MANUAL

Proficiência Digital – Nível Básico

CD_B2_D

Proteger dispositivos e dados pessoais e identificar riscos para a saúde e meio ambiente.

25 horas

SÍLVIA CUNHA

Índice

Introdução

Neste manual, o formando irá encontrar informações essenciais para fortalecer os conhecimentos de proficiência digital, concentrando-se na salvaguarda de dispositivos, dados pessoais e na identificação de riscos potenciais para a saúde e o meio ambiente.

Nos dias atuais, a tecnologia está entrelaçada às nossas vidas, facilitando a comunicação, o acesso à informação e a realização de tarefas diárias. No entanto, essa conexão constante também traz consigo desafios significativos. A proteção de nossos dispositivos contra ameaças digitais e a preservação de nossos dados pessoais tornaram-se preocupações primordiais em um mundo cada vez mais conectado.

Além disso, a crescente dependência da tecnologia também coloca-nos diante de riscos que podem impactar nossa saúde e o ambiente ao nosso redor. Identificar esses perigos e adotar práticas para mitigá-los são passos fundamentais para uma utilização consciente e responsável da tecnologia.

Este manual foi cuidadosamente elaborado para oferecer orientações claras e práticas sobre como proteger seus dispositivos eletrônicos, salvaguardar seus dados pessoais e reconhecer os potenciais riscos à saúde e ao meio ambiente decorrentes do uso da tecnologia.

Esperamos que este guia seja uma fonte valiosa de informações, capacitando-o(a) a adotar medidas proativas para garantir sua segurança digital e bem-estar, além de contribuir para a preservação do meio ambiente.

Conhecimentos a adquirir

- Identificar riscos e ameaças em ambientes digitais.
- Selecionar formas de proteger os dispositivos e conteúdo digital.
- Identificar riscos e ameaças da utilização de tecnologias digitais para a saúde e bem-estar.
- Identificar os impactos ambientais decorrentes das tecnologias digitais e da sua utilização.

Identificação de Riscos e Ameaças em Ambientes Digitais

- Quantas vezes está online e se questiona se deve realmente fazer aquele download da última versão do programa que lhe é sugerido de modo tão apelativo?

- Quantos emails citam o seu nome e cuja proveniência lhe é absolutamente desconhecida?

Distinguir Riscos e Ameaças em Ambientes Digitais

Para uma segura navegação na Internet, temos de estar conscientes das ameaças e dos riscos. Através desta porta que abrimos para o mundo pode "entrar" alguém com intenções menos boas. A Internet é isso mesmo, um enorme universo, mas a que todos acedemos.

E dentro deste "todos" cabe tudo: profissionais à procura de informações credíveis para desenvolver os seus trabalhos, pessoas à procura de entretenimento, outras que ali vão apenas para conversar com amigos e outras ainda para combater a monotonia.

O problema nasce quando encontramos quem ali se encontre apenas para beneficiar através do prejuízo alheio. Falamos de hackers, de ladrões de informação, de dados e, por vezes, de coisas que nunca julgávamos possível, como por exemplo, a nossa própria intimidade.

Para que possamos, então, integrar o mundo global ao qual mesmo que quiséssemos não conseguiríamos escapar, é necessário estarmos conscientes dos seus perigos. Poder-se-ia dizer que é como aprender a andar na rua.

Para nos mantermos seguros, nada melhor do que conhecermos as ameaças existentes e como o nosso próprio comportamento nos pode tornar vulneráveis.

Identificação de Riscos e Ameaças Nas Marcas

Phishing

Consiste no envio de mails supostamente confiáveis, mas que roubam dados confidenciais. Enganam os utilizadores para obter palavras-passe, códigos e informação que garante o acesso de piratas informáticos a coisas tão importantes como, por exemplo, o seu cartão de crédito.

Malware

Trata-se de um software que tem como finalidade aceder sem qualquer tipo de autorização a um equipamento e portanto ao seu conteúdo. Não é difícil imaginarmos os estragos que poderá causar acedendo, por exemplo, a informação que desejamos que seja confidencial.

