Como remover seus dados pessoais e boatos da Internet e evitar problemas?

Especialista em direito digital e proteção de dados, José Milagre, explica os riscos de exposição indevida de dados e fakenews na Internet e como pessoas e empresas podem se proteger e remover informações da rede, com 10 estratégias de atuação.

Danos catastróficos

É importante pensar que dados pessoais são, hoje em dia, considerados insumos para criminosos e fraudadores. Com estes dados, marginais podem criar contas, cadastros, contrair empréstimos, fazer compras, clonar chips, tomar perfis em redes sociais, cadastrar a pessoa em redes sociais sexuais, falsear identidade de alguém, além de inúmeras outras atividades que podem trazer inúmeros transtornos para o titular de dados e terceiros, sem contar o uso desabonador e vexatório, onde a vítimas poderá perder oportunidades de negócios, empregos, dentre outros.

Neste sentido, é possível falar ou cogitar em proteção de nossos dados pessoais, limpando-os da Internet? Notícias ou publicações com dados pessoais podem ser removidas? E falsas reclamações ou informações fake? Na verdade, é impossível vivermos sem que haja o compartilhamento de dados pessoais (ainda que inconscientemente), porém, podemos e devemos ter o controle de onde estes dados circulam e não podemos hesitar em agir caso estejam estampados para todo o mundo.

Não é bom que fiquem expostos em resultados de busca ou sites públicos dados financeiros, imagens antigas, de alta resolução, documentos, endereços, dados de familiares, vencimentos, dentre outras informações. No escritório especializado em direito digital, somos capacitados em gestão da reputação online (ORM), atuando com tools de última geração para detecção e procedimentos de remoção de conteúdos indevidos, atuando para empresas, políticos, personalidades, executivos, pessoas físicas e jurídicas em geral. Seja você uma pessoa pública ou não: Não é obrigado a conviver com exposição que pode lhe trazer danos morais,

físicos e materiais, sempre que pesquisam por seu nome na Internet ou redes sociais.

Neste texto, selecionei algumas estratégias que podem ajudar nesta tarefa de manter-se seguro e sem dados pessoais ou desabonadores na Internet.

Mas, qual o problema?

Talvez, o principal problema sobre nossas informações pessoais na Internet seja o fato de que a maioria delas está lá sem a nossa autorização, à medida em que navegamos, compartilhamos informações na web, muitas vezes sem permissão ou de forma inconsciente. Estes dados podem ser coletados por mineradores, bots, crawlers e são agrupados, classificados e podem revelar informações sobre uma pessoa, preferências, status financeiro, doenças, interesses, posses, paradeiros, etc. Estas inferências podem ser usadas para golpes, crimes digitais, contra a honra e discriminação.

Dark web

Os dados vazados ou copiados atualmente vão parar em painéis feitos por crackers (cibercriminosos) na Darkweb e ficam à disposição para compras e aquisições. Pode-se comprar um ou centenas de registros. Quem compra, compra para aplicar golpes. Então, quando você recebe uma ligação do seu "gerente do banco" (bandido se passando por ele) e seus dados pessoais são confirmados ou ele sabia todas as suas informações, provavelmente ele se valeu destas fontes criminosas que fazem do mercado de registros e dados um negócio altamente lucrativo.

Como descobrir?

Um ponto de partida são os buscadores, que podem revelar indícios na web de superfície. É provável que ao digitar seu nome do Google encontre registros que sequer sabia que existiam, dados pessoais, informações falsas ou equivocadas, preferências, processos judiciais em sigilo, empresas no nome, reclamações falsas e outras informações que não deveriam ser públicas, para sua segurança e de seu negócio. Além disso, no escritório, atuamos com inteligência cibernética e investigações técnicas, de modo a identificar dados pessoais em repositórios não acessíveis por meios convencionais ou hospedados em serviços internacionais.

Dá para apagar tudo?

Apagar por completo a pegada digital é muito difícil, pois a cada dia estamos gerando mais e mais dados e "pedaços de informações". Por isso, o monitoramento contínuo de exposição de dados pessoais ou dados corporativos sensíveis é fundamental, além do monitoramento da reputação, ataques indevidos ou falsas notícias e reclamações. Preparei opções para reduzir a exposição, com eliminação e controles sobre informações pessoais que aparecem sobre você na web.

Orientações preventivas

Dentre as estratégias para reduzir sua exposição digital e aumentar sua privacidade, posso citar dez essenciais:

1 Revise e exclua contas antigas em jogos ou em redes sociais. A ferramenta Mine® pode ajudar a você lembrar quais contas estão no seu nome/e-mail na Internet.

