Módulo de Aprendizagem

Unidade de Verificação

Projeto: B-SAFE
Número: 2018-1CZ01-KA204-048148
Nome do Autor: UDIMA
Última data de processamento: 24.8.2020

Funded by the
Erasmus+ Programme
of the European Union

1. As dez maiores ameaças da Internet para os utilizadores

Nesta era digital em que vivemos, a Internet é de fácil acesso e permite a exploração de um mundo virtual onde, ao contrário do mundo real, tudo é acessível. A Internet abriu um novo mundo e traz imensas vantagens, mas também muitos riscos.

1. Conteúdo inapropriado

Existe imenso conteúdo na Internet, e nem todo este conteúdo é socialmente aceitável ou até classificado por idade ou área. Alguns conteúdos podem inclusive ser ilegais, inapropriados, ofensivos ou inadequados para algumas faixas etárias. Qualquer pessoa pode encontrar conteúdo impróprio, perturbador ou explícito que pode ser facilmente acessível a crianças sem supervisão parental.

Muitos *websites* perturbadores não são necessariamente 'ilegais', o que significa que ninguém monitoriza e gere o conteúdo que está disponível *online*. Esse conteúdo pode incluir pornografia, violência, produtos perigosos (tais como armas), racismo ou ódio, sites "pro-ana", isto é, que promovem distúrbios alimentares (como por exemplo a anorexia) ou conteúdo extremista.

2. Roubo de dados

O roubo de dados pessoais e/ou financeiros ocorre através do uso de computadores, servidores e outros dispositivos eletrónicos por forma a obter algum benefício ou causar dano à(s) vítima(s). É ilegal obter deste modo informações sensíveis, nomeadamente números de cartões de crédito não encriptados, detalhes de contas bancárias de indivíduos, palavras-passe, informações armazenadas em empresas, segredos comerciais, propriedade intelectual, código-fonte, informações de clientes ou registos de funcionários.

O cibercriminoso pode aceder aos computadores destes utilizadores através de *spyware*, um *software* que permite a um utilizador obter informações sobre as atividades informáticas de outra pessoa.

3. Roubo de identidade

O roubo de identidade é o ato de roubar informações pessoais e identificativas com o intuito de cometer atos ilegais. Numa primeira fase, o infrator adquire uma identidade digital estrangeira. Isto é frequentemente feito através do roubo de dados eletrónicos (palavras-passe, dados de acesso, etc), normalmente através de cópias não autorizadas (*skimming*), *phishing* enganoso ou *hacking*.

Numa segunda fase, o infrator falsifica a identidade de uma outra pessoa, para benefício próprio e/ou para prejudicar a vítima, por exemplo, fazendo uso do seu nome em redes sociais como o Facebook. A identidade roubada pode ser usada com o intuito de cometer atos ilegais como abrir uma linha de crédito, alugar uma casa, comprar bens ou serviços, cometer fraude ou extorsão relacionada com leilões ou salários.

4. Atenção indesejada

Este tipo de atenção pode ser proveniente de alguém que está simplesmente obcecado com a vítima (ci*berstalking*) ou de alguém cuja intenção é lesar a vítima (ciberbullying).

Por um lado, o *ciberstalking* é a atenção obsessiva indesejada direcionada a uma pessoa em específico, através da Internet. É conduzida com recurso a tecnologia *online* tal como *email*, redes sociais, mensagens instantâneas, dados pessoais disponíveis *online* - tudo na Internet pode ser usado pelos *ciberstalkers* para estabelecer um contacto inapropriado com as suas vítimas. Algumas das técnicas desta prática passam por seguir a pessoa *online*, procurar informação pessoal da mesma de modo obsessivo, observar a pessoa *online* de forma secreta, fazer chamadas e enviar mensagens insistentemente para manipular a vítima, entre outros métodos de abordar a vítima inesperadamente.

Por outro lado, o *ciberbullying* é um crime que ocorre quando as redes sociais ou a Internet são empregues para intimidar, assediar, ameaçar ou denegrir os outros.

5. Golpes e truques

Um tipo de golpe ou truque que é bastante utilizado é o *phishing*, a prática de enviar comunicações fraudulentas que parecem vir de uma fonte de confiança, geralmente através do *email*.

Estas comunicações podem incluir *malware* (*spyware, ransomware,* virus e *worms*), normalmente sob a forma de cliques perigosos ou anexos de *email* que depois instalam *software* de risco.

6. Informação indesejada

Quando usamos a Internet, podemos acabar por encontrar informações que não procurávamos, informação incorreta ou perfis falsos. É possível contactar com estas informações enganosas em vez do que procurávamos ou sem solicitar a mesma.

O meio de comunicação *online* mais popular é o *email.* É muito comum usá-lo na nossa rotina diária e é por isso que este é também um dos meios mais usados para enviar *spam*. Os *emails* falsos são uma ameaça comum, mas também é possível receber estas comunicações enganosas através de mensagens nas redes sociais ou através de diversos sites.

Adicionalmente, é possível encontrar notícias falsas em todo o lado e não apenas quando se usa o *email*. Nas redes sociais também é muito comum encontrar não só notícias falsas mas também identidades falsificadas.

7. Propagação fácil e permanência longa

Informações como fotografias, notícias, etc podem ser divulgadas na Internet em qualquer altura, em qualquer lado, por qualquer pessoa. A partir do momento em que a informação se encontra *online*, permanece lá para sempre, pelo que é necessário ser cauteloso com qualquer informação partilhada *online.*

É também muito fácil espalhar a informação pelo mundo num curto espaço de tempo.

8. Destruição ou modificação de dados

Dados importantes podem ser destruídos ou modificados no computador de um utilizador por forma a causar danos.

