CNCS
Centro Nacional de Cibersegurança
PORTUGAL

CiberDocs
BP_VJC0001_V1.0

RECOMENDAÇÕES
PARA A SUA VIAGEM

SEJA UM VIAJANTE CIBERSEGURO!

O Centro Nacional de Cibersegurança (CNCS) disponibiliza este livro digital com algumas recomendações para proteger as informações pessoais e profissionais que tem nos seus dispositivos eletrónicos.

Este livro pretende dar a conhecer as possíveis ameaças e como lidar com elas.

Quando vai viajar a segurança da sua informação pessoal e profissional deve ser uma prioridade. Ao levar consigo o seu computador, telemóvel e/ou tablet, mesmo sendo do trabalho, pode estar a negligenciar as questões de cibersegurança porque estes dispositivos permitem a troca de dados. Muitos dos dados armazenados são confidenciais e pertencem à sua organização. A perda ou o roubo dessa informação tem consequências negativas para a sua atividade profissional. Numa viagem ao estrangeiro existem medidas para proteger os seus dispositivos móveis de riscos e ameaças.

Em locais públicos, como cafés, hotéis, escritórios, portos e aeroportos pode aceder à Internet em pontos de acesso sem fio (wi-fi), às vezes gratuitos, que estão acessíveis a todos e onde não existe garantia de confidencialidade das informações armazenadas. Os atacantes que pretendem roubar informações podem estabelecer estes pontos de acesso, para parecer confiáveis e ao utilizar uma destas redes pode comprometer os seus dados. Sabe-se que existem países que monitorizam os nossos dados quando estabelecemos uma ligação à rede local.

ANTES DE VIAJAR

1

CONHEÇA E RESPEITE AS REGRAS DE SEGURANÇA DA INFORMAÇÃO DA SUA ORGANIZAÇÃO.

Saiba quais as recomendações técnicas por alguém do departamento técnico ou dos sistemas de informação.

2

SAIBA MAIS SOBRE A LEGISLAÇÃO DOS DADOS DIGITAIS DO LOCAL DE DESTINO.

Está sujeito às leis que regem a propriedade inteletual, informações digitais e dados cifrados nos países que visita. Verifique se os Postos Consulados têm informações adicionais. Por exemplo sobre a utilização de dados cifrados, controlo de dados pelo Governo local, acesso a redes locais e wi-fi, ativos digitais, formato de documentos, ações para o uso de material digital.

3

CONFIRME QUE TEM O ANTIVÍRUS ATUALIZADO NOS SEUS DISPOSITIVOS.

O antivírus deve estar atualizado e a funcionar para se proteger de software malicioso que pode infetar os seus dispositivos.

4

ATUALIZE AS APLICAÇÕES QUE PODEM SER EXIGIDAS PELO SISTEMA OPERATIVO DOS SEUS DISPOSITIVOS.

Estas atualizações permitem corrigir erros e vulnerabilidades de segurança.

5

INSTALE AS APLICAÇÕES E OS PERIFÉRICOS QUE VAI PRECISAR NA SUA VIAGEM.

Assim não terá de comprar no país de destino.

6

LIMPE O HISTÓRICO DO SEU NAVEGADOR E OS COOKIES EM TODOS OS DISPOSITIVOS.

Caso se ligue a uma rede wi-fi pública, o histórico e os cookies são facilmente acedidos e podem ter informações que podem ser utilizadas em transações falsas.

7

COMUNIQUE À SUA ORGANIZAÇÃO QUE LEVA O CARTÃO DE CRÉDITO PARA A SUA VIAGEM.

Ao informar a empresa e o banco da posse de cartão de crédito, datas e locais de viagem, estas entidades podem estar atentas para quaisquer transações suspeitas.

8

RECORRA A AGÊNCIAS DE VIAGENS CONHECIDAS E EVITE SITES DE DESCONTO PARA RESERVAR ATIVIDADES NO PAÍS DE DESTINO.

Existem sites que podem ser configurados para roubar informações confidenciais. Se fizer uma reserva ou uma transação online, recorra a uma entidade de pagamento segura (ex. Paypal) para garantir que o seu cartão de crédito e informações pessoais permaneçam seguras.

9

LEVE OS DISPOSITIVOS QUE SÃO ESSENCIAIS PARA A SUA VIAGEM.

Os dispositivos eletrónicos, discos externos e unidades USB não devem conter informação para além da que necessita na sua viagem.

10

EVITE PUBLICAR PLANOS DE VIAGEM NAS REDES SOCIAIS.

