Co-funded by the
Erasmus+ Programme
of the European Union

Módulo de Aprendizagem

Proteção de *Hardware* e *Software*

Projeto: B-SAFE
Número: 2018-1CZ01-KA204-048148
Nome do autor: EDIT VALUE®
Última data de processamento: 28.10.2020

Co-funded by the
Erasmus+ Programme
of the European Union

Proteção de *Hardware* e *Software*

Introdução

O *hardware* e o *software* estão constantemente interligados isto porque, sem *software*, o *hardware* de um computador não teria qualquer função.

A digitalização está a transformar a economia em todo o mundo. Seja no trabalho ou na vida privada, há sempre algumas questões relativas ao *hardware* e ao *software* que nos afetam a todos. Além disso, o *hardware* e o *software* devem ser atualizados ou substituídos regularmente devido à existência de riscos graves para as organizações e também para a sociedade em geral.

Neste módulo de aprendizagem serão apresentados os ataques mais comuns ao *hardware* e *software* e o que se pode fazer para garantir a proteção contra esses ataques.

Sabias que a maioria dos problemas informáticos estão ligados ao *software*? Por exemplo, o *software* de um computador pode falhar por múltiplas razões, já que as infeções por vírus e/ou *malware* no computador são muito comuns, uma vez que as pessoas tendem a descarregar alguma coisa ou clicar em algo que tenha como objetivo causar danos ao dispositivo. Há muitas formas de corrigir problemas de *software*, tais como desinstalar, reinstalar e atualizar um programa, utilizar *software* antivírus atualizado e verificar o *website* do fabricante em busca de *patches* (ou seja, correções). Mas há mais que podemos fazer, como será demonstrado neste módulo de aprendizagem.

Relevância prática – Assim poderás aplicar os conhecimentos e competências aqui adquiridos

Com as aprendizagens concretizadas neste módulo, será possível identificar os tipos mais comuns de ataques ao *hardware* e *software*, bem como saber quais as dicas e recomendações a aplicar regularmente para ter uma proteção melhor e mais segura do *hardware* e *software.*

Co-funded by the
Erasmus+ Programme
of the European Union

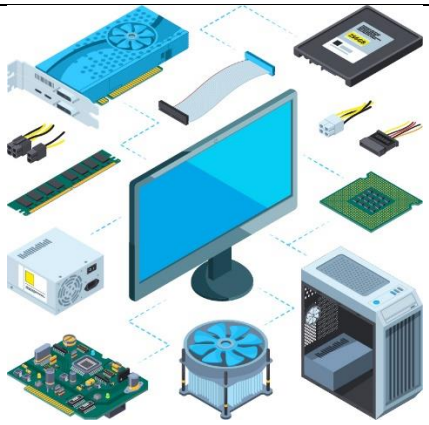
1.Desenvolver conhecimento- *Hardware*, *software* e os ataques mais comuns

A digitalização está a transformar as nossas economias a nível global. Apesar da quantidade de benefícios que surgem com este fenómeno, existem também **ameaças avançadas para a segurança digital que afetam a segurança e a privacidade** das nossas casas, automóveis, empresas e até das nossas redes. Isto porque estamos constantemente a usar dispositivos digitais na vida quotidiana, uma tendência que está a aumentar ininterruptamente.
Por conseguinte, o *hardware* e o *software* destes dispositivos devem ser **atualizados ou substituídos** frequentemente devido à existência de riscos e ameaças graves para a sociedade em geral.

Mas comecemos do zero: A que é que nos referimos exatamente quando falamos de *hardware* e *software*? No quadro abaixo encontra-se uma definição detalhada de *hardware* e *software*.

Definição
O ***hardware*** é qualquer **componente físico** utilizado no ou com o dispositivo, enquanto o *software* é o está dentro do disco rígido do computador, *smartphone* e/ou tablet. O *hardware* é a **parte física do computador ou *smartphone***, enquanto o *software* recolhe e processa dados no disco rígido do dispositivo. Alguns exemplos de componentes de *hardware* são: processador de computador (CPU), disco rígido, placa principal, monitor de computador, impressora ou um rato. O ***software*** é a **parte lógica** do seu computador ou *smartphone*; não pode ser tocado por ser imaterial. Ainda assim, **todo o *software* utiliza pelo menos um componente de *hardware* para funcionar**. Pode imaginar o *software* como um conjunto de instruções que diz a um dispositivo exatamente o que fazer. Pode assumir a forma de um programa ou de dados. Por exemplo, um jogo de vídeo ou o Microsoft Outlook.

