente ou está apenas sendo enviado para você para causar nervosismo, você pode se sentir bem descartando isso como uma tática de intimidação barata, bloquear e denunciar o assediador e seguir em frente. Pode ser apenas alguém tentando te irritar. No entanto, se o seus dados vazados incluem informações pessoais confidenciais, especialmente detalhes que não são fáceis de obter com um simples trabalho de detetive, ou aparece em um fórum público onde as pessoas distribuem informações na esperança de que outras pessoas ajam sobre ele, você pode querer tomar mais precauções. Isso é especialmente verdadeiro se você já faz parte de um grupo ou população alvos.

Quando você souber que teve dados vazados em um doxxing, é importante estabelecer quais informações podem se tornar ameaças reais. Frequentemente, doxxing é um precursor de assédio offline mais intrusivo ou

está conectado a ameaças para agir com base nas informações. Isso pode ser qualquer coisa, desde ligações ameaçadoras para a família ou locais de trabalho até ameaças de morte pontuais ou uma ligação da polícia.

Algumas vezes é difícil determinar o que faz uma ameça ser "real". A tática mais comum de quem faz doxxing normalmente é mandar mensagens para assustar ou intimidar em qualquer lugar onde eles pensam que podem alcançar você — redes sociais, email e familiares… coisas desse tipo. Frequentemente eles vão insinuar que tem mais informação do que realmente possuem; é comum dizerem que forneceram essas informações às autoridades da lei locais; frequentemente, toda informação que postaram publicamente é tudo o que eles possuem.

Seu patrão pode receber ligações demandando que te demitam. Até o momento, é raro que alvos de doxxing tenham sido fisicamente atacadas, mas já aconteceu. E é possível que aqueles que fizeram o doxx se esforcem para que seus dados caiam nas mãos de pessoas que não estão agindo de forma racional ou ética. É importante ser cautelosa, mas não entre em pânico ou se deixe mergulhar na ansiedade..

Pergunte-se:

- As informações estão corretas? Eles tem o endereço da sua casa, trabalho ou família? Eles sabem dos lugares que você frequenta? Sabem quem são suas amigas?
- Você corre o risco de perder seu trabalho se descobrirem qualquer uma dessas informações sobre você?
- Você sabe onde vivem seus assediadores? Eles estão próximos de sua comunidade física ou são apenas trolls em um fórum descentralizado? Você tem algum motivo para acreditar que as autoridades estarão interessadas nessas informações? Esses dados estão sendo compartilhados a partir de fontes locais de notícias da direita, colocando o seu rosto na frente de uma multidão de estranhos hostis que agora possuem suas informações?
- Eles possuem fotos suas privadas ou constrangedoras?
- Há alguma informação ligando você à atividades consideradas crimes que poderia fazer com que você seja presa?

Soluções

Aqui estão algumas coisas que você pode fazer em resposta aos perigos que podem sugir após ter sofrido doxxing:

- Criar um plano de auto-defesa, se inscrever em aulas de auto-defesa, entrar em contato com um grupo de defesa comunitário local.
- Informar as pessoas e grupos que foram nomeados no doxx — local de trabalho, camaradas, pessoas que você divide moradia, família..
- Converse sobre seus medos com pessoas que você confia..
- Entre em contato com pessoas que passaram por isso antes para buscar conselhos.
- Providencie ter uma advogada disponível no caso de você estar preocupada que a informação sobre você possa ser de interesse de agentes do Estado.
- Conecte-se com um grupo antifascista local — eles podem ser capazes de ajudar na identificação dos assediadores e de quem fez o doxxing, caso estejam postando a partir de uma conta falsa

Conversando no Trabalho e em Família

Essa conversa pode ser bem difícil, especialmente se o seu relacionamento com sua família é tenso. Tenha uma pessoa amiga de plantão com a cabeça fria para ajudar a mediar ou apoiar você depois, se necessário.

Pense com que frequência você está disposta a ser vulnerável com sua família e quantas oportunidades você terá, no futuro, para continuar com a conversa. Se for necessário falar com membros da família mas você sente que só terá uma chance, você pode ensaiar com uma amiga e se preparar para suas reações. Se você tem um relacionamento com a sua família que seja estável, aberto à conversas e de confiança, você pode explicar a situação para elas em uma série de conversas menores, no lugar de uma única longa conversa. Avalie o quanto de tempo e atenção você vai ter.

Para pessoas com as quais não quero ter uma conversa política, sempre me ajudou definir isso como "ter um assediador/stalker" — isso pode ser suficiente para explicar a gravidade da situação e porquê você precisa de privacidade. Mas pode valer a pena o esforço para ser honesto sobre o que está acontecendo. Isso pode ajudar a construir relações mais fortes e desmistificar essa ocorrência comum, enquanto encoraja outras pessoas (que podem achar que isso não aconteceria com elas ou com alguém que elas conhecem) a levarem a privacidade online a sério. A maioria das pessoas vai responder com

medo e simpatia, ainda que algumas vezes elas venham a sugerir ou mesmo insistir para você ligar para a polícia.