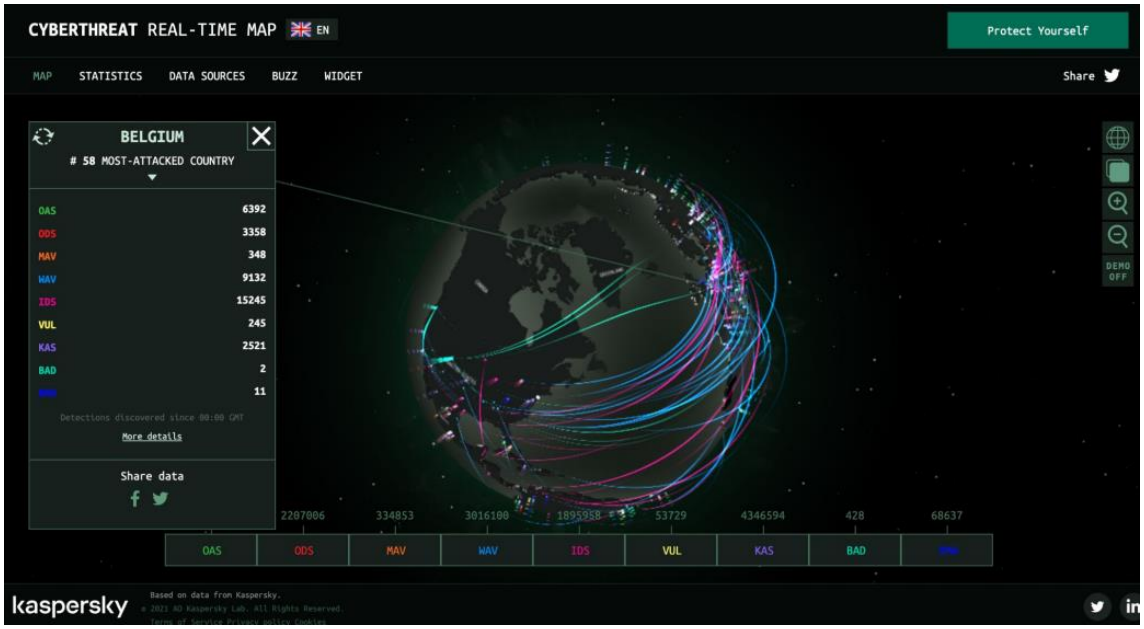
Crime Cibernético

O crime cibernético encaixou uns gritantes 450 mil milhões de dólares de receitas no ano passado, com dois mil milhões de registos perdidos ou roubados em todo o mundo.

Caleb Barlow, especialista em segurança, denuncia a insuficiência das nossas estratégias atuais para proteger os nossos dados.

A solução? Precisamos de reagir ao crime cibernético com o mesmo esforço coletivo que aplicamos numa crise de cuidados de saúde, partilhando atempadamente as informações sobre quem está infetado e como a doença se está a espalhar. Se não partilharmos, diz ele, estamos a contribuir para o problema

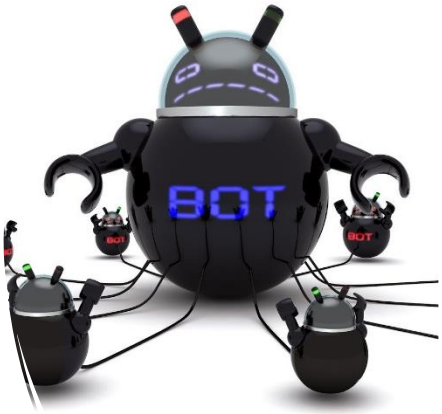
Ataques globais em tempo real



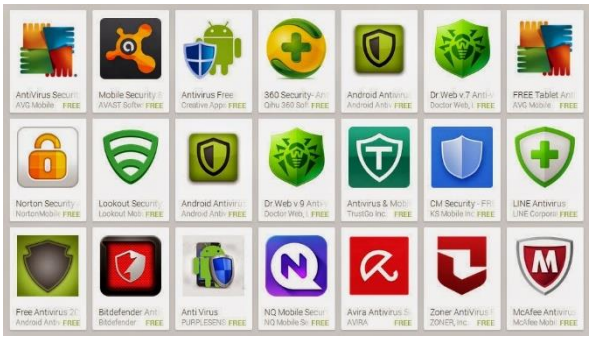
BAD (Botnet Activity Detection)

A deteção da atividade do Botnet mostra estatísticas sobre endereços IP identificados de vítimas de ataques DDoS e servidores C&C de botnet. Estas estatísticas foram adquiridas com a ajuda do sistema DDoS Intelligence deste software.