Isto pode ocorrer através de vírus, que são programas de computador concebidos para infetar outros programas informáticos, destruindo dados essenciais ao sistema e tornando as redes inoperáveis. Outro exemplo são os *trojans*, que são programas de computador que conseguem aceder ao dispositivo ou sistema, camuflados de *softwares* normais e inofensivos, de maneira a danificar processos do sistema, dados do disco rígido, etc.

9. Desativação do dispositivo
O sistema operativo do computador pode ser atacado por um *trojan*, um programa de computador que consegue obter acesso a um dispositivo ou sistema.

Os *trojans* conseguem camuflar-se, assumindo a forma de *software* regular, de modo a causar danos aos processos do sistema, aos dados do disco rígido, etc. Além disso, os *trojans* infiltram-se nos sistemas maioritariamente através de anexos de *emails*.

10. Ciberterrorismo
O ciberterrorismo é sempre mais severo do que outros comportamentos levados a cabo no ou através do ciberespaço.

Este tipo de crime é um ataque cibernético que tem como objetivo gerar medo ou intimidar a sociedade, com um propósito. Para este fim, o pirata informático utiliza computadores ou redes de comunicação por forma a causar destruição.

2. As dez regras mais importantes para um comportamento seguro na Internet

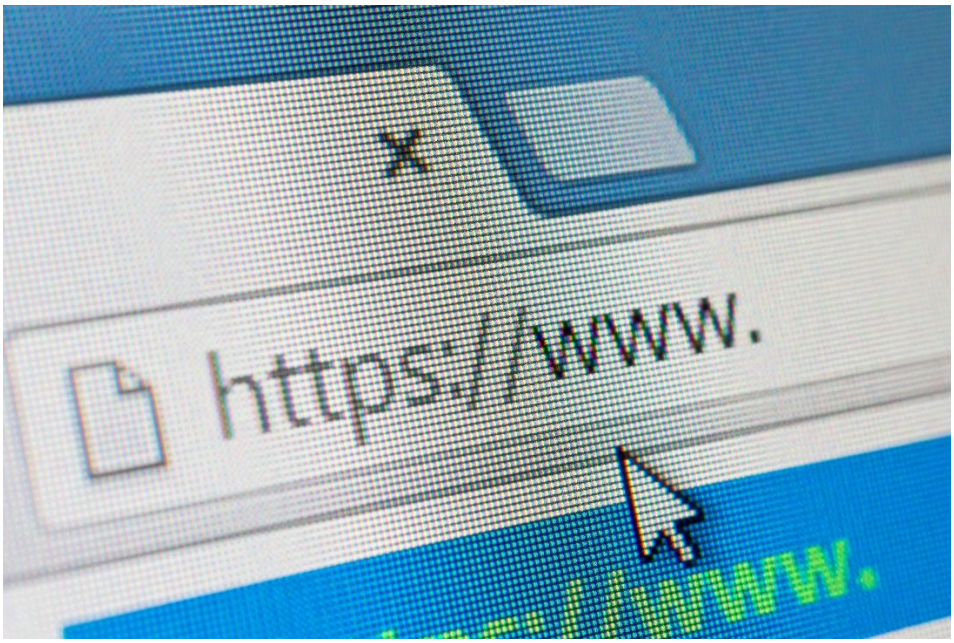
1. Palavras-passe
Muitos serviços na Internet estão protegidos com um código de acesso, de maneira a proteger a privacidade da informação. Se este código for simples ou comum, ou seja, se o código de acesso for muito usado entre vários utilizadores, pode ser facilmente descoberto, permitindo um acesso indevido à conta, como se fosse o verdadeiro utilizador a aceder. Por esta razão, recomenda-se o uso de uma palavra-passe forte, que contenha mais de 8 caracteres e combine letras (maiúsculas e minúsculas), dígitos e caracteres especiais. Deve também evitar-se a inclusão de informações pessoais, como o número identificativo nacional ou nomes de parentes ou conhecidos e nunca se deve utilizar padrões muito simples ou palavras do dicionário. Para garantir uma maior segurança, é aconselhado que se proceda a uma alteração periódica das palavras-passe. As *passwords* nunca devem ser registadas em cadernos ou ficheiros não encriptados.

2. Tecnologias de segurança
É importante criar várias cópias de segurança de todos os dados importantes e garantir que estes não estão todos armazenados no mesmo local. Adicionalmente, é pertinente manter o *software* que se utiliza sempre atualizado, bem como instalar um filtro ou *software* de *phishing* na aplicação de email e no navegador de Internet usado.

As soluções antivírus, *firewall* e anti-*spam* constituem alguns exemplos das aplicações mais importantes para garantir a proteção do computador contra as principais ameaças que se espalham na Internet. Ao utilizar estas tecnologias reduz-se o risco e a exposição aos perigos. Para combater os vírus, devem realizar-se verificações regulares através de um *software* antivírus, bem como garantir que o *software* antivírus instalado é compatível com o *software* anti-*spyware*.

3. Páginas de confiança
Através de técnicas de Engenharia social, muitos *websites* são frequentemente promovidos graças a dados que atraem a atenção do utilizador - tais como descontos na compra de produtos (ou mesmo ofertas gratuitas) ou materiais exclusivos sobre notícias atuais, material multimédia, etc. Para uma navegação segura, recomenda-se que o utilizador esteja atento a estas mensagens e evite aceder a páginas com estas características.

Neste sentido, é crucial verificar as credenciais SSL do *website* e nunca partilhar informação pessoal/sensível em sites que não tenham instalado um certificado SSL válido.



Com recurso a técnicas de SEO "*Black Hat*", os infratores colocam frequentemente os seus *websites* nos primeiros lugares dos resultados dos motores de busca, especialmente em casos de pesquisas de palavras-chave amplamente usadas pelo público, tais como assuntos atuais, notícias que chamam à atenção ou tópicos populares como por exemplo, desporto e sexo.

