SIS

Serviço
de Informações
de Segurança

PASSAPORTE

Segurança
nas Deslocações
ao Estrangeiro

PAÍSES DISTINTOS
COSTUMES DIFERENTES

As posições de topo dentro de uma organização e todos aqueles que trabalham com informação sensível correm maior risco de os seus dispositivos eletrónicos e de armazenamento serem alvo de ações de ciberespionagem.

... .

A exploração de novos mercados cria um conjunto de oportunidades para as organizações nacionais. Contudo, também se torna necessário acautelar o aumento dos riscos de segurança associados a essas oportunidades.

SIS

Hotéis, espaços públicos e gabinetes temporários não garantem confidencialidade e integridade a nível físico e digital.

Em muitos países os centros de reuniões e as redes públicas são monitorizados. O mesmo é válido para todas as redes de acesso à Internet. Independentemente de se tratarem de redes reservadas (e.g. wifi de hotéis ou de aviões) ou de redes de acesso generalizado (e.g. aeroportos ou restaurantes), todas são passíveis de serem rastreadas para a monitorização dos dispositivos a elas conectados.

Aspetos a ter presente numa viagem de trabalho

O quadro legal no país de destino pode ser muito distinto do existente em Portugal. Será que, por exemplo, é permitido transportar uma pen USB cifrada para esse país? Será que, ao abrigo das leis desse país, é possível estabelecer uma ligação por VPN?

SIS

Tenha em atenção dispositivos eletrónicos, cartões de memória ou USB oferecidos. Podem conter software malicioso

Situações permitidas em alguns países:

- Medidas repressivas arbitrárias do Estado
- Chantagem e criação de situações comprometedoras
- Buscas clandestinas e propositadas aos quartos de hotel (incluindo ao cofre) e à bagagem (nos aeroportos/hotel)
- Manipulação ou duplicação do conteúdo de dispositivos eletrónicos

SIS

- Infeção de dispositivos eletrónicos com software malicioso, como por exemplo spyware
- Proibição de acesso a determinados websites
- Proibição de utilização de VPN
- Monitorização da Internet, das telecomunicações e do serviço de correio eletrónico

SIS

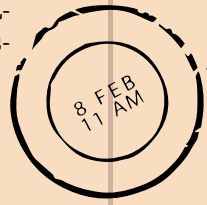
Ação Recomendada

Antes da Viagem:

- Pesquise informação sobre a situação de segurança, riscos e legislação do país de destino
- Leve informação de contactos para situações de emergência
- Divulgue a um número restrito de pessoas a viagem que vai realizar (local, motivo, agenda). Seja discreto
- Observe o princípio da economia de dados e transporte o mínimo de informação sensível da sua organização
- Utilize laptops/smartphones dedicados, específicos para viagens

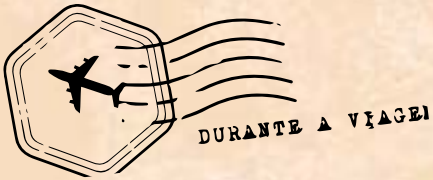
SIS

- As credenciais de acesso a todas as aplicações nesses dispositivos deverão ser válidas apenas nessa viagem e ative o multifator de autenticação
- Se possível, cifre a informação do seu laptop/smartphone
- Emita um certificado de autenticação da VPN específico para essa viagem
- Utilize serviços de armazenamento em Cloud autorizados pela sua organização
- No caso de não conseguir levar equipamentos dedicados, de viagem, apague o histórico de pesquisa e de chamadas. O mesmo para a memória cache, cookies, passwords de acesso a websites e ficheiros temporários



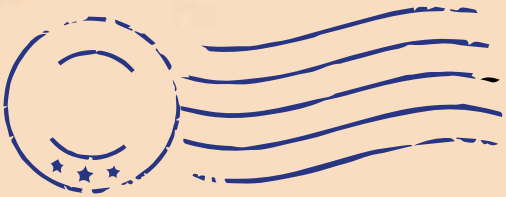
- Faça backups da sua informação e deixe-os em Portugal
- Tenha atenção aos pedidos de permissão das aplicações que instala, nomeadamente referentes ao uso de microfone e câmara
- Verifique se os seus dispositivos e todas as suas aplicações estão atualizados
- Configure software antivírus em todos os dispositivos

- Defina o número de tentativas falhadas da palavra-passe para que a opção de bloqueio do dispositivo seja ativada
- Ative as opções de bloqueio remoto em caso de perda do smartphone
- Configure nas redes sociais as opções de segurança e privacidade para salvaguardar os seus dados