2 Revise configurações de privacidade de aplicativos e redes sociais, ativando controles de segurança que permitam que seus conteúdos só sejam vistos por amigos. Denuncie imediatamente contas fakes identificadas.

3 Aja imediatamente em face de sites indexadores que coletam dados públicos, de processos judiciais e fazem dossiês sobre pessoas. Não é porque o dado é público que ele pode ser usado de qualquer modo, inclusive para criação de perfis que possam te prejudicar, com a agregação de informações. Lembre-se que muitos sistemas processuais mantêm cópias de documentos de partes e dados sensíveis. Se for caso, peticione pedindo sigilo.

5 Jamais cadastre ou publique seu e-mail usado para autenticações bancárias em sites, redes sociais, blogs/fóruns na Internet. Prefira ter um e-mail privado, apenas para autenticação em bancos e fintechs. Cuidado com códigos via SMS para acesso a contas. Prefira sempre APPs autenticadores ou um e-mail seguro.

6 Limpe sempre os cookies e histórico de navegação, dificultando o rastreio virtual.

7 Troque o Google, que hoje totaliza 96% das pesquisas de usuários, por buscadores mais privados. Faça o mesmo com seu navegador. Hoje existem

navegadores menos populares, mas muito mais seguros. Uma sugestão é o *Duck Duck Go* (https://play.google.com/store/apps/details?id=com.duckduckgo.mobile.android&hl=en_US&gl=US&pli=1) A consultoria de um *privacy expert* pode lhe orientar a criar ambientes seguros e privados, seja no âmbito pessoal ou empresarial.

8 Utilize uma VPN (Virtual Private Network), do mesmo modo, prejudicando a coleta de dados de navegação e o rastreio de suas atividades. Existem excelentes opções gratuitas. A minha indicação é a HotSpot Shield, acessível em https://www.hotspotshield.com/

9 Assine um sistema de gestão de reputação online ou vazamento de dados pessoais, monitorando em tempo real quando ocorrem, para que saiba rapidamente e aja para impedir que criminosos utilizem os dados ou causem danos. Uma plataforma gratuita que pode lhe dar inputs sobre dados vazados, contas em seu nome e outras informações, como chaves PIX criadas é o registrato, acessível em https://registrato.bcb.gov.br

10 Em caso de recusa, impossibilidade de remoção ou de identificação dos responsáveis, conte com um escritório de advocacia especializado em direito digital, para procedimentos especializados de identificação das ofensas e remoção de dados e informações falsas, desabonadoras ou prejudiciais, ou aplicação do direito ao esquecimento.

Aja imediatamente

A cada dia que os dados pessoais ou informações falsas e equivocadas permanecem no ar, maiores os riscos às pessoas, familiares e empresas. O escritório especializado em Direito Digital (http://www.direitodigital.adv.br) atua há mais de 15 anos e com expertise em remoção de dados pessoais, fakenews, informações equivocadas e descabidas da Internet. Além disso, atuamos com a apuração da autoria de boatos, calúnias, concorrência desleal, ofensas na Internet, mesmo que publicadas em domínios internacionais.

Temos parceria com a empresa de perícia digital CyberExperts (http://www.cyberexperts.com.br) e seu serviço Minha Imagem – Monitoramento de dados pessoais e exposição indevida da imagem. Com isso, oferecemos a clientes e empresas, monitoramento em tempo real de vazamentos, dados pessoais, informações inverídicas e boatos e imediatamente iniciamos

procedimentos especializados, com objetivo de identificar responsáveis e remover os conteúdos, fazendo a gestão da reputação online de crises, com procedimentos técnicos e jurídicos.

Portanto, em tempo de dados pessoais como insumos de crimes, e de confiança cega no que "está na Internet", adotar medidas para se proteger e atuar com segurança demonstra-se fundamental.

Canal Youtube

Você já conhece meu canal? No meu canal no Youtube você encontra inúmeros tutoriais e vídeos sobre como aprimorar sua privacidade e segurança digital. Acesse https://www.youtube.com/user/josemilagre/ e não deixe de se inscrever para ser avisado dos vídeos exclusivos semanais. Me siga no Instagram http://www.instagram.com/dr.josemilagre

José Milagre é Diretor de Forense Digital e Resposta a Incidentes da CyberExperts. Advogado e Perito Especialista em Segurança Digital, Resposta a Incidentes e Crimes Cibernéticos. Certificaçõs CIPM, CDPO IAPP, DPO EXIN, ISO 27701 Lead Implementer PECB, Graduação em Análise de Sistemas, Pós Graduado em Gestão de Tecnologia da Informação. Mestre e Doutor em Ciência da Informação pela Universidade Estadual Paulista UNESP, Presidente da Comissão de Direito Digital da OAB Barueri/SP.