Uma das maneiras mais seguras de não deixar rasto na Internet passa por instalar uma rede privada virtual ou de um servidor *proxy* que atue como um intermediário na comunicação com os *websites* visitados.

4. Partilhar informação

Todas as informações pessoais carregadas na Internet, as imagens partilhadas nas redes sociais, deixam sempre um rasto digital que é conhecido como a "identidade digital" de cada um de nós. É necessário, portanto, estar ciente da identidade digital que criamos e divulgar na Internet apenas informação pessoal que consideramos 100% pública.

Por forma a prevenir a divulgação de informação adicional, nunca se deve dar acesso à localização, câmara ou microfone dos dispositivos. É também recomendado que se evite o uso do GPS para mostrar a localização do próprio em publicações.

É aconselhável que se interaja e aceite pedidos apenas de contactos conhecidos, tanto nas plataformas de mensagens instantâneas como nas redes sociais, de modo a evitar o acesso aos perfis criados pelos agressores para comunicar com as vítimas e expô-las a várias ameaças, tais como o *malware*, *phishing*, *ciberbullying*, entre outros.

5. Redes WiFi gratuitas

O uso de redes WiFi gratuitas para navegação em páginas públicas acarreta um risco mínimo. Contudo, é desaconselhada a navegação em páginas *web* que permitam a introdução de dados pessoais, tais como palavras-passe ou nomes de utilizador, uma vez que a rede WiFi pode estar comprometida, o que facilita a interceção ilegítima desses dados pessoais. Devemos prestar a mesma atenção quando nos ligamos a redes WiFi conhecidas.

6. Ligações suspeitas

Um dos meios mais utilizados para direcionar vítimas para *websites* maliciosos são as hiperligações ou *links*. Evitar clicar nestes *links* impede o acesso a páginas *web* que tenham ameaças capazes de infetar o utilizador.

As ligações podem estar presentes em *emails*, janelas de *chat* ou mensagens em redes sociais: é crucial analisar o contexto em que estas são recebidas - se forem enviadas numa situação suspeita que cause dúvida (por exemplo, um convite para ver uma foto feito numa língua estrangeira), se forem enviadas por um remetente desconhecido ou se se referem a um sítio *web* não fiável.

7. Download de ficheiros

Uma das maiores falhas de segurança provém do *download* de ficheiros inseguros. Se a origem dos ficheiros descarregados não inspira completa segurança, é mais prudente evitar o *download* ou verificar o ficheiro antes de proceder ao seu *download*. Muitos *websites* fingem oferecer programas populares que são adulterados, modificados ou substituídos por versões que contêm algum tipo de *malware* e descarregam o código malicioso no momento em que o utilizador instala o programa no seu sistema informático. É, por isso, recomendado que os *downloads* de aplicações sejam realizados apenas quando provêm de páginas oficiais.

Por outro lado, a propagação de *malware* é geralmente feita através de ficheiros executáveis. Recomenda-se assim evitar a execução de ficheiros a menos que a sua segurança seja comprovada e a sua origem seja proveniente de uma fonte fiável/fidedigna (quer provenha de um contacto de mensagens instantâneas, um *email* ou um *website*).

8. Atualização do sistema operativo e aplicações

Manter o sistema operativo (*Windows, Linux, Apple*…) e todas as aplicações instaladas corretamente atualizadas é uma das principais garantias para não deixar as "portas" do computador abertas para que um cibercriminoso consiga entrar no sistema e encontrar alguma fragilidade que possa explorar. Embora a atualização de computadores demore tempo, e por vezes exija que o mesmo seja reiniciado, é essencial corrigir as vulnerabilidades de segurança no *software* instalado.

A par destas precauções tomadas para a atualização de computadores portáteis e de secretária, é também importante que se apliquem as mesmas regras no caso dos telemóveis. Através de dispositivos como *smartphones*, os proprietários de outros são mais suscetíveis a violações de elementos de segurança que o sistema operativo pode oferecer.

9. Evitar introduzir informações pessoais em formulários duvidosos

Quando o utilizador é confrontado com um formulário *web* que contém campos com informação sensível (por exemplo, nome de utilizador e palavra-passe), é recomendado que verifique a legitimidade do *site*. Uma boa estratégia é verificar o domínio e a utilização do protocolo HTTPS para garantir a confidencialidade da informação. Desta forma, os ataques de *phishing* que tentam obter informações sensíveis podem ser evitados através da simulação de uma entidade de confiança.

10. *Cookies*

Uma *cookie* é um ficheiro criado por um *website* que contém pequenas quantidades de dados, enviados entre um remetente e um recetor, a fim de conhecer as preferências do utilizador e tornar a sua experiência no *site* mais fácil. No entanto, a informação que é partilhada é passível de ser transmitida a terceiros, pelo que é pertinente avaliar o tráfego destes dados e, em qualquer caso, é possível, a partir do próprio navegador de Internet, decidir eliminar estes *cookies* para evitar sustos desnecessários.

Aplicar conhecimento

Cibercrime

1. Qual é a definição de cibercrime?

Tarefa: Escolha única – apenas uma frase está correta.

a) Cibercrime é ver conteúdo inapropriado na Internet.
b) Cibercrime é um ato ilegal em que o computador é uma ferramenta, ou um alvo, ou ambos.
c) Cibercrime é a monitorização de *emails* de trabalho de colaboradores por parte da entidade patronal.
d) Cibercrime é a obtenção de informações públicas através da Internet.

