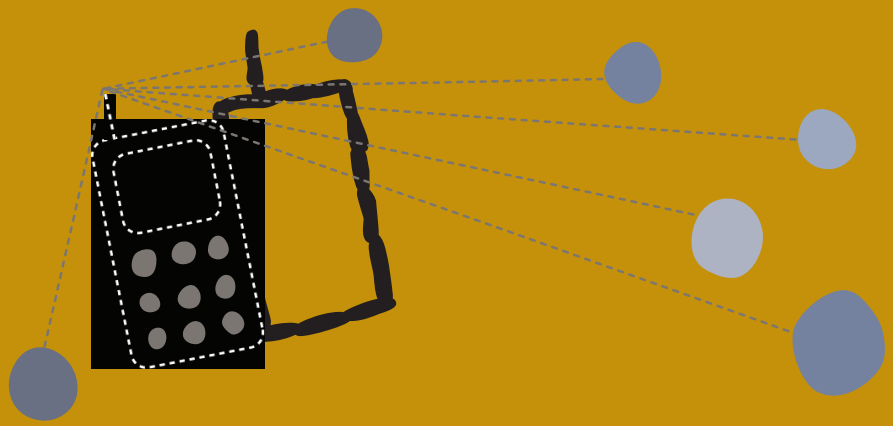
Segurança & Privacidade Online & Móvel



AS NOVAS TECNOLOGIAS, COMO OS TELEFONES MÓVEIS E A INTERNET, SÃO PODEROSAS FERRAMENTAS PARA O ATIVISMO; MAS SEU USO PARA O REPASSE DE INFORMAÇÕES DELICADAS OU SENSÍVEIS PODE CRIAR RISCOS PARA VOCÊ, PARA SEUS CONTATOS, AMIGOS E COLEGAS. ESTE CARTÃO VAI AJUDÁ-LO/A A ACESSAR INFORMAÇÕES DE MANEIRA SEGURA E A PROTEGER SEUS DADOS QUANDO ESTIVER USANDO O TELEFONE CELULAR E A INTERNET.

O QUE É SEGURANÇA E PRIVACIDADE DIGITAL?

Eis alguns sinais de que os direitos de comunicação e a segurança digital possam ter sido comprometidos:

- Senhas que mudam misteriosamente
- Mensagens privadas que parecem ter sido lidas por outra pessoa além do destinatário
- Sites que tenham se tornado inacessíveis a partir de certos países
- Autoridades revelando conhecimento sobre correspondência privada, incluindo datas, nomes ou tópicos discutidos
- Conversas ao telefone celular que as pessoas achem terem sido monitoradas

SERÁ QUE EU PRECISO ME PREOCUPAR COM ISSO?

Se tais situações forem capazes de comprometer seus projetos ou de colocar você ou seus contatos à mercê de perseguição, então você deve se preocupar. O conhecimento e os programas computacionais necessários

para empreender esses ataques contra sua privacidade digital costumam estar disponíveis na própria internet. Se o atacante tiver acesso suficiente à infraestrutura de internet e de telefonia móvel no seu país, a tecnologia necessária é bastante simples. Órgãos governamentais, Provedores de Serviço de Internet (ISPs) e empresas de telefonia móvel têm acesso privilegiado a essa infraestrutura, mas colegas de trabalho, vizinhos e as lojinhas de internet (cyber cafés) também podem ter acesso.

QUAIS SÃO OS PROBLEMAS DE SEGURANÇA COBERTOS NESTE CARTÃO?

Neste cartão são enfatizadas as ferramentas baseadas na internet e os telefones móveis. Entretanto, há muitas outras tecnologias que também podem torná-lo vulnerável a censura, vigilância e perseguição. Embora não sejam discutidas aqui, as precauções básicas mais importantes são: manter regularmente atualizado o sistema operacional do seu computador, os programas de proteção antivírus e os procedimentos de back-up. Se você tiver alguma razão para suspeitar que seus computadores ou dispositivos de armazenamento de dados, inclusive seus back-ups, estejam correndo algum risco de se perderem, de serem roubados ou confiscados, ou de que sua organização possa ser alvo de vigilância através da internet (ou se isso for comum nas regiões em que você atua), então é melhor você consultar a suíte de ferramentas Tactical Tech's Security in-a-Box.

Ferramentas de incidência baseadas na internet

Ao usar ferramentas públicas baseadas na internet, como Blogger, Facebook e Twitter para mobilização ou coordenação de ações, lembre-se de que as informações que você armazena nessas plataformas torna-se, até certo ponto, propriedade das empresas que operam estes serviços e que muitas dessas ferramentas expõem mais informação do que você pensa.

