Homeland Security

Departamento de Segurança Interna (DHS)
Escritório de Parceria e Engajamento (OPE)

Recursos pessoais relativos à ameaça de Doxing

16 de janeiro de 2024

O QUE É DOXING?

Doxing é a prática de coleta de informação pessoal identificável (PII) acompanhada da distribuição pública dessa informação, com propósitos maliciosos de humilhação pública, perseguição, apropriação indébita de identidade, ou com vistas a assédio direcionado.

EXEMPLOS DE INFORMAÇÃO CONFIDENCIAL

- **Nome completo**
- **Informações de contato**
- **Endereço residencial**
- **Membros da família**
- **Detalhes do local de trabalho**
- **Informação Financeira**
- **Número da Previdência Social**

FONTES COMUNS DE INFORMAÇÃO CONFIDENCIAL

- **Postagens nos meios de comunicação social**
- **Registros relativos a bens e justiça**
- **Anúncios sobre matrimônio e obituário**
- **Boletins informativos**
- **Conferências públicas**
- **Fóruns, Blogs e salas de discussões**
- **Redes desprotegidas**
- **Listas de registro de eleitor**

COMO EU POSSO ME PROTEGER DE DOXING?

- **Tenha cuidado** com postagens pessoais na Internet, inclusive fotos e vídeos, mesmo que temporárias.
- **Remova** as PII (endereço, data de nascimento, no. de telefone, etc.) dos seus perfis na mídia social.
- **Examine** os seus seguidores e rejeite pedidos de todas as pessoas desconhecidas.
- **Requisite** a remoção dos seus dados pessoais dos sites de registros públicos. Sites bem conhecidos são: BeenVerified, FastPeopleSearch, Intelius, PeopleFinders, Spokeo, TruthFinder, e Whitepages.
- **Remova** aplicativos e extensões de navegador desnecessários evitando a coleta de dados pessoais.
- **Restrinja** o monitoramento de local em aplicativos e sites da web. Desative os serviços de localização em cada aplicativo ou plataforma.
- **Ative** as configurações de privacidade na mídia social, nos aplicativos e em outros sites de web.
- **Configure** a verificação de duas fases, utilize senhas complexas e não repita a mesma senha em diferentes contas.

DHS OPE

COMO EU POSSO ME PROTEGER DE DOXING?

Solicite a remoção de conteúdo falso, abusivo ou ameaçador
Considere o envio de solicitação de remoção para a plataforma ou o site de web, de acordo com as regras e exigências.

Faça a documentação da ocorrência
Considere medidas para preservar as evidências. Salve todos os e-mails, mensagens de voz e de texto que recebe, e faça a captura de tela de comentários na mídia social.

Reporte o incidente
Se você recebeu uma ameaça contra a sua segurança física ou se sente assediado criminosamente, reporte o incidente à polícia local, bem como à plataforma de mídia social ou ao administrador do site de web.

RECURSOS ADICIONAIS E ORIENTAÇÕES

Melhores Práticas e Recursos de Segurança Cibernética da Agência de Segurança e Infraestrutura Cibernética (CISA) : cisa.gov/cybersecurity

Fundamentos de Cibernética da CISA: cisa.gov/cyber-essentials

Dicas da CISA: Evite ataques de engenharia social e de phishing]: cisa.gov/tips/st04-014

Perspectivas da CISA: Melhoramento de segurança de e-mail e navegação: cisa.gov/publication/enhance-email-and-web-security

Orientações da CISA sobre ameaças na mídia social para funcionários de escola e infografia para autoridades: https://www.cisa.gov/resources-tools/resources/social-media-threat-guidance-school-staff-and-authorities-infographic

Caso você seja vítima de um crime cibernético, apresente uma denúncia **para o Centro de Denúncia de Crimes Cibernéticos do FBI (IC3)** no ic3.gov