2. Qual dos seguintes exemplos é phishing?

Tarefa: Escolher as opções corretas usando o princípio da escolha múltipla: pode haver mais do que uma resposta certa

a) Receber um *email* comemorativo a anunciar que será oferecido um iPhone a quem enviar algumas informações pessoais para receber o prémio.
b) Receber um *email* com algumas ofertas de bens que podem ser comprados.
c) Receber um *email* a requisitar a mudança da palavra-passe de uma conta bancária, contendo um link direto para fazer essa mudança.
d) Receber um *email* informativo sobre um evento cultural a acontecer nas redondezas.

3. Verdadeiro ou falso?

O *hacking* também pode ser percecionado como um ato útil e produtivo.

V ☐ F ☐

Explicação: Contudo, o hacking não pode ser visto como uma ameaça dado que também é utilizado também para causas produtivas. Este tipo de hacking envolve boas intenções e é conhecido por hacking ético. Este tipo de hacking é feito para assegurar que os sistemas operativos estão a funcionar.

4. Correspondência de respostas - pode escolher a resposta correta a partir do menu disponível para a parte respetiva do texto

_____ é o ato de roubar informações pessoais e identificativas com o intuito de cometer atos ilegais, tais como: abrir uma linha de crédito, alugar uma casa, comprar bens ou serviços, ou cometer fraude ou extorsão relacionada com leilões ou salários.

_____ é o contacto constante com a pessoa; dizer coisas ofensivas à pessoa ou dar informação errada sobre a pessoa a terceiros. Por exemplo, o infrator cria um grupo do Facebook chamado "Eu odeio…" e convida todos os amigos a juntarem-se ao mesmo.

_____ inclui atividades que geram lucro de forma desonesta para todos os envolvidos na conduta em questão. Consiste na exploração de informação privilegiada ou na aquisição da propriedade de outra pessoa por engano para assegurar um benefício material. O crime financeiro geralmente compreende o seguinte: fraude, branqueamento de capitais, suborno e corrupção, entre muitos outros.

_____ é uma obsessão em descobrir o máximo possível sobre a pessoa (sem realmente lhe perguntar). Por exemplo, o infrator descobre o local de nascimento da pessoa, se a pessoa é casada, etc.

5. Completar a frase com a palavra correta – preencha o espaço em branco.

Um ciberataque que use ou explore redes informáticas ou de comunicação com o objetivo de causar destruição ou disrupção suficiente para gerar medo ou intimidar uma sociedade para um objetivo ideológico chama-se (_____).

Proteção contra conteúdos impróprios

1. Correspondência de respostas – pode escolher a resposta correta a partir do menu disponível para a parte respetiva do texto

_____ é caracterizado como uma descrição explícita ou imagem que visa estimular sentimentos sexuais.

_____ é a promoção ou incitação do ódio contra indivíduos ou grupos com base na origem étnica, religião, deficiência, idade, nacionalidade, estatuto de veterano, orientação sexual, género, identidade de género, ou qualquer outra característica.

_____ são os *websites* que promovem a anorexia como um estilo de vida, não como uma doença.

_____ fornecem informações atrativas sobre tópicos como eventos históricos, mas distorcem os factos e referem outras fontes de informação já manipuladas por uma perceção deslocada do mundo.

2. Qual é a classificação que pode ajudar a reconhecer os websites com conteúdo inapropriado?

Tarefa: Escolher as opções corretas usando o princípio da escolha múltipla: pode haver mais do que uma resposta certa

a) Classificação da *Motion Picture Association* (por exemplo, PG)
b) Escala LT Int. (por exemplo, classificações LT Corporate Family)
c) Escala Nacional (por exemplo, NSR)
d) Classificações PEGI de jogos *online* (por exemplo, PEGI 7)

3. Qual das seguintes ferramentas é útil para o controlo parental de conteúdo online?

Tarefa: Escolha única – apenas uma frase está correta.

a) *App* de proteção *online*
b) iWebfilter
c) K10 Web Protection
d) Anti-game

4. *Que competências são necessárias para ensinar as crianças a minimizar os riscos do conteúdo inadequado?*

Tarefa: Escolher as opções corretas usando o princípio da escolha múltipla: pode haver mais do que uma resposta certa

a) Competências informáticas
b) Pensamento criativo e resiliência
c) Competências digitais
d) Formas positivas de utilizar a tecnologia

5. Correspondência de respostas - pode escolher a resposta correta a partir do menu disponível para a parte respetiva do texto

Ainda que existam ferramentas úteis de proteção como leis, controlo parental, configurações de *software*, instituições de apoio, a chave é _____ entre os adultos e as crianças.

Proteção de dados pessoais

1. Correspondência de respostas - pode escolher a resposta correta a partir do menu disponível para a parte respetiva do texto

_____, também conhecido como privacidade da informação, é um aspeto da segurança dos dados que lida com o tratamento adequado de _____. Protege principalmente os dados pessoais do indivíduo de _____. A _____ dos dados pessoais é um direito _____ na Europa há anos. A proteção de dados tornou-se cada vez mais importante nos últimos anos devido a _____ e _____ que facilitam a recolha, processamento, armazenamento, disseminação e análise de dados. O _____ é um regulamento juridicamente vinculativo sobre a proteção dos indivíduos no que diz respeito ao tratamento de dados pessoais.

2. Verdadeiro ou falso?

O RGPD aplica-se exclusivamente ao processamento automático de dados pessoais
V □ F □
Os dados pessoais referem-se a dados sensíveis sobre um indivíduo
V □ F □
Os dados sensíveis devem ser cada vez mais protegidos
V □ F □
Os dados pessoais incluem, por exemplo, nome, data de nascimento, idade ou morada, número de conta
V □ F □
A informação sensível inclui, por exemplo, número de cartão de crédito, crença religiosa, filiação sindical, origem racial e étnica
V □ F □

3. Correspondência de respostas - pode escolher a resposta correta a partir do menu disponível para a parte respetiva do texto

O RGPD define _____ princípios-chave que devem ser rigorosamente cumpridos no contexto de _____. As violações destes princípios podem resultar em _____. Para dados pessoais _____, o RGPD tem à disposição _____ princípios básicos legais para processamento, uma vez que o processamento de _____ é proibido em geral, a menos que sejam cumpridas condições específicas. Aplicam-se requisitos especiais ao tratamento de _____. O tratamento de dados só é permitido em _____ específicos.