Ao confiar um projeto sensível a empresas operadoras de ferramentas online, não deixe de ler as normas de privacidade ou os contratos com o usuário pertinentes. Lembre-se de que mesmo os regulamentos mais apurados deixam suas informações sob o controle direto dos administradores da plataforma, que podem revelar, vender ou divulgar tais informações por engano sem sua permissão ou conhecimento. Mesmo depois de encerrar sua conta, muitos desses sites não eliminam efetivamente o conteúdo que você postou ou as informações pessoais que você forneceu ao abri-la. Por fim, a menos que seja importante usar um dado serviço comercial em particular, seja pela acessibilidade ou porque isso o ajuda a se mesclar com usuários mais discretos, considere algumas das alternativas mais progressistas: Blip.tv em vez do YouTube; riseup.net em vez do Gmail. Se tiver os recursos técnicos, você pode até administrar seu próprio serviço com base na internet.

Se você usa plataformas comerciais, tome as precauções necessárias para se proteger da malícia daqueles que sabem extrair informações privadas desses serviços. Isso é especialmente válido para plataformas de sites de redes sociais como o Facebook ou o MySpace. Compreenda bem os dispositivos de privacidade embutidos nessas plataformas e considere o tipo de informação que você vai despretensiosamente revelar sobre si mesmo ou sobre sua organização; por exemplo, seu nome verdadeiro, onde mora, os lugares para onde viaja e detalhes dos eventos programados ou encontros marcados. Se essas informações forem monitoradas durante um período prolongado, elas também podem passar um quadro geral dos seus hábitos e práticas de trabalho.

Uma técnica bastante útil é criar várias contas em qualquer desses serviços baseados na internet, permitindo que você use um perfil ou conta diferente para cada projeto e mantenha contas de teste que possa usar para "espiar" a si mesmo. Sua privacidade ficará mais bem protegida se você for capaz de verificar de maneiras diferentes o que é revelado sobre sua conta; por exemplo, através de buscas na internet ou de pessoas que têm privilégios especiais de acesso.

SENHAS

A maioria dos recursos baseados na internet depende de uma única senha para proteger sua conta. Se um indivíduo ou organização mal intencionada descobrir essa senha, independentemente da confiabilidade dos administradores do site ou do cuidado com que os testes de privacidade foram feitos, você perderá imediatamente a confidencialidade e o anonimato. Maneiras menos conhecidas de quebrar uma senha: alguém pode instalar um software mal-intencionado num computador que você use para fazer login num site seguro. Ou pode monitorar sua conexão com ao internet enquanto você faz login num site inseguro.

Para se proteger contra o primeiro tipo de ataque, use seu próprio computador ou um computador mantido por alguém de sua confiança e mantenha atualizado o sistema operacional e os programas de proteção. Para se proteger contra o segundo tipo de ataque, a maioria das plataformas de email, redes sociais, blogs, mapas e vídeo baseadas na internet oferecem conexões seguras, chamadas HTTPS. Você pode verificar se a conexão com uma página na internet é segura quando for "https://" e não apenas "http://" no início da barra de endereços do seu navegador. Muitas das ferramentas baseadas na internet, entretanto, não usam HTTPS para proteger informações além da senha que você usa para acesso ao site. Por causa disso, se alguém monitorar sua conexão por tempo suficiente, vai ficar sabendo o que você armazenou naquele site. A melhor defesa que você tem contra isso é procurar as ferramentas baseadas na internet que usam HTTPS para todas as páginas.

DRIBLANDO A CENSURA

Você pode usar proxies de segurança baseados na internet, ferramentas para contornar a censura ou softwares de anonimato como o Tor para esconder sua identidade dos sites que visita ou para contornar os filtros da internet. Essas ferramentas são úteis quando você precisa acessar sites bloqueados, por exemplo, para pesquisa ou para o envio de atualizações para plataformas baseadas na internet como o Facebook.

O ANONIMATO ONLINE

Os softwares de anonimato como o Tor são úteis quando você não quer revelar quais sites visitou. O Tor ricocheteia sua conexão entre vários computadores voluntários aleatórios de forma a evitar que o seu provedor de internet ou observadores no nível governamental saibam o que você está fazendo na internet. Entretanto, não use o Tor quando estiver enviando ou recebendo informações sensíveis de sites inseguros. A menos que você esteja conectado a um site que suporte HTTPS, um dos computadores voluntários consegue monitorar o conteúdo quando este estiver sendo carregado. O Tor é bastante seguro, mas, por ora, ainda diminui a velocidade da sua conexão com a internet.