Ao não publicar sobre a sua viagem, os atacantes terão dificuldade em saber qual o melhor momento para atacar de forma digital.

11

FAÇA UM BACKUP DOS SEUS FICHEIROS EM OUTRO DISPOSITIVO E COLOQUE-O EM LOCAL SEGURO OU ARMAZENE OS FICHEIROS EM NUVEM.

Em caso de perda, roubo ou apreensão de equipamento poderá recuperar as suas informações quando regressar da sua viagem.

12

EVITE EXPOR DADOS CONFIDENCIAIS E REMOVA DADOS CONFIDENCIAIS DOS DISPOSITIVOS.

Se possível aceda à rede da sua entidade profissional através de uma ligação segura ou através do serviço de correio eletrónico onde os dados são cifrados.

13

RECORRA A MECANISMOS DE AUTENTICAÇÃO PARA ACEDER AOS SEUS DISPOSITIVOS ELETRÓNICOS.

Pode trabalhar nos seus documentos em locais apropriados e que não sejam de acesso visual ou por cópia de terceiros.

14

IDENTIFIQUE OS SEUS DISPOSITIVOS.

Coloque uma marca colorida ou escreva o seu nome em parte visível do seu dispositivo para evitar trocas. Pode configurar o seu computador com o seu nome e endereço local para ser devolvido se alguém o encontrar.

15

ATIVE A OPÇÃO DE BLOQUEIO DE DISPOSITIVO QUANDO SE INSERE MUITAS VEZES UMA PALAVRA-CHAVE INCORRETA.

Se perder o seu dispositivo, só perderá os seus dados se a opção de apagar, todos os dados, for acionada quando uma palavra-chave é inserida muitas vezes.

16

ATIVE AS OPÇÕES DE BLOQUEIO REMOTO, AUTO-LOCALIZAÇÃO E SOFTWARE ANTI-ROUBO.

Caso tenha um equipamento com estas opções, assegure-se que estão ativas.

DURANTE A VIAGEM

1

MANTENHA OS SEUS DISPOSITIVOS SOBRE VIGILÂNCIA.

Durante a viagem leve os dispositivos na sua bagagem de mão, incluindo cartão SIM e bateria. Não os deixe no escritório, sala de conferência e coloque-os no cofre do quarto do hotel. Mesmo quando eles estão a carregar bateria e caso esteja por perto, as informações podem ser comprometidas.

2

SE TIVER DE SE SEPARAR DOS SEUS DISPOSITIVOS, RETIRE O CARTÃO SIM E SE POSSÍVEL A BATERIA.

O cartão pode conter dados pessoais e profissionais que sejam confidenciais.

3

UTILIZE PALAVRAS-CHAVE PARA PROTEGER O ACESSO AOS SEUS DISPOSITIVOS.

Utilize palavras-chave seguras no acesso aos dispositivos e verifique as políticas de passwords da sua entidade patronal.
Bloquei o seu dispositivo, através dos atalhos do teclado (ex. teclas logótipo Windows+L)

4

REMOVA O HISTÓRICO DAS SUAS CHAMADAS, REGISTOS E DAS PÁGINAS WEB.

Deve remover dados da memória, palavras-chave para acesso a websites e ficheiros temporários.

5

UTILIZE PALAVRAS-CHAVE E PINS DIFERENTES DOS COMUNS

Uma boa forma de configurar uma palavra-chave é combinar três ou quatro palavras relacionadas para criar um código que não seja comum. Adicione números e caracteres especiais.

6

NÃO LIGUE O SEU EQUIPAMENTO AOS POSTOS DE TRABALHO OU PERIFÉRICOS DE COMPUTADORES QUE NÃO SÃO CONFIÁVEIS.

Cuidado com as trocas de documentos em Pen USB durante os eventos. Caso utilize uma Pen para troca de informação, descarte a unidade após o seu uso.

7

INFORME A SUA ENTIDADE EM CASO DE INSPEÇÃO OU APREENSÃO PELAS AUTORIDADES.

Forneça as palavras-chave e dados cifrados se tiver de fazê-lo às autoridades locais.

8

CASO O EQUIPAMENTO OU INFORMAÇÃO SEJA PERDIDA OU ROUBADA, INFORME A SUA ORGANIZAÇÃO.

Peça um conselho ao Posto Consulado antes de qualquer abordagem às autoridades locais.

9

AO UTILIZAR O SEU WI-FI, VERIFIQUE QUE ESTÁ NUM LOCAL SEGURO.