Para que fique ainda mais claro, demonstram-se, na tabela abaixo, as principais diferenças entre *hardware* e *software*:

	Hardware	*Software*
		
Função	O *hardware* é uma **parte física** de um dispositivo físico que é responsável pelo processamento de dados/informações	O *software* é um **conjunto de instruções** que diz a um computador exatamente o que fazer

Co-funded by the Erasmus+ Programme of the European Union

	O *hardware* **não funciona sem qualquer *software***	O *software* é **responsável por fazer funcionar o *hardware***
Características	O *hardware* é composto por dispositivos eletrónicos físicos que podemos ver e tocar O *hardware* não pode ser afetado por vírus informáticos	É possível ver e utilizar o *software* mas não é possível tocar-lhe O *software* é **afetado por vírus informáticos**
Ciclo de vida	Pode ficar fisicamente danificado	Pode tornar-se obsoleto
Inicialização	Funciona assim que o *software* é instalado	Tem de ser instalado no *hardware* para funcionar
Manutenção	As peças podem ser transferidas de um lugar para outro	Pode ser reinstalado e transferido
Exemplos	Rato, CPU, monitor, impressora, disco rígido, etc	Microsoft Word, Firefox, Skype, Adobe Reader, etc

Como podemos ver na tabela anterior, ***hardware* e *software* estão interligados** e sem o *software*, o *hardware* de um computador não teria qualquer função.

A proteção de *hardware* e *software* tornou-se um tema importante para todos, especialmente hoje em dia. Mas porque é que é esse o caso? Na tabela abaixo, podemos ver três objetivos principais da proteção de *hardware* e *software*.

Proteção de *hardware*	Proteção de *software*
1. O *hardware* do computador pode ser bastante frágil (por exemplo, calor, água, utilização inadequada e acidentes físicos causados por pessoas são as maiores ameaças para a segurança física de um computador)	**1.** As atualizações regulares de *software* têm muitas vantagens, tais como a prevenção de *bugs* de computador e prevenção de debilidades nos programas de *software* ou sistemas operativos
2. O *hardware* deve ser devidamente limpo de modo a protegê-lo de calor excessivo	**2.** As atualizações de *software* ajudam a lidar com as falhas/vulnerabilidades de segurança
3. Alguns incidentes como um roubo ou queda de água no *hardware* podem causar perda/roubo de dados, danificar o sistema e estragar ficheiros de dados	**3.** O *software* ajuda a proteger os dados/ informações preciosas contra fontes externas de *malware*

Por conseguinte, a segurança do *hardware* e *software* desempenha um papel crucial na garantia da confiança, integridade e autenticidade. **Vejamos agora a alguns exemplos que clarificam porque é que a proteção de *hardware* e *software* é tão importante!**

Exemplo
Sabias que, em 2011, a Sony Pictures sofreu um ataque de um grupo de *hacktivistas* que divulgou cerca de 1 milhão de contas de utilizadores, incluindo dados pessoais (palavras-passe, e-mails, endereços de casa, datas de nascimento, etc.) que quebraram a política de privacidade do seu serviço?

Co-funded by the Erasmus+ Programme of the European Union

Em 2017, o gigante HBO foi atacado e o *hacker* lançou o guião de um episódio de uma série televisiva muito popular (Game of Thrones) que não tinha sido transmitida e também obteve acesso a documentos financeiros, lista de contactos do elenco e da equipa técnica da série e outras informações confidenciais.
Estes tipos de incidentes podem ser evitados se se tiver uma forte proteção de *software* e *Hardware*.

2. Aplicar conhecimento

Exercício de ESCOLHA MÚLTIPLA

Objetivo específico associado: OE_Proteção de *hardware* e *software*_01_01

Situação: O que significa *hardware* e *software*?
Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- O *software* é uma parte do computador em que se pode tocar.
- O *hardware* pode ser afetado por vírus informáticos.
- O *software* é responsável por fazer o *hardware* funcionar.
- O *hardware* e o *software* só funcionam se estiverem juntos.