- DDoS: ataques de rede distribuídos muitas vezes são chamados de ataques de negação de serviço distribuído.



MAV (Mail Anti-Virus)



Mostra o fluxo de deteção de malware durante o scan do Mail Antivírus quando aparecem novos objetos numa aplicação de correio eletrónico (Outlook, The Bat, Thunderbird). O MAV analisa as mensagens recebidas e chama a OAS ao guardar anexos num disco.

- OAS: verificação de acesso

WAV (Web Anti-Virus)

Mostra o fluxo de deteção de malware durante o scan do Web Antivírus quando a página HTML de um website abre ou quando um ficheiro é descarregado. Verifica as portas especificadas nas definições do Antivírus da Web.

IDS (Intrusion Detection System)

Mostra o fluxo de deteção de ataques de rede.

Medidas de Segurança e Proteção Digital

Proteger os dispositivos e conteúdo digital

Existem 4 pilares da segurança da informação:

- 1. A integridade - os dados mantêm-se inalterados.
- 2. A confidencialidade - só acede à informação quem autorizamos. 3. A autenticidade - fontes fidedignas.
- 4. A disponibilidade - acesso aos dados limitado apenas a utilizadores autorizados.

Se estes quatro princípios forem observados, será certo que a capacidade de enfrentar riscos, no ambiente digital, estará reforçada, proporcionando-lhe um tipo de segurança diferente e muito mais robusto.

Outras das medidas importantes, dizem respeito à realização de um backup de segurança para a proteção de informação, ao recurso a criptografia e à adoção de uma política de controlo de acessos por parte dos utilizadores.

Internet of Things (IoT)

Internet das Coisas é a tradução literal da expressão em inglês Internet of Things (IoT). Em português, o nome mais adequado poderia ser algo como "Internet em Todas as Coisas", mas, no fundo, isso não tem importância: o que vale é entender e usufruir da ideia.

- Quais os objetos que usa para se ligar à internet?
- Smartphone, tablet, notebook, computador. Utiliza pelo menos um destes dispositivos, certo?

  Mas há outros equipamentos que se conectam à internet para realizar atividades específicas, como por exemplo, câmaras de segurança que, por estarem online, permitem que uma pessoa monitorize a sua casa remotamente ou vigie a sua loja quando o estabelecimento estiver fechado.

  Outro exemplo: smart TVs. Com elas, você pode aceder a serviços como Netflix, YouTube e Spotify de modo direto, sem ter que ligá-las ao seu PC ou smartphone.

Segurança e Risco da Internet das Coisas

Se a Internet das Coisas descreve um cenário em que quase tudo está conectado, é claro que há riscos associados. É por essa razão que as convenções que tratam do conceito devem ter em consideração vários parâmetros preventivos e corretivos, especialmente sobre segurança e privacidade.

Imagine os transtornos que uma pessoa teria se o sistema de monitorização de sua casa fosse desligado inesperadamente por causa de uma falha de software ou por uma invasão conduzida por hackers.

Os riscos não são apenas individuais. Problemas de ordem coletiva também podem surgir. Pense, por exemplo, numa cidade que tem todos os semáforos conectados.

Políticas de Privacidade

Formas de Proteção de Dados Pessoais e Privacidade

Quando pensa nos seus dados pessoais, deve ter em conta que as informações que são recolhidas, ficam disponíveis e podem ser consultadas. Pensando num exemplo extremo, um criminoso poderá utilizar os seus dados, para realizar esquemas de phishing, para usar a sua identidade ou ainda para realizar outros crimes.

O melhor a fazer, será sempre começar por ler as políticas de privacidade das páginas ou entidades que visita e não partilhar mais do que necessita. Menos informação partilhada é sempre sinónimo de maior segurança. Deve ter em conta a autorização que dá ou não, relativamente ao acesso de cookies aos equipamentos, sendo que nem todos requerem esta autorização.