Os atacantes sabem usar ligações wi-fi abertas para aceder a outros dispositivos na rede.

10

MANTENHA O SEU WI-FI E O BLUETOOTH DESLIGADOS ENQUANTO NÃO ESTÁ A UTILIZAR O SEU DISPOSITIVO.

Quando não está ligado à Internet, consegue economizar a vida útil da bateria e pode ajudar a manter os seus dispositivos protegidos contra atacantes.

11

NÃO LIGUE O SEU DISPOSITIVO A UMA UNIDADE FLASH USB (PEN) DESCONHECIDA.

Qualquer dispositivo que se ligue a uma porta USB pode ser considerado um dispositivo que armazena software malicioso.

12

EVITE USAR DISPOSITIVOS DE ARMAZENAMENTO (CDS OU DVDS) NO SEU COMPUTADOR.

Estes dispositivos podem conter software malicioso que lêem automaticamente o conteúdo.

13

USE SOFTWARE DE CRIPTOGRAFIA DURANTE A VIAGEM.

Não comunique informações confidenciais por contacto telefónico ou por transmissão de voz (serviços VoIP, Skype, FaceTime)

14

NÃO CARREGUE O SEU EQUIPAMENTO EM TERMINAIS PÚBLICOS.

Alguns terminais podem ser usados para copiar dados e documentos sem o seu consentimento.

15

DESLIGUE O DISPOSITIVO SE ESTIVER NUM LOCAL DE RISCO ELEVADO.

Os locais de convenções e protestos são vulneráveis ao comprometimento das nossas informações.

16

NÃO TRANSMITA INFORMAÇÃO QUE NÃO GOSTARIA DE DIVULGAR A PESSOAS NÃO AUTORIZADAS.

Confirme o nome da ligação de acesso à Internet antes de iniciar a sessão porque qualquer informação que envie pode ser intercetada através de uma rede desconhecida.

17

DESATIVE A SUA REDE BLUETOOTH ENQUANTO VIAJA PARA EVITAR TENTATIVAS DE LIGAÇÃO FALSAS.

Tenha cuidado na troca de dados com outros utilizadores. Alguns dispositivos permitem uma ligação automática com outras redes Bluetooth, sem qualquer autorização.

18

EVITE CARREGAR O SEU DISPOSITIVO EM EQUIPAMENTOS QUE NÃO CONTROLA.

O software malicioso pode ser armazenado num equipamento desconhecido e transferido para o seu dispositivo. Utilize o seu computador ou uma ficha de tomada direta para carregar outro dispositivo.

ANTES DO SEU REGRESSO DA VIAGEM

1

TRANSFIRA OS SEUS DADOS PARA A REDE DA SUA ORGANIZAÇÃO ATRAVÉS DE UMA LIGAÇÃO SEGURA.

Caso contrário, use a sua caixa de correio eletrónico para receber ficheiros cifrados (que serão excluídos no seu regresso). Em seguida, exclua-os de sua máquina, de forma segura com o software fornecido para esse fim.

2

REMOVA O HISTÓRICO DAS SUAS CHAMADAS E REGISTOS DE NAVEGAÇÃO NA WEB.

Incluindo terminais de roaming de países terceiros (telemóvel e tablet) do seu computador.

DEPOIS DA VIAGEM

1

ALTERE AS SUAS PALAVRAS-CHAVE QUE UTILIZOU DURANTE A VIAGEM.

Podem ter sido intercetadas sem o seu conhecimento.

2

VERIFIQUE OS SEUS DISPOSITIVOS.

Não ligue os dispositivos à sua rede antes de ter pelo menos um antivírus e um teste de anti-spyware realizado.

3

LIMPE O HISTÓRICO DO SEU NAVEGADOR, COOKIES E OUTROS DADOS TEMPORÁRIOS DOS SEUS DISPOSITIVOS.

Ao limpar o histórico de navegação em browsers (ex. Internet Explorer, Chrome, Firefox) de computadores e dispositivos móveis não permite deixar sinais das suas ações.

4

EXECUTE O SEU ANTIVÍRUS EM TODOS OS DISPOSITIVOS QUE LEVOU NA VIAGEM.

Ao correr o antivírus permite que sejam detetados erros de segurança e até é possível eliminar vírus.

CNCS
Centro Nacional
de Cibersegurança
PORTUGAL

PROTEJA-SE POR SER CIBERSEGURA/O.
LEIA ESTE PASSAPORTE HOJE.

Siga-nos em www.cncs.gov.pt