Exercício de ESCOLHA MÚLTIPLA

Objetivo específico associado: OE_Proteção de *hardware* e *software*_01_02

Situação: Relativamente à proteção de *hardware* e *software*, é favor selecionar as frases corretas.
Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- Os ataques mais comuns ao *hardware* são maioritariamente causados por fontes externas.
- A proteção de *software* deve ser feita regularmente.
- Os ataques de *software* são os mais comuns, pelo que se deve procurar múltiplas proteções de *software*.
- O *software* deve ser protegido por algum antivírus.

2.Desenvolver conhecimento - Melhor proteção do *hardware*

Agora que sabemos o que é *hardware* e *software* e porque estes devem ser protegidos, nos próximos dois capítulos serão abordados os ataques típicos a *hardware* e *software* e medidas para evitar ambos.

Nas páginas seguintes, serão apresentados os ataques mais comuns a *hardware* e, para garantir a melhor segurança dos equipamentos, serão cedidas também algumas dicas e recomendações para se prevenir problemas de *hardware*.

Mas, antes de mais, é preciso saber o que é a proteção do *hardware* e quais são os ataques mais comuns a *hardware*.

Co-funded by the Erasmus+ Programme of the European Union

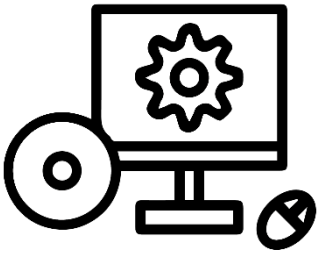
A **proteção de *hardware*** está relacionada com a **proteção dos dispositivos físicos** que devem ser executados por uma pessoa.

Mas quais são os ataques mais comuns a *hardware*?

Existem três tipos de ataques que ocorrem mais frequentemente. Os dois mais comuns estão apresentados na tabela que se segue:

HARDWARE	
Acidentes físicos	***Modding***
Acidentes físicos tais como queda de água numa componente física ou uso impróprio por parte de pessoas. Este tipo de problemas de *hardware* pode constituir uma ameaça à segurança física do computador.	Modificar *hardware*, *software* ou qualquer outra coisa para desempenhar uma função que não tenha sido originalmente concebida ou pretendida pelo *designer*/futuro proprietário original do *hardware*

Algumas das principais consequências dos ataques comuns ao *hardware* são:

Modding 	As **modificações maliciosas de *hardware*** por parte de pessoas internas representam uma ameaça séria. Por conseguinte, é importante conhecer a fonte original de onde vêm os componentes de *hardware*. Por exemplo, componentes de infraestruturas críticas como microprocessadores podem estar dentro de um computador para o controlar.
Acidentes físicos 	**O *hardware* pode ser muito frágil e também muito valioso**. Calor, humidade, vibração, extremos de temperatura, poeira, água e acidentes com componentes físicos são na realidade as maiores ameaças para a segurança física de um computador. Por conseguinte, deve manter-se todo o *hardware* devidamente limpo, longe de fontes de calor excessivo e manter os líquidos longe dos computadores, *smartphones* e *tablets*.

Depois de sabermos o que pode acontecer ao *hardware* é importante mencionar algumas dicas e recomendações para manter o *hardware* seguro.

Seguem-se **alguns passos** para proteger o *hardware* na seguinte lista:

1. **As modificações de *hardware* são ilegais** a menos que haja consentimento na realização desse tipo de alterações. Por exemplo, podem fazer-se algumas modificações num computador a fim de melhorar algo (velocidade, capacidade, etc). Devido a isso, deve-se **evitar comprar componentes de *hardware* de fontes/países de risco** como plataformas *online* que ainda são desconhecidas do público em geral, mesmo que o preço seja muito baixo e atrativo porque,

normalmente, o *hardware* que vem de fontes não confiáveis pode constituir uma ameaça à segurança;

2. Existem também **sistemas especiais de rastreio** que podem ser utilizados, por exemplo, se o *hardware* for roubado ou perdido;
3. A fim de ter cuidado com o *hardware*, deve-se sempre **instalar e utilizar *software* de segurança atualizado**. Esta dica será explorada com maior detalhe neste documento posteriormente, depois de apresentarmos a temática sobre proteção de *software*;
4. **Deve-se evitar colocar o *hardware* em superfícies altas e longe de fontes de calor, água, circuito elétrico;**
5. Recomenda-se que se **limpe muito suavemente o *hardware*** com um pano seco ou uma ferramenta especial, como uma escova de cabo longo e cerdas macias, toalhetes que se podem comprar em lojas específicas que vendam material de *hardware*. Esta dica deve ser mantida como regra de manutenção e proceder-se à limpeza tantas vezes quantas forem necessárias.