Não existe uma abordagem única que sirva para todos as situações. No meu caso, tive que exigir que minha mãe conservadora prometesse não envolver a polícia. O fiz apelando ao meu direito à segurança pessoal e à minha autonomia enquanto vítima da situação, pedindo a ela que respeitasse meus desejos e lembrando que a polícia não poderia fazer muita coisa em relação a assédios direcionados desse tipo — e ligar para a polícia apenas faria seria me tornar alvo deles, uma vez que eu estava sendo acusada de uma atividade criminosa. Essas conversas podem ser bem difíceis, mas muitas vezes são necessárias. Lembre seus amigos e familiares de não reagir ou responder a nenhuma ligação telefônica, email ou solicitações em mídias sociais.

Você pode ler um guia de como discutir isso com seu patrão no artigo online.

Coisas para lembrar quando estiver conversando com suas amigas e família

- O objetivo dos assediadores é tensionar seus relacionamentos e arruinar sua vida. Não deixe que eles consigam fazer isso. Fale para sua família que a melhor maneira de te apoiar é recusar cair na tática deles.
- Não jogue anarquistas e antifascistas na fogueira para que você seja salva; não alegue que você está sendo atacada sem motivo. Isso não vai te ajudar se aparecerem motivos — e vai apenas deslegitimar e colocar ainda mais em perigo aquelas que não conseguem se distanciar de políticas anarquistas.
- Não deixe ninguém te culpar pelo que está acontecendo, seja pela política em que você se engaja ou por sua irresponsabilidade em se colocar "nesta situação". Lutar por um mundo melhor envolve desafios.
- Sugira maneiras concretas de ajudá-los a entender a situação e a se protegerem. Mande esse artigo ou uma lista de referência para eles; ofereça-se para ajudá-los a fechar suas mídias sociais se eles não forem muito entendidos de tecnologia.
- Converse sobre o que eles podem ficar preparardos — ligações de assédio, emails, talvez vizinhos recebam mensagens sobre você. Prepare-os para o pior cenário possível, mas enfatize que é improvável.
- Seja claro quanto ao que você precisa deles.

Vivendo Sua Vida, Seguindo em Frente

Respire fundo. Não se culpe. Emocionalmente, isso pode ser perturbador e disruptivo, adicionando uma camada de estresse agudo em sua vida. Podem existir pessoas lá fora que sabem como você é, e você não tem ideia de quem elas são. Algumas vezes informações de doxxing tornam-se parte permanente da internet se o seu nome for buscado no Goggle; isso pode afetar suas perspectivas de trabalho. Algumas vezes isso não leva a nada, mas alguém pode tentar continuar de onde o último doxxer parou.

Até você ter certeza que a exposição acabou, talvez precise alterar alguns aspectos da sua vida. Pergunte-se: "Que tipo de vida eu quero viver? Como posso lidar com minha ansiedade? Existem maneiras que eu possa assumir ser uma figura mais pública? Pode ser importante tomar medidas de segurança mais rigorosas.

Aqui estão algumas das medidas que você pode escolher para adotar:

- Não deixe quem você não confie te fotografar. Isso pode criar algumas conversas desconfortáveis, especialmente em eventos de família ou em situações profissionais. Esteja ciente de quem aparece em fotos com você; informe-as que aparecer em uma foto com você pode atrair atenção indesejada. Pode ser útil ensaiar as conversas que você talvez precise ter.
- Mantenha registos históricos de todos os assédios que você experenciar.
- Se você se mudar, não atualize seu endereço. Não se registre em lojas ou de seu endereço residencial verdadeiro para instituições que possam indicar onde você mora ou onde é possível te encontrar.
- Use pseudônimos online e pessoalmente, se for necessário. Não use o mesmo constantemente.
- Procure terapia para trabalhar qualquer trauma que você tenha passado.
- Ajude suas amizades e família a compreender a importância da segurança online.
- Tenha conversas francas com pessoas fora de seus círculos de afinidade política. Você pode se surpreender com o quanto elas expressam empatia.

Não importa o quanto as pessoas que te perseguem tentem fazer você se sentir isolada, você não está nisso sozinha. Enquanto uma comunidade, devemos proteger umas às outras e nossas redes online do assédio, prisões, violência política e intimidação. ***Juntas, podemos fazer isso***.

Não importa o quanto as pessoas que te perseguem tentem fazer você se sentir isolada, você não está nisso sozinha. Enquanto comunidade, devemos proteger umas às outras e nossas redes online contra assédio, prisões, violência política e intimidação.

Juntas, podemos fazer isso.