4. O que é que está correto sobre violações de dados?

Tarefa: Escolher as opções corretas usando o princípio da escolha múltipla: pode haver mais do que uma resposta certa

a) É o dever de um controlador de dados informar imediatamente o processador de dados na eventualidade de ocorrer qualquer violação de dados.
b) Se ocorrer uma violação de dados, o responsável pelo tratamento de dados deve cumprir com a sua obrigação de comunicar e notificar sobre o sucedido.
c) Se ocorrer uma violação de dados, o responsável pelo processamento de dados deve cumprir com a sua obrigação de comunicar e notificar sobre o sucedido.
d) A autoridade de proteção de dados deve ser informada no prazo de 24 horas.
e) A autoridade de proteção de dados deve ser informada no prazo de 72 horas.
f) A autoridade de proteção de dados deve ser informada se a violação for suscetível de constituir um risco para os direitos e liberdades das pessoas em causa.
g) A notificação adicional da pessoa em causa nem sempre é necessária se existir um risco elevado para os direitos e liberdades das pessoas em causa

5. Correspondência de respostas - pode escolher a resposta correta a partir do menu disponível para a parte respetiva do texto

A fim de assegurar a proteção de _____, a questão da _____ é uma questão central. Neste contexto, _____ e _____ são palavras-chave importantes. _____ refere-se à proteção de dados através de _____. Isto significa que, ao desenvolver novas tecnologias, devem ser asseguradas soluções adequadas, em conformidade com a proteção de dados. _____ significa privacidade através de _____. A pessoa responsável deve assegurar, através de configurações para o efeito, que só são processados os _____, que são absolutamente necessários.

Proteção de Smartphones

1. *Que medidas de prevenção deves levar a cabo para proteger o teu smartphone e os dados privados nele armazenados em caso de perda ou roubo?*

Tarefa: Escolher as opções corretas usando o princípio da escolha múltipla: pode haver mais do que uma resposta certa

a) Utilizar um número de identificação pessoal (PIN) e um bloqueio de ecrã
b) Utilizar um PIN com uma combinação de números comum para que seja fácil de lembrar
c) Anotar o número de série do *smartphone*
d) Não instalar uma aplicação antirroubo

2. Quais das afirmações estão corretas no que toca às mensagens instantâneas?

Tarefa: Escolher as opções corretas usando o princípio da escolha múltipla: pode haver mais do que uma resposta certa

a) Mensagens instantâneas são um *chat offline* para troca de mensagens.
b) Mensagens instantâneas são comunicações que ocorrem na Internet através de aplicações móveis
c) A transmissão da mensagem tem lugar no chamado procedimento *pull*
d) Mensagens instantâneas servem apenas para a transmissão de textos.
e) Exemplos de serviços mensagens instantâneas são o WhatsApp, Skype ou Facebook Messenger

3. A maioria das aplicações de mensagens instantâneas são gratuitas. Que riscos estão a surgir disso?

Tarefa: Escolher as opções corretas usando o princípio da escolha múltipla: pode haver mais do que uma resposta certa

a) A aplicação tem de ser paga mais tarde, com custos elevados
b) Os dados do indivíduo são geralmente o produto
c) A comunicação é maioritariamente encriptada
d) Existe *malware* de todos os tipos escondidos nas aplicações

4. Verdadeiro ou Falso?

Não há qualquer problema na conceção de permissões ilimitada às aplicações
V □ F □

Os programadores das *apps* têm interesse nos teus dados pessoais
V □ F □

Todos os acessos a dados pessoais são óbvios via formulários de permissão de uma *app*
V □ F □

A proteção de dados é cada vez mais importante no que toca às mensagens instantâneas e *apps*
V □ F □

Existe um risco de *phishing*
V □ F □

Não há qualquer problema com a comunicação não encriptada
V □ F □

5. Correspondência de respostas - pode escolher a resposta correta a partir do menu disponível para a parte respetiva do texto

Dados os potenciais _____ da utilização de aplicações no teu *smartphone*, provavelmente estás a pensar como podes proteger-te melhor e à tua privacidade. Aqui estão algumas dicas sobre o que considerar ao utilizar aplicações no teu *smartphone*: utiliza sempre a versão _____ da aplicação, _____ utilizar imagens que não possuis como foto de perfil, lê a _____ cuidadosamente antes de instalar uma aplicação, introduz apenas os dados _____, utiliza um _____ que não revele muito sobre ti e não te incomode no que toca a spam, verifica os direitos de _____ da aplicação e ajusta-os se necessário, ajusta a _____ das aplicações (por exemplo, visibilidade de imagens de perfil) e _____ contactos indesejados.