2. Aplicar conhecimento

Exercício de ESCOLHA MÚLTIPLA

Objetivo específico associado: OE_Proteção de *hardware* e *software*_02_01

***Situação*: O que significa proteção de *hardware*?**
Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

1. A proteção do *hardware* depende apenas das pessoas.
2. A proteção do *hardware* é o que uma pessoa pode fazer para proteger os componentes físicos.
3. A proteção do *hardware* não pode ser feita apenas por uma pessoa.
4. A proteção do *hardware* está apenas relacionada com a implementação de ações/medidas físicas.

Exercício de ESCOLHA MÚLTIPLA

Objetivo específico associado: OE_Proteção de *hardware* e *software*_02_02

***Situação*: O que pode acontecer na eventualidade de um ataque de *hardware*?**
Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

1. O ataque mais comum ao *hardware* está relacionado apenas com modificações físicas não autorizadas.
2. Os acidentes físicos acontecem mais frequentemente porque as pessoas por vezes têm comportamentos/ações irresponsáveis.
3. Os ataques ao *hardware* podem comprometer a informação pessoal e a segurança física do proprietário do *hardware*.
4. Os ataques ao *hardware* estão relacionados com incidentes físicos e com a modificação de *hardware*.

Exercício de ESCOLHA MÚLTIPLA

Objetivo específico associado: OE_Proteção de *hardware* e *software*_02_03

Situação: Quais são as recomendações que podem ser implementadas relativamente à proteção de *hardware*?
Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

1. Manter o *hardware* limpo e longe de fontes de calor e água.
2. A proteção do *hardware* deve ser complementada com a proteção do *software*.
3. Evitar comprar componentes de *hardware* de fontes/países de risco devido a possíveis alterações indesejadas.
4. As pessoas podem usar sistemas especiais de rastreio e dispositivos de autodestruição, se necessário.

3.Desenvolver conhecimento - Melhor proteção de *software*

É também pertinente saber mais sobre proteção de *software*, especialmente porque há muitos ataques que podem acontecer. Hoje em dia, todos nós usamos vários tipos de *software* e, por vezes, nem sequer nos apercebemos disso.

Agora que sabemos o que é a proteção de *hardware*, devemos também conhecer a definição de proteção de *software*.

A **proteção de *software*** é uma **metodologia e arquitetura de segurança de redes informáticas** que combina dispositivos de segurança e proteção defensiva de fontes (externas e internas). A proteção de *software* requer uma combinação de técnicas relacionadas com diferentes *software*s. A proteção de *software* é agora um aspeto crítico não só para empresas mas também para indivíduos.

Mas, quais são os ataques mais comuns ao *software*?

Embora existam muitos ataques ao *software*, apresentam-se na tabela abaixo os mais comuns.

SOFTWARE			
***Trojan* (Cavalo de Tróia)**	***Malware***	**Vírus**	***Phishing***
Programa de computador que obtém acesso a um computador ou sistema, camuflado sob a forma de *software* normal a fim de causar danos aos processos do sistema, dados do disco rígido, etc. Introduz-se no dispositivo principalmente através de anexos de	Pode incluir *spyware*, *ransomware*, vírus e *worms*. O malware ocorre normalmente devido a cliques em links perigosos ou anexos de *email* que instalam *software* de risco	Programa de computador concebido para infetar outros programas informáticos, destruindo dados essenciais do sistema e tornando as redes inoperacionais	Prática de envio de comunicações fraudulentas que parecem vir de uma fonte de confiança, geralmente através de correio eletrónico. O objetivo é roubar informações/dados a alguém (como cartão de crédito, informações de login, etc.)

