

VIAGENS AO EXTERIOR



POR QUE SE PROTEGER NO EXTERIOR?

Países, empresas e grupos de interesse estão em competição permanente na busca de um melhor posicionamento estratégico no cenário internacional.

A **Espionagem** é uma ameaça real, que emprega diversas técnicas para enganar, manipular ou explorar a confiança das pessoas, a fim de obter informações privilegiadas.

Também é real a intenção de influenciar os rumos políticos do País para favorecer interesses estrangeiros em detrimento dos nacionais. Chamamos essa ameaça de **Interferência externa**.

Em solo estrangeiro, autoridades e servidores públicos em missão oficial precisam ter consciência das próprias **vulnerabilidades**, redobrar a atenção e observar algumas medidas de segurança.

POR QUE ESTARIAM INTERESSADOS EM MIM?

Porque, como servidor público e representante do Governo brasileiro, você tem acesso a informações **sigilosas ou privilegiadas**, o que o torna uma atraente fonte de informações estratégicas sobre nossa política externa, comércio, agricultura, energia, etc.

Para evitar situações de risco, confira 10 dicas de segurança elaboradas pelo Programa Nacional de Proteção do Conhecimento Sensível (PNPC), da Agência Brasileira de Inteligência (ABIN).



Aperte os cadeados e boa viagem!

A silhouette of a man in a suit and tie, seen from behind, walking through an airport terminal. He is pulling a suitcase on a cart. The terminal has large windows showing the outside. The image has a warm, orange-tinted glow.

Antes de Partir

1

ANTECIBE O DISCURSO



O que dizer? Reflita sobre informações pessoais e profissionais que podem ou não ser compartilhadas com entidades estrangeiras e combine o discurso com os colegas.

Minha história. Tenha consciência ainda de seu background étnico, geográfico e religioso. Essas características podem ser exploradas em uma eventual abordagem.

Quem sou? Reflita ainda sobre suas vulnerabilidades, como sociabilidade excessiva, vaidade, ambição, indiscrição, abuso de bebidas alcoólicas, etc.



Frase do dia: Dados cotidianos para você podem ser valiosos para os outros.

2

DEIXE FORA DA MALA



Sem papel. Não leve documentos impressos e outros materiais de trabalho que, se apreendidos por autoridades de segurança locais, possam gerar riscos aos servidores ou à instituição.

Meu celular, minha vida. Apague conteúdos sensíveis armazenados em seus aparelhos eletrônicos, como celular, *laptop*, *tablet* e *smartwatch*.

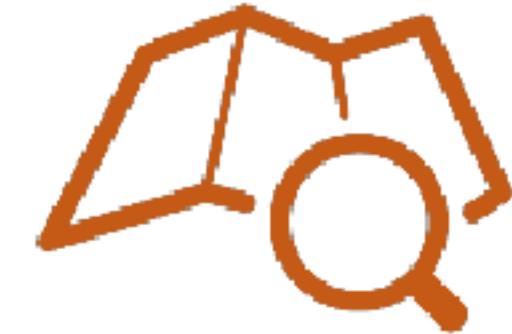
Mala diplomática. Use criptografia para proteger arquivos e leve documentos classificados por mala diplomática.



Frase do dia: Menos é mais.

3

PESQUISE SOBRE O DESTINO



O que me espera? Informe-se sobre leis e regulamentos, especialmente em relação ao controle na fronteira e uso de criptografia. Busque ainda conhecimentos sobre cultura e costumes.

Quem são eles? Procure saber mais sobre seus interlocutores estrangeiros, além de dados sobre o local de encontro ou reunião oficial, se for o caso.

S.O.S. Tenha em mãos contatos do consulado ou da embaixada do Brasil, em caso de emergência.



Frase do dia: **Informação é poder.**

Durante a Viagem



4

NÃO CRIE EXPECTATIVA DE PRIVACIDADE



Não estou em casa. Não crie expectativa de privacidade em ambientes públicos nem mesmo em privados, como quartos de hotel.

No hotel. Caso seja imprescindível deixar dispositivos eletrônicos e documentos no cofre do hotel, deixe as cortinas fechadas, coloque o aviso *Do Not Disturb* e leve a chave com você.

Posts. Evite publicar fotos da viagem em redes sociais até voltar ao Brasil. Elas podem revelar suas rotinas e sua localização.



Frase do dia: Nenhum lugar é 100% seguro.