Fluxo de informação e comunicação *online*

1. O meio de comunicação online mais comum é

Tarefa: Escolha única – apenas uma frase está correta
a) Mensagens instantâneas
b) *Email*
c) *Websites*

2. Correspondência de respostas - pode escolher a resposta correta a partir do menu disponível para a parte respetiva do texto

_____ são *emails* indesejáveis que procuram enganar-te com informações enganosas para te levar a realizar atos prejudiciais. Programas maliciosos são, por exemplo, frequentemente transferidos por via de *emails* falsos através de _____. Por isso, é importante estar atento às características típicas dos *emails* maliciosos. É importante ter cuidado com o seguinte: o *email* promete algo que parece _____ (demasiado bom para ser verdade), o conteúdo do *email* de alguma forma não se enquadra no (suposto) _____ de confiança, o *email* contém certas palavras _____ no assunto (por exemplo, "último lembrete" ou "conta bloqueada"), é pedido que reveles _____, o _____ parece estranho, o *email* contém muitos _____ (ortografia ou gramática), o *email* é automaticamente movido para a

_____ ou é pedido que executes programas com _____ estranhos (por exemplo, jpg.vbs" ou "gif.exe").

3. Os fóruns e salas de chat *são plataformas muito conhecidas e usadas para a comunicação online e troca de informação. Quais das seguintes afirmações estão corretas?*

Tarefa: Escolher as opções corretas usando o princípio da escolha múltipla: pode haver mais do que uma resposta certa

a) Os fóruns são adequados para a comunicação em tempo real
b) Os chats são adequados para comunicação em tempo real
c) Os fóruns são adequados para discussões em que nem todos os participantes precisam de estar *online* ao mesmo tempo
d) Os chats são adequados para discussões em que nem todos os participantes precisam de estar *online* ao mesmo tempo
e) Os fóruns são mais bem organizados
f) Os chats são mais bem organizados
g) Só os fóruns requerem um registo com um endereço de email válido
h) Os chats e os fóruns permitem a troca de mensagens de texto, mas normalmente também podem ser utilizados para trocar imagens, vídeos, links ou ficheiros

4. Quais são os principais riscos da utilização de fóruns e chats?

Tarefa: Escolher as opções corretas usando o princípio da escolha múltipla: pode haver mais do que uma resposta certa

a) Identidades falsas
b) *Malware*
c) Custos elevados
d) Links para sites de *phishing*
e) Comunicação não encriptada
f) Comunicação encriptada

5. Correspondência de respostas - pode escolher a resposta correta a partir do menu disponível para a parte respetiva do texto

Nas redes sociais, a presunção de anonimato pode levar a um comportamento irrefletido ao lidar com _____ e _____. Como consequência, as redes sociais estão cada vez mais a ser alvo de atividades _____. Existe o perigo de seres enganado por _____ ou pela disseminação consciente ou inconsciente de _____. Assim, deves sempre considerar os seguintes aspetos ao lidar com _____: nunca publicar e discutir informação _____ e _____ a informação divulgada num espaço virtual público, utilizar os _____ fornecidos para tornar a informação apenas acessível a um determinado grupo de pessoas, ser criterioso quando se _____ pedidos de amizade, verificar as _____ das redes sociais e estar ciente da informação _____. Se detetares uma má utilização ou má conduta nas redes sociais, deves _____ ao prestador de serviços, _____ e organizações adequadas.

Controlo Parental

1. As consequências do sexting *para a vítima são:*

Tarefa: Escolher as opções corretas usando o princípio da escolha múltipla: pode haver mais do que uma resposta certa

a) Humilhação e linchamento social para o protagonista das imagens.
b) O menor enfrenta o insulto público, que afeta antes de mais a sua autoestima, numa idade em que a sua personalidade está a ser formada e depende em grande parte da imagem que os outros difundem, pois a opinião dos outros é importante.

c) Há também sentimentos de impotência, principalmente quando o caso é dito aos pais ou educadores ou culpa por se encontrarem nessa situação.
d) Não há consequências

2. *Correspondência de respostas - pode escolher a resposta correta a partir do menu disponível para a parte respetiva do texto*

O aliciamento é definido como um tipo de _____ realizado deliberadamente por um _____ para estabelecer uma relação e controlo emocional sobre um menor, a fim de preparar o terreno para o _____ sexual. Em alguns casos, acontece entre menores, mas normalmente com uma grande diferença de idade, onde o mais velho tende a ser o _____. O objetivo do aliciamento é ganhar a confiança do _____, obter imagens ou vídeos de teor _____ e até mesmo encontrarem-se pessoalmente.

3. Correspondência de respostas - pode escolher a resposta correta a partir do menu disponível para a parte respetiva do texto

Um dos primeiros passos do _____ tende a envolver um infrator que insulta ou ameaça a _____, ameaçando vazar informações que podem _____ a sua _____. A informação enviada pelo infrator sobre o assediado pode ser verdadeira, sendo, neste caso, divulgada propositadamente pelo facto de ser _____ ou prejudicial aos interesses do assediado ou pode ser efetivamente falsa. Se assim for, pode ser categorizada como _____.

4. Correspondência de respostas - pode escolher a resposta correta a partir do menu disponível para a parte respetiva do texto

Uma forma de descobrir se o _____ sofre de _____ é necessário analisar a quantidade de tempo gasto a usar dispositivos _____, a frequência e as manifestações _____ de não estar ligado à rede. Se o menor parece estar ansioso ou agitado quando não está *online*, ou se passa por mudanças de _____ frequentes, a dependência da Internet pode ser a razão por detrás disso.

5. Correspondência de respostas - pode escolher a resposta correta a partir do menu disponível para a parte respetiva do texto

Várias técnicas podem ser utilizadas para _____ dados secretamente a partir de um dispositivo digital. Por vezes, os _____ escondem as suas intenções, disfarçando os seus esquemas como algo diferente do que são. Por exemplo, através de anúncios que requerem informações pessoais para disponibilizar a visualização do conteúdo ou através da solicitação de_____ dos utilizadores para que estes possam desfrutar de um serviço_____. Contudo, na maioria das vezes, os_____ partilham os seus dados porque não estão conscientes do perigo, pelo que é vital incitar um comportamento mais responsável na_____.

Proteção de Hardware e Software

1. *Correspondência de respostas - pode escolher a resposta correta a partir do menu disponível para a parte respetiva do texto*

O *hardware* refere-se aos elementos _____ do computador. Alguns exemplos de componentes de *hardware* são: _____. O *software*, comummente conhecido como _____ é composto por todas as instruções que dizem ao *hardware* como funcionar de certa forma. O *software* é capaz de desenvolver _____ tarefas diferentes com o mesmo *hardware* de base.