e-mail.			
Ransomware	***Worms***	***Spyware***	***Cryptojacking***
Bloqueia o acesso aos componentes chave da rede do utilizador	Programa de *malware* que se reproduz para se espalhar para outros computadores	*Software* que permite a um utilizador obter informações sobre as atividades informáticas de outro	Utilização não autorizada do computador de outra pessoa para minar moedas criptográficas. Estes ataques tendem a ser feitos através de uma ligação maliciosa num e-mail, um *website* infetado ou publicidade *online*

A título de exemplo, as **três principais consequências dos ataques comuns ao *software*** são:

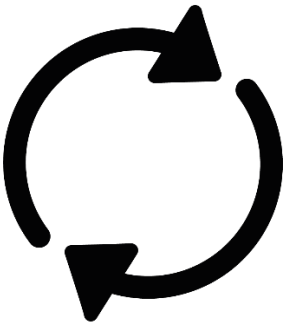
Bugs	Uma fonte comum de defeitos de segurança do *software*. Alguns *bugs* representam vulnerabilidades de segurança que podem resultar numa fuga de informação ou num acesso não autorizado.
Autenticação quebrada e falha na proteção de dados	Por vezes, as funções relacionadas com a autenticação estão incorretas e, por isso, podem surgir algumas questões de segurança. Esta situação pode levar a que pessoas não autorizadas acedam às contas dos utilizadores para assumir a sua identidade. Neste caso, as pessoas podem perder informações empresariais cruciais e as suas informações pessoais roubadas podem ser utilizadas para prejudicar o próprio e/ou aos seus clientes.
Perturbação das atividades comerciais	Um ataque ao *software* pode levar um negócio à falência. Além disso, a confiança dos clientes pode ser afetada se souberem que o negócio foi vítima de um ataque.

Explorados os ataques mais comuns ao *software* é preciso saber o que se pode fazer para evitar este tipo de incidentes. Depois de ver alguns dos ataques mais comuns é indiscutível que a proteção do *software* é uma questão chave.

Abaixo, é possível encontrar **algumas dicas** sobre o que se pode fazer para se proteger relativamente aos ataques mais comuns ao *software*:

	Manter as informações pessoais seguras utilizando **múltiplas palavras-passe fortes e fazer cópias de segurança frequentes**. Também é possível encriptar informação. Criar várias **cópias de segurança de todos os dados pessoais importantes**, garantindo que não estão todos armazenados no mesmo

	local/fonte. Manter sempre ***firewalls* de *software***. Para tal, deve-se verificar as definições de *hardware* e ter a *firewall* predefinida ativada juntamente com *software* antivírus respeitável.

	**Instalar atualizações frequentemente** e manter sempre o *software* atualizado. **Instalar um filtro/*software* de *phishing*** na aplicação de e-mail e também no *browser* de internet. Estes filtros não irão conseguir bloquear todas as mensagens de *phishing* mas irão reduzir o número de tentativas de *phishing*. Manter o **sistema operativo e o *software* de segurança atualizado**. **Executar regularmente scans programados** com o *software* antivírus e garantir de que o *software* antivírus e *anti-spyware* são compatíveis.

	**Nunca abrir um anexo de e-mail** ou executar um programa sem ter 100% de certeza que se trata de uma fonte segura. **Verificar as credenciais SSL** do *website* e **nunca usar informação pessoal/sensível** em *websites* que não tenham um certificado SSL válido instalado. Para ver as credenciais SSL do *website* deve clicar no ícone de cadeado num navegador, onde diz "Clique na marca de confiança". **Evitar a utilização de redes públicas.** **Implantar um filtro do *website*** para bloquear *websites* maliciosos. Um filtro de *website* pode ajudar a controlar *websites*, criando uma lista permitida ou uma lista bloqueada. Para mais informações é possível ver neste *website* como proceder: www.currentware.com/web-filter.

Como podemos ver, a **prevenção é a chave** para evitar problemas de *software* e ser proactivo ou, por outras palavras, tomar algumas ações para nos protegermos é sempre a melhor opção.

Co-funded by the
Erasmus+ Programme
of the European Union

Para terminar, é importante ter em mente que os ataques evoluem a cada dia que passa e, por isso, é necessário **mantermo-nos atualizados sobre os últimos ataques e medidas de proteção**. O principal objetivo é mantermo-nos a par do *malware* que existe por forma a garantirmos a nossa segurança.