Recorde-se que os cookies, se destinam a memorizar as preferências que são detetadas nos equipamentos. Quando lhe é pedida a referida autorização, o sítio de web deverá, obrigatoriamente, explicar como poderão ser usadas as informações recolhidas e de que forma as poderá desativar.

Medidas de Proteção

Seja no âmbito individual, seja no universo empresarial, para nos protegermos e aos dados que desejamos manter privados, há, então, uma série de medidas que deveremos adotar sob pena de permitirmos o acesso de pessoas indesejáveis a informação que nos diga respeito, à nossa empresa ou àquela em que trabalhamos com prejuízos que muitas vezes não conseguimos sequer calcular.

Na União Europeia (UE) há regras que garantem a proteção de dados pessoais sempre que, por exemplo, fazemos compras online ou nos candidatamos a uma vaga de emprego ou pedimos um empréstimo ao banco.

Estas regras são aplicadas não só às empresas e organizações que estão localizadas no espaço europeu, mas também àquelas que prestam serviços e bens ao nosso espaço comunitário. Como exemplo desta realidade temos o Facebook e a Amazon.

Proteção de Dados Pessoais

Quando pensa nos seus dados pessoais, deve ter em conta que as informações que são recolhidas, ficam disponíveis e podem ser consultadas. Pensando num exemplo extremo, um criminoso poderá utilizar os seus dados, para realizar esquemas de phishing, para usar a sua identidade ou ainda para realizar outros crimes.

O melhor a fazer, será sempre começar por ler as políticas de privacidade das páginas ou entidades que visita e não partilhar mais do que necessita. Menos informação partilhada é sempre sinónimo de maior segurança.

Cookies

Os cookies (testemunhos de conexão) são ficheiros de texto que um determinado site nos pede para instalar no nosso equipamento através do nosso programa de navegação. Servem para memorizar as nossas preferências e acompanhar a nossa navegação na net. Deste modo habilitam-se a mostrar-nos publicidade seletiva com base nas nossas preferências.

Antes de serem instalados têm de ser autorizados por nós e o respetivo site terá de explicar-nos como irá usar a informação que aqueles irão recolher, dando-nos também a possibilidade de retirarmos o nosso consentimento. Há, no entanto, cookies que não requerem a nossa utilização. São os que se destinam apenas a transmitir uma comunicação ou a fornecer um serviço online solicitado por nós.

Proteção de Privacidade

Para garantir a sua segurança e privacidade online, deve saber mais sobre gestão de cookies. Os cookies consistem em etiquetas de software, que ficam armazenadas nos seus equipamentos, através do browser. Têm como objetivo guardar informações acerca das suas preferências. Nesse sentido, os cookies servem para identificar a utilidade, o interesse e o número de utilizações dos seus websites, possibilitando uma navegação mais rápida e eficiente.

- Existem dois tipos de cookies: Os cookies permanentes e os cookies de sessão ou temporários.

Cuidados a ter online

A sua segurança online é absolutamente fundamental. Não pode, de modo algum, permitir que qualquer programa aceda às suas informações ou dados pessoais. Deve ter esta noção sempre em mente, quando visita uma página. É necessário também cultivar essa sensibilidade, para que saiba estar alerta, de forma a proteger-se o mais possível, de uma invasão à sua privacidade.

Menos é mais. Quanto menos revelar ou menos deixar disponível a que seja revelado, mais seguro estará. Para esse efeito, deve começar por assegurar a proteção das suas contas.

Palavra-Passe

Para garantirmos o mais possível que os nossos dados e a nossa informação se encontram a salvo, temos que apostar na criação de diversas palavras-passe, para aceder a diversos sites e no cuidado de nelas integrarmos combinações complexas com números, caracteres, maiúsculas e minúsculas, entre outros. Será escusado dizer que nunca é aconselhável partilhar a palavra-passe de acesso ao email pois é a partir deste que se tem acesso a todas as outras páginas e informações.

Ligações Seguras

Uma vez online, há algumas noções que nos são essenciais e que devemos manter sempre bem presentes. Saiba que todas as ligações podem ser hackeadas, mesmo quando o URL do site começa por http, indicando que a ligação é segura. Há quem pense, por exemplo, que ao adquirirmos um equipamento (computador ou telefone) estamos livres de perigos, o que não é verdade. A segurança do novo dispositivo não está imediatamente configurada ao máximo, pelo que quando adquirimos qualquer equipamento devemos logo verificar as configurações de segurança e realizar as adaptações e atualizações necessárias.