2. *Que dicas/truques podes aplicar para melhorar a proteção do software? (escolha múltipla – uma resposta está incorreta)*

Tarefa: Escolha única – apenas uma frase está correta

a) Atualizações regulares ao *software*
b) Cria várias cópias de segurança
c) Não instales *softwares de firewalls*
d) Encriptar informação

3. *Um exemplo de proteção de hardware é evitar comprar componentes de hardware de fontes/países de risco. (Verdadeiro/falso)*

a) Verdadeiro
b) Falso

4. *Que medidas podes implementar para teres uma melhor proteção de software?*
   Tarefa: Escolher as opções corretas usando o princípio da escolha múltipla: pode haver mais do que uma resposta certa

a) Instalar um antivírus e mantê-lo atualizado
b) Explorar as ferramentas de segurança que instalas
c) Instalar as atualizações do sistema operativo de vez em quando
d) Desativar a partilha de ficheiros e media, se não precisares

5. *Quais são os ataques mais comuns ao hardware?*
   Tarefa: Escolher as opções corretas usando o princípio da escolha múltipla: pode haver mais do que uma resposta certa

a) Acidentes físicos
b) *Modding*
c) *Trojan*
d) *Phishing*

Proteção de dados pessoais nas redes sociais

1. *Com que questões de segurança deves ter cuidado quando usas as redes sociais?*
   Tarefa: Escolher as opções corretas usando o princípio da escolha múltipla: pode haver mais do que uma resposta certa

a) Se um *link* te redireciona para um *website*, deves prestar atenção para ver se existe um endereço físico e contactos
b) Ver se um *website* tem uma política de devolução e verificar a sua política de envio
c) Quando receberes um pedido de amigo de alguém que não reconheças, podes tentar fazer uma pesquisa de imagem inversa
d) Para evitares um ataque de *phishing* deves ver o URL completo isso ajudar-te-á a mostrar se esse conduz a um site legítimo.

2. *Correspondência de respostas - pode escolher a resposta correta a partir do menu disponível para a parte respetiva do texto*

A maioria dos *websites* permite a definição de informação que está a ser publicada como informação pública ou privada, usando a opção de controlo "_____".

A forma como os dados pessoais são apresentados ou armazenados numa determinada rede social é da responsabilidade do _____.

O ataque mais comum nas redes sociais utiliza uma estratégia para atrair o utilizador, nomeadamente através de um _____.

3. *Quais das seguintes características são associadas às redes sociais?*
   Tarefa: Escolha única – apenas uma frase está correta

a) Interativas

b) Facilitam a criação ou partilha de informação, ideias, interesses de carreira e outras formas de expressão
c) Estimulam a ligação entre duas ou mais pessoas
d) Mais de 4 mil milhões de utilizadores ativos das redes sociais

4. *Quais são os riscos mais comuns nas redes sociais?*

Tarefa: Escolha única – apenas uma frase está correta

a) *Software* que utiliza encriptação para desativar o acesso da vítima aos seus dados, como fotografias ou documentos até que o resgate seja pago
b) Tipo de código malicioso ou *software* que parece legítimo mas que pode tomar o controlo do computador
c) Forma de *malware* que é capaz de se copiar e se espalhar para outro computador
d) Forma de *malware* que causa danos físicos no computador.

5. *Que dicas podes aplicar para estar sempre um passo à frente de um potencial cibercrime nas redes sociais?*

Tarefa: Escolha única – apenas uma frase está correta

a) Não guardes as tuas credenciais de acesso nos teus dispositivos/parâmetros/aplicações
b) Evita partilhar informação pessoal *online*
c) Ter o mais recente *software* de segurança
d) Verifica a tua configuração de privacidade

Cibersegurança

1. *O que não é a cibersegurança?*

Tarefa: Escolha única – apenas uma frase está correta

a) Prevenir e detetar ataques digitais, protegendo sistemas, *hardware* e *software*
b) Prática de defesa de computadores, servidores, dispositivos móveis, sistemas eletrónicos, redes e dados de ataques maliciosos
c) A cibersegurança só se aplica ao *software* e *hardware*
d) Técnicas de proteção de computadores, redes, programas e dados contra acessos não autorizados ou ataques que visam a sua exploração

2. *A fim de melhorar a tua segurança cibernética online que medidas podes aplicar?*

Tarefa: Escolha única – apenas uma frase está correta

a) Criar diferentes palavras-passe para diferentes contas e perfis
b) Alterar as palavras-chave de vez em quando e usar uma combinação de letras maiúsculas e minúsculas, símbolos e números
c) Guardar as palavras-passe numa folha de cálculo no computador
d) Usar um fator de autenticação multifator (se possível) para diferentes contas *online*

3. *Que precauções deves tomar quando fazes compras online?*

Tarefa: Escolha única – apenas uma frase está correta

a) Ler críticas e ver se outros consumidores tiveram uma experiência positiva ou negativa nesse *website* específico
b) Criar cartões de crédito virtuais
c) Manter o *software* antivírus e anti-*spyware* atualizado juntamente com a firewall
d) Não ler os termos e condições dos diferentes *websites* porque são todos muito semelhantes

4. *A partir da lista, por favor seleciona as frases incorretas relativamente à definição e aplicação da computação em cloud*

Tarefa: Escolha única – apenas uma frase está correta

a) Prática de usar uma rede de servidores remotos alojados na Internet para armazenar, gerir e processar dados em vez de um servidor local ou um computador pessoal

b) Entrega de diferentes serviços através da Internet, incluindo servidores, armazenamento, bases de dados, redes, *software* e análises
c) Existe apenas um tipo de solução de computação em *cloud*
d) A computação em *cloud* pode ser feita sem interação humana