5. Aplicar conhecimento

Exercício de ESCOLHA MÚLTIPLA

Objetivo específico associado: OE_Proteção de *hardware* e *software*_03_01

Situação: O que significa a proteção de *software*?
Tarefa: Escolher a(s) opção(ões) correcta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

1. A proteção de *software* requer uma combinação de múltiplas técnicas e métodos.
2. A proteção de *software* é, na sua maioria, reativa.
3. A segurança do *hardware* e *software* deve ser uma prioridade mas a proteção de *software* precisa de ser feita com mais frequência.
4. A proteção de *software* é mais importante porque as pessoas utilizam mais o *software* diariamente.

Exercício de ESCOLHA MÚLTIPLA

Objetivo específico associado: OE_Proteção de *hardware* e *software*_03_02

Situação: O que pode acontecer numa situação de ataque ao *software*?
Tarefa: Escolher a(s) opção(ões) correcta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

1. Uma consequência comum de um ataque de *software* é a fuga de informação.
2. Outra consequência comum de um ataque com *software* é o acesso não autorizado.
3. É muito comum ter perdas financeiras no caso de um ataque com *software*.
4. A autenticação quebrada e a falha na proteção acontecem frequentemente ao mesmo tempo.

Exercício de ESCOLHA MÚLTIPLA

Objetivo específico associado: OE_Proteção de *hardware* e *software*_03_03

Situação: Quais as recomendações que podem ser implementadas no tocante à proteção de *software*?
Tarefa: Escolher a(s) opção(ões) correcta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

1. As pessoas devem implementar vários métodos para proteger o *software* e realizar testes de desempenho com a maior frequência possível.
2. Ter *firewalls* atualizados, antivírus, filtros de *phishing* são exemplos de proteção de *software*.
3. Como os ataques estão a tornar-se mais complexos, os métodos de proteção também devem ser atualizados em conformidade.
4. Porque os ataques de *software* estão a evoluir, as medidas de proteção de *software* também devem ser constantemente atualizadas.

Co-funded by the
Erasmus+ Programme
of the European Union

Fontes

Diana, J. (n.d.). *Hardware e Sorfware.* https://www.todamateria.com.br/*Hardware*-e-*software*/

Hossain, F. R. (4 Julho 2018). *Importance of Security in Software Development.* Retirado de https://medium.com/brainstation23/importance-of-security-in-*software*-development-f92669838a90

Para relembrar

A proteção de *hardware* e *software* são aspetos essenciais da segurança, **sendo responsáveis pela preservação de bens valiosos de *software* devido a atividades maliciosas sobre *software***.
Apesar de o ***hardware* e *software* estarem interligados**, e de se saber que sem o *software* o *hardware* de um computador não funcionaria (e vice-versa), *hardware* e *software* são dois conceitos distintos: o ***hardware*** é qualquer **componente físico** usado no ou com um dispositivo, enquanto o ***software*** é a **parte lógica** do computador ou outro dispositivo. Alguns exemplos de *hardware* são a placa principal, monitor de computador, impressora ou um rato e alguns exemplos de *software* são um videojogo ou um programa como o Microsoft Office.
Embora seja impossível evitar a possibilidade de ter um incidente de *hardware* ou *software*, existem múltiplas medidas/ferramentas que devemos seguir para nos prevenirmos da melhor maneira possível. O ***hardware* está exposto a erro humano**, ficando danificado sem os devidos cuidados, como limpeza regular e proteção física contra os elementos (água, calor, frio, etc.). O ***software*** é exponencialmente mais sensível a ameaças externas: **pode ser afetado por ciberataques** como cavalos de Tróia, vírus, ataques de *phishing*, *spywares*, *malwares*, entre muitos outros. Por conseguinte, é crucial que se tomem medidas para minimizar o risco de ameaças cibernéticas. Por exemplo, **devem usar-se múltiplas palavras-passe fortes e cópias de segurança frequentes**, manter ***firewalls* de *software*** e um **antivírus atualizado** bem como implantar um **filtro de *websites*** para bloquear *websites* maliciosos.
Como podemos ver, a **prevenção é a chave** para evitar problemas de *software*, daí que a solução seja a proatividade. Por outras palavras, a melhor opção é sempre tomar algumas ações para se proteger de ameaças de segurança cibernéticas!
Para concluir, é importante ter em mente que os ataques estão em constante evolução e, por isso, é necessário **mantermo-nos atualizados relativamente aos mais recentes comportamentos de segurança e medidas de proteção**.