Durante a Viagem:

- Não coloque informação sensível na bagagem de porão
- Marque os equipamentos com um sinal para evitar trocas, como por exemplo nos aeroportos e no tapete junto ao detetor de metais
- Em caso de desaparecimento de dispositivos ou informação, notifique de imediato a sua organização
- Opte por levar um powerbank. Não carregue o seu equipamento nos terminais elétricos self-service, por exemplo de aeroportos. Alguns desses terminais poderão ser utilizados como porta de aces-

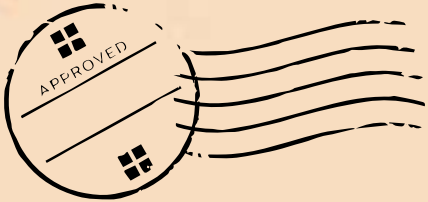


so do atacante ao seu dispositivo

- Não se ligue a wifi gratuitos, sobretudo de aeroportos, hotéis e restaurantes. Se precisar mesmo de se ligar, utilize uma VPN e autenticação multifator para acesso à rede profissional
- Mantenha o bluetooth, wifi, NFC e geolocalização desligados quando não está a utilizá-los
- Não abra links nem anexos de emails desconhecidos, nem de entidades que possam parecer fidedignas sem confirmar telefonicamente com o emissor
- Conecte-se apenas a websites HTTPS e não armazene passwords

no seu browser

- Evite o acesso e a utilização de dados bancários em ambiente digital no decurso da viagem e, em particular, quando estiver ligado a uma rede de wifi gratuita. No caso de ter mesmo de aceder, privilegie o uso de 4/5G e de uma VPN
- Não aceda a websites de streaming e de jogo online não oficiais, pois muitos contêm malware nos ficheiros que disponibilizam
- No avião, trabalhe com filtros de écran no seu portátil e não discuta assuntos de trabalho em espaços públicos
- Esteja sempre alerta para tentati-

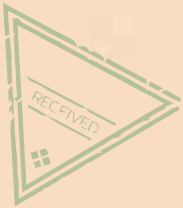


vas de abordagens inusitadas (em táxis, hotéis, restaurantes) e a pessoas que o abordam com interesses pessoais coincidentes com os seus

- Se possível, transporte sempre consigo os seus dispositivos eletrónicos e a informação que quer proteger. Em determinados destinos, o quarto de hotel e o cofre não são seguros
- No quarto de hotel, quando se ausentar para jantar, deixe um cartão de eletricidade acionado, a TV ligada e o dístico "do not disturb" pendurado na maçaneta exterior da porta
- Nunca perca o controlo físico e

visual relativamente aos seus dispositivos eletrónicos e esteja atento em momentos propícios a uma separação obrigatória face aos mesmos (e.g. piscinas, bagagem de porão, spas, etc.)

- Nunca discuta assuntos relevantes em português na presença dos seus interlocutores estrangeiros. Não sabe qual o domínio que poderão ter da nossa língua
- Esteja atento a desvios da agenda durante reuniões de trabalho
- Não envie informação sensível enquanto estiver fora (nem por e-mail nem por mensagem escrita no smartphone) e não discuta as-



suntos sensíveis ao telefone

- Não divulgue nas redes sociais onde está, nem porquê, nem publique fotografias que identifiquem o local
- Não utilize dispositivos USB que lhe tenham oferecido (pen drives, cartões de memória, cabos, gadgets)

Depois da Viagem:

- Avalie retrospetivamente os diferentes momentos e situações da viagem para se aperceber de eventuais situações suspeitas
- Troque experiências com os seus colegas
- Não ligue os equipamentos à rede interna da organização sem primeiro fazer uma verificação de segurança
- A informação dos equipamentos dedicados deverá ser totalmente "limpa" e efetuada uma reinstalação das aplicações necessárias para uma nova viagem

- Caso não tenha viajado com um equipamento dedicado, ao regressar a Portugal altere todas as passwords usadas durante a viagem e faça uma verificação de segurança e limpeza ao seu laptop de viagem, ao smartphone e a todos os dispositivos de armazenamento de dados para deteção de malware
- Revogue o certificado de autenticação da VPN criado especificamente para essa viagem
- Em caso da presença de qualquer indício ou ocorrência suspeitos, contacte a unidade de cibersegurança da sua entidade

Caso suspeite de atividades suscetíveis
de configurar situações de espionagem,
não hesite em contactar-nos

SIS
Serviço
de Informações
de Segurança

Para mais informações:
https://ppc.sis.pt | e-mail: ppc.sis@sis.pt