Telefones celulares s

Os telefones celulares são usados por militantes no mundo inteiro, mas em geral armazenam uma quantidade imensa de informações que deveriam ser mantidas em privacidade. Além das listas de contato, um telefone celular pode conter históricos de chamadas, calendários, mensagens de texto e emails.

Pense nas informações que você armazena no seu telefone, particularmente pela facilidade com que eles são confiscados. Por exemplo, quem faz um trabalho voltado para a defesa de direitos de natureza sensível provavelmente não precisa manter todos os contatos no celular e, por isso, deve eliminar as informações do aparelho e do SIM card sempre que possível. Ao organizar eventos ou redes de mobilização, é sempre uma boa idéia usar SIM cards pré-pagos, anônimos, e mudar de aparelho de vez em quando. Por ser fácil dar busca e filtrar os SMS, é bom evitar o envio de senhas importantes através de mensagens de texto. Basta que esteja ligado para o seu telefone celular poder ser usado para rastrear onde você se encontra. As pessoas que forem participar de encontros de natureza sensível devem desligar o telefone celular e tirar a bateria antes de começar para só recolocá-la e tornar a ligar o aparelho depois que saírem da reunião. As operadoras de telefonia celular têm acesso a detalhes de toda

chamada: para quem, quando e onde foi feita. Elas podem estar obrigadas por lei a manter esses detalhes, ou a liberá-los se assim requisitadas pelas autoridades, e podem guardar tais registros por vários anos.

ATIVIDADE: IDENTIFICAR OS RISCOS DE SEGURANÇA A QUE VOCÊ ESTÁ SUJEITO

Use as perguntas abaixo para avaliar os riscos de segurança que você corre e para decidir quais ferramentas usar para reduzi-los.

1. **Eu lido com informações sensíveis.** É importante saber se você está lidando com informações de natureza sensível que possam fazer com que outros queiram espreitar suas atividades. Você tem envolvimento com atividades que possam ser consideradas pelo governo, pela polícia, pelo exército ou por alguma empresa privada como sendo de natureza sensível ou prejudicial? Se estiver, você pode estar correndo risco, ou colocando em risco outras pessoas à sua volta, a menos que coloque em prática algumas medidas de segurança.
2. **Eu trabalho com gente cujas identidades e detalhes devem ser mantidos em privacidade.** Talvez você esteja coletando informações das pessoas que apóia, como informações sobre violência doméstica, trabalhos forçados ou estupro. Se as pessoas lhe passam informações que podem colocá-las em risco, você precisa tomar providências para manter a privacidade destas pessoas.
3. **Às vezes eu me comunico online com gente que lida com informações de natureza sensível.** Mesmo que você ache que não corre riscos com segurança, ao se comunicar online com gente que corre tais riscos você também pode ser visado por aqueles que são contra elas. Isso é porque terceiros podem usar você para ter acesso às informações privadas daqueles com quem você tem contato.
4. **Eu visualizo ou divulgo conteúdo em sites que podem ser considerados de natureza sensível.** Talvez você contribua com informações para sites de direitos humanos ou divulgue artigos contrários a grupos que acredita estarem desrespeitando direitos humanos. Uma simples visita na internet a sites de natureza sensível pode fazer de você um alvo.

Recursos de segurança & privacidade na internet

Para aprender mais e baixar ferramentas de seguraça:

1. **Security in-a-box** foi criada pela Tactical Tech e pela Front Line para atender as necessidades de segurança e privacidade dos militantes e defensores dos direitos humanos. http://security.ngoinabox.org
2. **Digital Security and Privacy for Human Rights Defenders** da Front Line fornece informações úteis avaliar e tratar de ameaças digitais. http://bit.ly/1aCkSs (frontlinedefenders.org)
3. **Mobiles in-a-box** da Tactical Tech contém toda uma seção sobre privacidade e segurança da telefonia móvel. http://mobiles.tacticaltech.org/security
4. **Anonymous Blogging with Wordpress & Tor.** A Global Voices criou esse guia em apoio a defensores dos direitos que desejam revelar a verdade e querem se expressar online, mas que, ao fazê-lo, podem se colocar em risco. http://advocacy.globalvoicesonline.org/projects/guide/
5. **Be anonymous online and circumvent censorship.** A Tor foi projetada para aumentar o anonimato das suas atividades na internet e também pode ser usada para contornar os filtros da internet. É possível baixá-la no computador ou rodá-la a partir de um pen drive (USB). http://www.torproiect.org