Co-funded by the
Erasmus+ Programme
of the European Union

As respostas corretas estão assinaladas a negrito

Situação: O que significa *hardware* e *software*?
Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- O *software* é uma parte do computador em que se pode tocar.
- O *hardware* pode ser afetado por vírus informáticos.
- **O *software* é responsável por fazer o *hardware* funcionar.**
- **O *hardware* e o *software* só funcionam se estiverem juntos.**

Situação: Relativamente à proteção de *hardware* e *software*, é favor selecionar as frases corretas.
Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

- Os ataques mais comuns ao *hardware* são maioritariamente causados por fontes externas.
- **A proteção de *software* deve ser feita regularmente.**
- **Os ataques de *software* são os mais comuns, pelo que se deve procurar múltiplas proteções de *software*.**
- **O *software* deve ser protegido por algum antivírus.**

Situação: O que significa proteção de *hardware*?
Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

1. **A proteção do *hardware* depende apenas das pessoas.**
2. **A proteção do *hardware* é o que uma pessoa pode fazer para proteger os componentes físicos.**
3. A proteção do *hardware* não pode ser feita apenas por uma pessoa.
4. A proteção do *hardware* está apenas relacionada com a implementação de ações/medidas físicas.

Situação: O que pode acontecer na eventualidade de um ataque de *hardware*?
Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

1. **O ataque mais comum ao *hardware* está relacionado apenas com modificações físicas não autorizadas.**
2. **Os acidentes físicos acontecem mais frequentemente porque as pessoas por vezes têm comportamentos/ações irresponsáveis.**
3. **Os ataques ao *hardware* podem comprometer a informação pessoal e a segurança física do proprietário do *hardware*.**
4. **Os ataques ao *hardware* estão relacionados com incidentes físicos e com a modificação de *hardware*.**

Situação: Quais são as recomendações que podem ser implementadas relativamente à proteção de *hardware*?
Tarefa: Escolher a(s) opção(ões) correta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

1. **Manter o *hardware* limpo e longe de fontes de calor e água.**
2. **A proteção do *hardware* deve ser complementada com a proteção do *software*.**
3. **Evitar comprar componentes de *hardware* de fontes/países de risco devido a possíveis alterações indesejadas.**

4. As pessoas podem usar sistemas especiais de rastreio e dispositivos de autodestruição, se necessário.

Situação: O que significa a proteção de *software*?
Tarefa: Escolher a(s) opção(ões) correcta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

1. A proteção de *software* requer uma combinação de múltiplas técnicas e métodos.
2. A proteção de *software* é, na sua maioria, reativa.
3. A segurança do *hardware* e *software* deve ser uma prioridade mas a proteção de *software* precisa de ser feita com mais frequência.
4. A proteção de *software* é mais importante porque as pessoas utilizam mais o *software* diariamente.

Situação: O que pode acontecer numa situação de ataque ao *software*?
Tarefa: Escolher a(s) opção(ões) correcta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

1. Uma consequência comum de um ataque de *software* é a fuga de informação.
2. Outra consequência comum de um ataque com *software* é o acesso não autorizado.
3. É muito comum ter perdas financeiras no caso de um ataque com *software*.
4. A autenticação quebrada e a falha na proteção acontecem frequentemente ao mesmo tempo.

Situação: Quais as recomendações que podem ser implementadas no tocante à proteção de *software*?
Tarefa: Escolher a(s) opção(ões) correcta(s) usando o princípio de escolha múltipla: Nenhuma, uma, mais do que uma ou todas as opções podem ser verdadeiras.

1. As pessoas devem implementar vários métodos para proteger o *software* e realizar testes de desempenho com a maior frequência possível.
2. Ter *firewalls* atualizados, antivírus, filtros de *phishing* são exemplos de proteção de *software*.
3. Como os ataques estão a tornar-se mais complexos, os métodos de proteção também devem ser atualizados em conformidade.
4. Porque os ataques de *software* estão a evoluir, as medidas de proteção de *software* também devem ser constantemente atualizadas.