OSINT: DICAS DE SEGURANÇA ONLINE

*Por Fanny Tan**

Nmedia/Adobe Stock.

Antes de se aventurar com atividades OSINT, é essencial seguir algumas regras para fortalecer sua segurança online.

Em OSINT (*open source intelligence*, inteligência de fontes abertas), a segurança operacional (OPSEC, *operational security*) envolve o desenvolvimento e a adoção de um processo para proteger nossa identidade online. Não é um mero detalhe desnecessário; pelo contrário, é um passo crucial que deve ser dado antes de iniciar qualquer investigação de código aberto.

Ocultar os nossos rastos durante uma investigação OSINT é essencial para garantir que, do ponto de vista das pessoas que visamos, permanecemos anônimos. Isto não só as impede de alterar seu comportamento de qualquer forma, mas também nos protege de potenciais ameaças representadas pelas pessoas e organizações visadas pela nossa investigação.

Aqui estão algumas dicas para praticantes de OSINT amadores que desejam iniciar suas primeiras investigações e manter-se seguros online.

SEMPRE COMPARTIMENTALIZE

Trabalhar em um ambiente exclusivamente OSINT é uma excelente etapa antes de iniciar qualquer investigação de código aberto. Nossos dispositivos e contas

pessoais contêm uma variedade de informações que podem vazar durante nossas investigações online, fornecendo pistas que os alvos podem usar para nos rastrear. Separar nossas vidas pessoais de nossas atividades OSINT evita qualquer contaminação cruzada e elimina o risco de indivíduos ou organizações visadas nos identificarem.

Se você não tiver um segundo computador específico para trabalhar em suas investigações, deverá criar e trabalhar a partir de uma conta separada de não-administrador em seu computador para obter essa camada extra de proteção. Você também pode trabalhar a partir de uma máquina virtual instalada em seu computador, principalmente se sua pesquisa ocorrer em ambientes online mais obscuros e menos moderados, como a *dark web*.

CRIE CONTAS FALSAS (E MANTENHA-AS ATIVAS)

Quando se trata de coletar informações das redes sociais, é essencial não usar as suas próprias contas pessoais. Alguns sites de mídia social (LinkedIn, por exemplo) notificam os usuários quando alguém visita seu perfil. Isso pode revelar parcial ou totalmente a identidade do pesquisador.

Ao usar contas falsas, você reduz o risco de erros inadvertidos, como revelar acidentalmente a sua verdadeira identidade ao reagir com um "Curtir" a uma postagem online.

Existem várias ferramentas gratuitas para aumentar a credibilidade de suas contas-fantoches. Por exemplo, o site Fake Name Generator permite gerar rapidamente nomes e sobrenomes, enquanto o This Person Does Not Exist gera fotos realistas de rostos inexistentes que podemos usar como fotos de perfil para nossas contas online falsas.

USE UMA REDE PRIVADA VIRTUAL (VPN)

Os administradores de sites podem rastrear facilmente o endereço IP de um pesquisador que visitou sua plataforma. Para permanecer anônimo enquanto navega, é melhor usar uma VPN (*Virtual Private Network*), que oculta seu endereço IP e, portanto, sua identidade. Existem muitas soluções VPN disponíveis, portanto, leia com atenção os termos de uso e escolha a VPN mais segura possível.

UTILIZE AS FERRAMENTAS DISPONÍVEIS

Uma ampla gama de ferramentas – a maioria delas gratuitas – está disponível para nos ajudar a pesquisar diferentes redes sociais simultaneamente, identificar usuários de fóruns obscuros ou acessar diversas bases de dados. Mas como escolher essas ferramentas com sabedoria e evitar surpresas desagradáveis?

Não existem atalhos para garantir que estamos equipados com ferramentas que realmente nos ajudarão em nossas investigações: investir tempo em pesquisá-las é fundamental. Recomendamos visitar fóruns e outros sites criados especificamente para pesquisadores OSINT, como o canal Discord do Bellingcat,

onde profissionais e entusiastas OSINT compartilham dicas e truques para otimizar as ferramentas disponíveis para a comunidade.

NUNCA TRABALHE SEM UM MODELO DE AMEAÇA

Por último, o nível de proteção de que necessitamos varia de acordo com o tipo de investigação que realizamos. Por exemplo, a pesquisa GEOINT (*geospatial intelligence*, inteligência de geolocalização) exigirá menos precauções do que a SOCMINT (*social media intelligence*, inteligência de mídias sociais) ou as pesquisas na *dark web*. É por isso que é crucial desenvolver o nosso próprio modelo de ameaças individual, que não só identifique e priorize as ameaças reais e potenciais às quais estamos expostos, mas também defina medidas práticas para mitigar esses riscos.

Publicado no InCyber.

***Fanny Tan** é pesquisadora e estudante de ciências políticas na UQAM. É bacharel em mídia digital na UQAM e certificada em design de videogames. Como jornalista freelance, escreve regularmente na mídia canadense sobre questões sociais relacionadas a novas tecnologias e é colaboradora de tecnologia no programa de rádio Moteur de Recherche (ICI Première). Tan é membro da organização de defesa da privacidade Lab 2038.*