5. *Que medidas podes usar para melhorar a computação em cloud?*

Tarefa: Escolha única – apenas uma frase está correta

a) Utilizar uma autenticação multi-fator
b) Definir diferentes níveis de autorização de informação de acordo com o que as pessoas precisam
c) Assegurar formação relativa à proteção de dados e informação privada
d) Fazer cópias de segurança dos teus dados/informações de vez em quando

Internet das coisas

1. *Quais das seguintes informações sobre IoT estão corretas?*

Tarefa: Escolher as opções corretas usando o princípio da escolha múltipla: pode haver mais do que uma resposta certa

a) A IoT vai melhorar os transportes públicos
b) A IoT está a transformar objetos físicos num ecossistema de informação partilhada entre dispositivos que são vestíveis, portáteis, mesmo implantáveis, tornando as nossas vidas tecnológicas e ricas em dados
c) As aplicações de negócio de IoT são numerosas
d) Carros inteligentes, aparelhos de rastreio e fitness viáveis, assistentes de voz e carros inteligentes são todos exemplos de tecnologias IoT

2. *Da lista, por favor seleciona as opções corretas relativamente à Internet das Coisas*

Tarefa: Escolha única – apenas uma frase está correta

a) A IoT só pode ser aplicada a pessoas, a casas e à indústria automóvel
b) Sistema de dispositivos informáticos inter-relacionados, máquinas mecânicas e digitais
c) Convergência de múltiplas tecnologias, análise em tempo real, aprendizagem de máquinas, sensores de mercadorias e sistemas incorporados
d) O termo IoT engloba tudo o que está ligado à internet

3. *Quais são as aplicações mais comuns da Internet das Coisas?*

Tarefa: Escolher as opções corretas usando o princípio da escolha múltipla: pode haver mais do que uma resposta certa

a) Dispositivo que monitoriza a glicemia
b) Um frigorífico que cria automaticamente listas de compras
c) Cidades inteligentes e casas inteligentes
d) Cartões de retalho e cartões ligados

4. *Para te protegeres de ataques cibernéticos em todas as camadas que compõem os dispositivos IoT, que medidas da lista, podes aplicar?*

Tarefa: Escolher as opções corretas usando o princípio da escolha múltipla: pode haver mais do que uma resposta certa

a) Identificar ameaças e vulnerabilidades
b) Instalar programas de segurança de Internet de boa reputação nos teus computadores, tablets e *smartphones*
c) Utiliza uma solução VPN porque ajuda a proteger os dados transmitidos na tua casa ou em Wi-Fi público
d) Verifica regularmente o *website* do fabricante do dispositivo para atualizações de *firmware*

5. *Quais são os passos mais importantes para prevenir uma quebra de segurança cibernética?*

Tarefa: Escolher as opções corretas usando o princípio da escolha múltipla: pode haver mais do que uma resposta certa

a) Identificar ameaças e vulnerabilidades
b) Exposição ao risco dos ativos através de diferentes tipos de análises
c) Desenvolver planos de proteção e de contingência
d) Determinar quando alertar a equipa de resposta a emergências, profissionais de segurança cibernética, prestadores de serviços e/ou provedores de seguros

Respostas

Cibercrime

1:b
2: a, c
3: V
4: Roubo de identidade, Ciberbullying, crimes financeiros, *Ciberstalking*
5: Ciberterrorismo

Proteção contra conteúdos impróprios

1: Pornografia; racismo ou ódio; *websites* pro-ana; sites com conteúdo extremista
2: a, d
3: b
4: b, d
5: Confiança

Proteção de dados pessoais

1: Privacidade de dados; dados pessoais; uso indevido; proteção; fundamental; desenvolvimentos técnicos; globalização das redes; RGPD
2: F; F; V; V, F
3: sete; processamento de dados; sanções máximas; não sensíveis; seis; dados pessoais; dados sensíveis; casos excecionais
4: b, e, f
5: dados pessoais; segurança de dados; privacidade por design; privacidade por defeito; privacidade por design; design tecnológico; configurações por defeito; dados pessoais

Proteção de *Smartphones*

1: a, c
2: b, e
3: b, d
4: F, V; F; V; V, F
5: riscos de segurança, mais recente, evitar, política de privacidade, estritamente necessários, endereço de email alternativo, acesso, configuração da privacidade, bloqueia

Fluxo de informação e comunicação *online*

1: b
2: Emails falsos, anexos, irrealista, remetente de email, atrativas, informação confidencial, remetente, pasta de spam, nomes de ficheiros
3: b, c, e, h
4: a, b, d, e
5: dados, informações, fraudulentas, identidades falsas, informações falsas, redes sociais, pessoais, confidencial, filtros, aceita, proteções de privacidade, fraudulenta, reportar, autoridades

Controlo Parental

1: a, b, c
2: Ciberbullying, adulto, abuso, agressor, menor, sexual

3: Ciberbullying, vítima, prejudicar, reputação, negativa, desinformação
4: Menor, dependência da Internet, digitais, emocionais, humor
5: Divulgar, agressores, passwords, online, menores, internet

Hardware e Software

1: físicas; monitor e rato; programas e aplicações; muitas
2: a
3: Verdadeiro
4: a, b, c, d
5: c, d

Proteção de dados pessoais nas redes sociais

1: a, b, c, d
2: Definições de privacidade; Proprietário/fornecedor de redes sociais; ataque de *Phishing*
3: d
4: d
5: a

Cibersegurança

1: c
2: c
3: d
4: c
5: a, b, c, d

Internet das Coisas

1: a, b, c, d
2: a
3: a, b, c, d
4: a, b, c, d
5: a, b, c, d