5

PROTEJA OS ELETRÔNICOS



No avião. Leve os aparelhos eletrônicos na mala de mão. Use senhas fortes para bloqueio dos equipamentos, de preferência, diferentes das utilizadas em outras contas e dispositivos pessoais.

Em todo lugar. Desligue o *bluetooth* e evite usar *wi-fi* de hotéis, aeroportos e locais turísticos. Não use carregadores públicos (algo comum em aeroportos), especialmente aqueles conectados em portas USB.

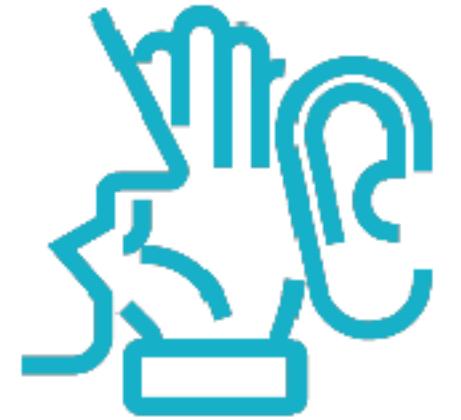
Criptografados. Não use *WhatsApp* ou e-mail particular para enviar informações sensíveis.



Frase do dia: Pare, pense, conecte.

6

NÃO CONTE “SEGREDOS” EM PORTUGUÊS



What? Em viagem ao exterior, você já fez algum comentário em língua portuguesa sem se preocupar por achar que ninguém estava entendendo?

Oops. É possível que serviços de Inteligência estrangeiros gravem conversas ou infiltram pessoas fluentes na língua portuguesa em ambientes onde representantes brasileiros se encontram.

Alô? Evite usar o português como proteção a dados sensíveis em *Uber*, táxi, restaurantes... Inclusive durante conversas ao telefone.



Frase do dia: Eles também falam português.

7

FUJA DE PROVOCAÇÕES



Discrição. Evite entrar em situações comprometedoras: seja cético, discreto e vigilante em ambiente de trabalho ou de lazer.

Não, obrigado. Cuidado com abordagens de estrangeiros sobre suas necessidades e interesses pessoais. Seja evasivo quanto ao seu salário e sua satisfação com o trabalho. Resista a bajulações, facilidades e benefícios.

Não sei... Desinforme seu acesso a informações e use dados ostensivos, que estão em leis e decretos, para responder a perguntas delicadas. Ou, simplesmente, diga que não sabe.



Frase do dia: **Não existe almoço grátis.**



Depois da
Missão

8

DESCARTE CERTOS PRESENTES



Presente de grego. É cada vez mais comum a entrega de *pen drives* como brindes em eventos (conferências, palestras, cursos, etc.). Mais comum ainda é o que vem nesses “presentes”: vírus.

***Spyware*.** Esses *malwares* são usados para que o governo ou entidade estrangeira consiga acesso a informações de seu computador pessoal ou funcional.

Descarte. Não utilize *pen drives*, *HD* externos e outros dispositivos presenteados.



Frase do dia: Presente de grego, literalmente, é Cavalo de Troia.

9

FAÇA O *CHECK-UP* DOS APARELHOS



Pós-evento. Não abra anexos de e-mail ou *links* enviados depois de eventos patrocinados por estrangeiros, como apresentações de *Power Point*. Muitas vezes eles vêm com vírus para roubar as informações dos seus aparelhos eletrônicos.

TI. Se o conteúdo for importante para o seu trabalho, peça para o setor de tecnologia de informações avaliar o material antes de acessá-lo.

Check-up. Verifique se houve contaminação de *malware* nos seus aparelhos eletrônicos. Também é recomendável trocar senhas utilizadas durante a viagem.



Frase do dia: **Antes seguro que curioso.**

10

REPORTE INCIDENTES



Avalie a viagem. Troque experiências com colegas de trabalho sobre as situações vivenciadas e reflita sobre prós e contras. Faça um relatório ou memória da viagem.

Será? Caso você tenha percebido algum comportamento “estranho” de estrangeiros ou tenha desconfiado de algumas situações, informe seu chefe e o setor de segurança do seu órgão.

Reporte. Você pode ainda enviar um e-mail para reporte@abin.gov.br. Às vezes parece ser uma questão boba ou passageira, mas, na verdade, você pode ter sido espionado durante a missão!



Frase do dia: Qualquer semelhança não é mera coincidência.