Se mantiver o software atualizado e nunca clicar em links ou abrir anexos de emails suspeitos e fizer backups frequentes e recorrer a um antivírus estará sempre mais seguro e, claro, se for vítima de um ataque denuncie imediatamente a situação às autoridades (Polícia Judiciária, Centro Nacional de Cibersegurança).

Cuidados a Adotar

Há certas medidas que não convém adotar, como por exemplo tentar cancelar a subscrição de um spam. Em vez de clicarmos em qualquer link que estas mensagens possam apresentar, o melhor será marcarmos o email como spam ou lixo e com o phishing devemos fazer exatamente o mesmo. Quando estas mensagens nos chegam via SMS ou através de uma qualquer rede social, o melhor será optarmos por bloquear o número ou o remetente.

No que diz respeito à utilização do telemóvel há outra medida importante no que toca à segurança dos nossos dados e que é facilmente aplicável. Dependendo do fabricante e do modelo pode optar por várias formas de desbloquear o seu equipamento. A melhor proteção consiste na escolha de uma palavra-passe complexa, mas a escolha dos dados biométricos (desbloqueio através da impressão digital, do reconhecimento da íris ou facial) também é Segura.

O código pin representa uma proteção razoável (no caso de escolha de seis números ou mais) mas atualmente desaconselhada (no caso de quatro dígitos) por ser mais facilmente descoberto. O mesmo passa-se relativamente ao desbloqueio através do desenho de uma senha padrão no ecrã, já que o rasto da impressão digital pode ficar marcado no ecrã.

Saúde e Bem-estar

O que podemos fazer, para nos protegermos, da assoberbante enchente de informação e de solicitações que nos chegam todos os dias? As várias solicitações que recebemos, podem conduzir a uma escalada de ansiedade, de falta de descanso e de stress.

A saúde e o bem-estar em ambientes digitais, podem preservar-se de inúmeras formas. Devemos começar, obrigatoriamente, por proteger a nossa privacidade, que poderá ser utilizada para nos prejudicar em termos práticos.

Pensar que alguém poderá vigiar os seus passos, saber mais acerca de si do que deseja ou até aceder à sua informação, é em si bastante perturbador. Agora imaginemos as várias áreas da nossa vida, em que isto poderá suceder. O stress aumenta. Por essa razão, há um conjunto de práticas, que pode adotar, para proteger a sua saúde e bem-estar, em várias áreas da sua vida digital.

Na utilização do seu smartphone, pode começar por proteger os seus dados, alterar o nome do dispositivo, limitar o acesso à sua localização, bem como às fotos e contactos. Por outro lado, procure deter as notificações e eliminar as aplicações que já não usa. Descansar e tirar tempo livre dos seus dispositivos, é também essencial.

Pode definir um tempo limite para utilizar as aplicações que mais ocupam o seu tempo ou definir o intervalo horário durante o qual não utiliza o telefone, como por exemplo, a partir da hora do jantar.

No que diz respeito às redes sociais, a melhor opção será a de adotar perfis privados, de modo a que sejam só acessíveis, às pessoas que autoriza. É como acontece em nossas casas. Só entra quem é convidado.

Lembre-se sempre que, quanto mais tempo passar numa rede social, mais ela percebe acerca de si. Este tipo de plataformas, recorre a estudos psicológicos, que avaliam constantemente, as suas preferências, estados de espírito, vulnerabilidades pessoais e etc.

Quanto ao uso do computador, procure manter a caixa de e-mail o mais vazia possível. Deve eliminar o que não necessita e apagar todos os que, a dada altura, transportaram informação acerca de si. Se quiser guardar essa informação, o melhor será copiá-la para um documento. A partir daí, poderá obter uma maior sensação de tranquilidade.

Por último, nunca é demais recordar, que o seu software, deverá estar sempre atualizado, para o proteger de vírus e outro malware, reduzindo assim as suas vulnerabilidades e o perigo de ser invadido.