Gerir a Sua Pegada Digital

A pegada digital é toda a informação que existe na Internet como resultado da atividade online. Inclui, entre outras coisas, as suas publicações nas redes sociais, conversas, textos, histórico de navegação, e-mails, compras online e dados de localização. A sua pegada digital pode:

- **Aumentar o risco de ser vítima de uma burla.** Os burlões e os autores de fraudes podem aproveitar a sua pegada digital para o perseguir, fazer-se passar por si ou roubar as suas informações.
- **Deixá-lo exposto à vigilância, incluindo por parte de agências governamentais ou pessoas abusivas ou controladoras.** Isto inclui saber onde está caso a sua localização esteja ativada ou se estiver a consultar as redes sociais.
- **Aumentar a probabilidade de perseguição** Os criminosos utilizam a pegada digital das pessoas para as atrair para situações de trabalho forçado ou coagido. Os extremistas e outras pessoas mal intencionadas também podem usar a pegada digital das pessoas para as atacar com discursos de ódio e crimes de ódio.
- **Afetar negativamente o seu processo de imigração.** As contas das redes sociais, nomes de utilizador/handles e outras informações digitais devem agora ser divulgadas como parte de muitos processos de imigração comuns, e os dispositivos eletrónicos podem ser revistados quando alguém pretende entrar nos EUA ou fica sob custódia do Departamento de Segurança Interna. A atividade online de uma pessoa pode ser utilizada para influenciar decisões sobre detenção, deportação, alterações

no estatuto, naturalização, asilo ou outras formas de auxílio à imigração.

A gestão da sua pegada digital é fundamental para a sua segurança, proteção e reputação!

12 Conselhos para Gerir a Sua Pegada Digital

1. **Proteja os seus dispositivos e contas.** Certifique-se de que todos os seus dispositivos têm uma palavra-passe forte e, idealmente, autenticação de dois fatores. Por autenticação de dois fatores entende-se quando existem dois métodos de autenticação, como uma palavra-passe mais a introdução de um código recebido no telemóvel.

2. **Não partilhe informações privadas.** Não publique o seu nome completo, morada, número de telefone ou outras informações privadas na internet, incluindo nas redes sociais.

   Não identifique a sua localização nas redes sociais.

   Não publique fotografias que possam identificar onde está, onde vive, o local de trabalho ou a escola, por exemplo, números de porta, placas de rua, matrículas, emblemas de uniformes, etc.

3. **Torne as suas contas privadas.** Se tem contas nas redes sociais, certifique-se de que são privadas. Geralmente, pode fazê-lo acedendo à sua conta, indo a Definições ou Privacidade e confirmando que a opção «privado» está selecionada.

4. **Elimine contas antigas.** Se já não utiliza uma conta, elimine-a. Da mesma forma, desative o armazenamento na cloud ou as contas em quaisquer dispositivos antigos que ainda tenha, mas que raramente utilize.

5. **Desative a localização.** Para desativar os serviços de localização num dispositivo, aceda às definições do mesmo, que normalmente se encontram em «Privacidade», «Segurança» ou «Localização». De seguida, desative os Serviços de Localização para não permitir que as aplicações e os serviços fiquem a saber a sua localização.

6. **Limite o que publica.** Publique uma quantidade mínima de dados online.

   Seja consciente do que publica, uma vez que o conteúdo pode ser mal

interpretado ou expô-lo a um maior risco de se tornar um alvo. Por exemplo, publicar uma fotografia a beber álcool, a segurar uma arma, etc.

7. **Não aceite pedidos de amizade de pessoas que não conhece.** Certifique-se de que só aceita pedidos de amizade de pessoas que conhece. Qualquer pessoa pode esconder-se atrás de um perfil, incluindo burlões, traficantes e pessoas que tentam persegui-lo. Elimine os amigos das suas contas se não os conhecer pessoalmente.

8. **Elimine material e aplicações sensíveis dos telemóveis e outros dispositivos**. Em viagens internacionais, os agentes do Departamento de Segurança Interna podem revistar os dispositivos eletrónicos nos pontos de entrada quando voltar a entrar nos EUA. Apague todas as mensagens, fotografias, aplicações e outros materiais que possam ser mal interpretados.

9. **Comunique de forma segura.** Utilize aplicações de comunicação que ofereçam encriptação de ponta a ponta, como o WhatsApp, o Signal e o Telegram.

   Nota: Embora mais seguras, mesmo as plataformas de mensagens encriptadas podem contribuir para a sua pegada digital através de metadados armazenados, como com quem comunica e quando, bem como conteúdos partilhados, como vídeos, imagens e informações de perfil. Tenha atenção ao que comunica.

10. **Tenha cuidado ao navegar na Internet.** Não clique em links suspeitos de remetentes que não conhece nem aceda a sites não confiáveis, pois podem expô-lo a vírus e a uma potencial vigilância.

    Forneça apenas as informações necessárias e tenha muito cuidado com os sites ou aplicações que solicitam mais informações pessoais do que as necessárias.

    Limpe regularmente os cookies e a cache do seu browser. Normalmente, pode fazê-lo indo às Definições do seu navegador, depois às Definições de Privacidade e, de seguida, procure «limpar dados de navegação» ou uma opção semelhante.

11. **Utilize um telemóvel provisório ou descartável.** Estes telefones são frequentemente pré-pagos e não estão vinculados a um contrato, o que os torna mais fáceis de utilizar para manter o anonimato e evitar o rastreamento. No entanto, se utilizar um telefone provisório, certifique-se de que as pessoas que precisam de o contactar (assistente social, advogado, etc.) têm o seu número

atualizado. Por vezes, as pessoas optam por ter dois telefones – um telefone provisório para a sua atividade online e um telefone permanente para comunicações importantes e estáveis com pessoas importantes.

12. **Utilize tampas para a câmara.** Utilize tampas para a câmara dos telemóveis e computadores portáteis para bloquear a lente quando não estiver a ser utilizada. Isto pode evitar invasões de privacidade.