DICAS DA “UNITED STATES NATIONAL COUNTERINTELLIGENCE EXECUTIVE” PARA SEGURANÇA EM VIAGENS INTERNACIONAIS.

VOCÊ DEVE SABER

Na maioria dos países, você não tem nenhuma expectativa de privacidade em Internet cafés, hotéis, escritórios ou locais públicos.
Centros de negócios do hotel e redes de telefonia são monitorados regularmente em muitos países.
Em alguns países, quartos de hotel são muitas vezes monitorados.

Todas as informações que você envia eletronicamente - por fax, assistente digital pessoal (PDA), computador ou telefone - podem ser interceptadas.
Os dispositivos sem fios são especialmente vulneráveis.

Serviços de segurança e criminosos podem controlar seus movimentos usando seu telefone celular ou PDA e podem ligar o microfone do dispositivo mesmo quando você acha que ele está desligado.
Para evitar isso, remova a bateria.

Serviços de segurança e criminosos podem inserir software malicioso em seu aparelho através de qualquer conexão que eles controlem.
Eles também podem fazê-lo quando seu aparelho está habilitado para uso com redes “wi-fi”.
Quando você se conectar ao seu servidor de casa, o "malware" pode migrar para o seu negócio, agência ou sistema de home, pode inventariar seu sistema, e pode enviar informações de volta para o serviço de segurança ou potencial criminoso.

Malware pode ser transferido para o dispositivo através de pen drives (USBsticks), disco de computador e outros "presentes".

Transmitir informação governamental, pessoal, ou proprietárias do exterior que sejam sensíveis é arriscado.

Funcionários de empresas e governos estão em risco maior, mas não assuma que você é demasiado insignificante para ser alvo.

Serviços de segurança estrangeiros e criminosos são adeptos a "phishing" - ou seja, fingem ser alguém da sua confiança, a fim de obter informações pessoais ou confidenciais.

Se um aduaneiro oficial exigir examinar o seu dispositivo ou o seu quarto de hotel tiver sido revistado sem sua presença e o dispositivo estava no quarto, você deve assumir que o disco rígido do dispositivo foi copiado.

ANTES DE VIAJAR

Se você pode viajar sem o dispositivo, não o leve.

Não leve informação que você não precisa, incluindo informações de contatos sensíveis.
Considere as consequências se suas informações forem roubadas por um governo estrangeiro ou concorrente.

Faça backup de todas as informações que você leva; deixar os dados de backup em casa.
Se possível, use um telefone celular ou PDA diferente do seu habitual e remova a bateria quando não estiver em uso.

Em qualquer caso, o dispositivo deverá ser examinado por sua agência ou empresa quando você voltar.

Procure alertas oficiais de segurança cibernética em:

www.onguardonline.gov e

www.us-cert.gov/cas/tips

PREPARE SEU DISPOSITIVO

Crie uma senha forte (números, letras maiúsculas e minúsculas, caracteres especiais - pelo menos 8 caracteres). Nunca armazene senhas, números de telefone, ou sequências de “sign-on” em qualquer dispositivo.

Alterar senhas em intervalos regulares (e, logo que você voltar).
Baixar e atualizar o antivírus, a proteção contra “spyware”, “patches” de segurança do “OS”, e um firewall pessoal.

Criptografar todas as informações sensíveis no dispositivo.
Em alguns países, as autoridades aduaneiras podem não lhe permitir entrar com informações criptografadas.

Atualize seu navegador Web com as configurações de segurança mais restritivas.

Desative portas e recursos que você não precisa em relação ao infravermelho.

Use uma máquina virtual para rodar sua área de trabalho durante a viagem, a fim de garantir que todas as alterações feitas no sistema estão isoladas dentro do ambiente virtual.

ENQUANTO VOCÊ ESTIVER FORA

Evite transportar dispositivos na bagagem despachada.

Use os recursos de assinatura e criptografia digitais, quando possível.

Não deixe aparelhos eletrônicos sem vigilância.
Se você tem que encostá-lo, remova a bateria, o cartão SIM e mantenha-o com você.

Não use pen drives dados a você; eles podem estar comprometidos.
Não utilize o seu próprio pen drive em um computador externo, pela mesma razão.
Se você é obrigado a fazê-lo de qualquer maneira, suponha que você tenha sido comprometido; limpe o seu aparelho assim que você puder.

Proteger senhas da vista dos outros.
Não utilize o recurso "Remember Me" em muitos sites; digite novamente a senha toda vez.

Esteja ciente de quem está olhando para sua tela, especialmente em áreas públicas.

Terminar ligações quando você não a estiver usando.

Limpe seu navegador após usar: Excluir arquivos de histórico, caches, cookies, URL, e arquivos temporários da internet.

Não abra e-mails ou anexos de fontes desconhecidas.

Não clique em links de e-mails.
Esvazie a sua "trash" e as pastas "recentes" após cada utilização.

Evite redes Wi-Fi, se puder.
Em alguns países, elas são controladas pelos serviços de segurança; em todos os casos, elas são inseguras.

Se o dispositivo ou informação for roubado, comunique imediatamente a sua organização, a embaixada dos EUA ou consulado local.

QUANDO VOCÊ RETORNAR

Alterar sua senha.
Peça para sua empresa ou agência examinar o dispositivo para verificar a presença de software malicioso.

Para alertas de viagem e informações gerais, consulte:

http://travel.state.gov/content/passports/english/alertswarnings.html

Bibliografia: Official (ISC)² Guide to the CISSP CBK Edição 4 (paginas 935/937).
Tradução: Jaime Orts Y Lugo.
Data: 13/08/2015.