Módulo de aprendizagem

Controlo Parental

Projeto: B-SAFE
Número: 2018-1CZ01-KA204-048148
Nome do autor: UDIMA
*Última data de processamento: 2*8.10.2020

Funded by the
Erasmus+ Programme
of the European Union

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

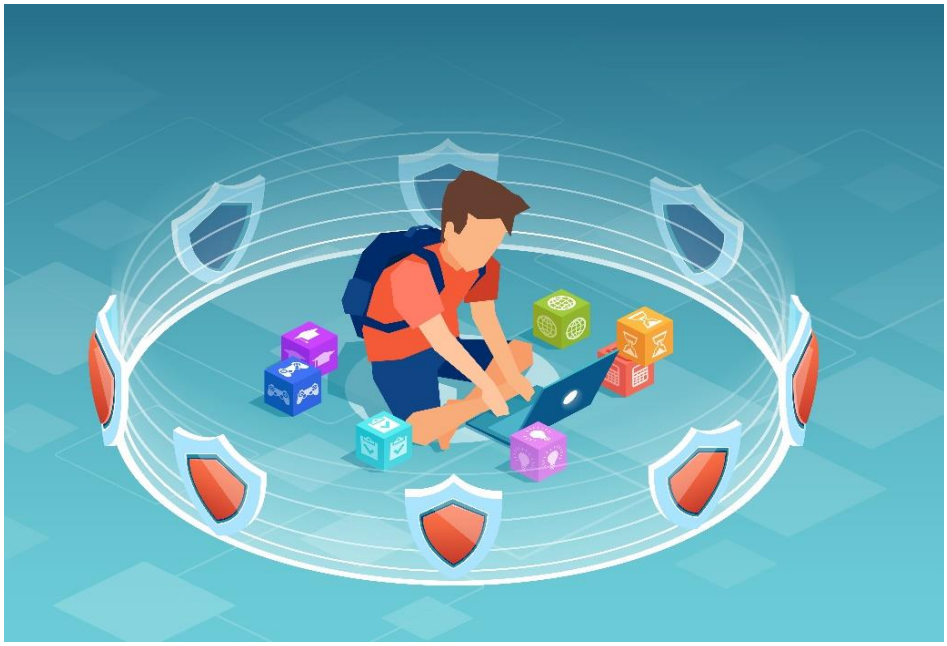
Controlo Parental

Introdução

O exercício do controlo parental por forma a garantir a segurança de crianças menores ao seu cuidado foi sempre uma das funções dos pais e tutores. Atualmente espera-se que esta função seja desempenhada pelos próprios e, nos dias que correm, torna-se cada vez mais importante.

As crianças estão sujeitas a numerosos perigos, tais como *sexting*, aliciamento de menores, ciberbullying, dependência da internet e divulgação de informação. Estes perigos consistem em expor ou estar exposto a conteúdos sexuais, sofrer de assédio por parte de um adulto, ser intimidado, tornar-se viciado na Internet ou ter os seus dados expostos.

Todos estes perigos que se encontram na Internet podem ter consequências negativas para a vítima no que diz respeito tanto à sua saúde emocional como física. Por este motivo, deve-se prestar atenção a estes perigos e às primeiras consequências dos mesmos sendo que é possível detetar este tipo de problemas através de algumas técnicas.



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

Com as aprendizagens concretizadas neste módulo, ficará explícita a importância do controlo parental para proteger crianças e adolescentes de situações perigosas em que se possam envolver enquanto utilizam diferentes dispositivos tecnológicos.

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

1. Desenvolver conhecimento - Quais são os princípios do controlo parental e porque é que precisamos dele?

Atualmente, dado o grande avanço das novas tecnologias, as crianças, os adolescentes e os jovens têm cada vez mais contacto com o mundo digital. De facto, em inúmeras ocasiões, os jovens assumem a responsabilidade de ensinar os adultos que os rodeiam a utilizar computadores, tablets ou até mesmo telemóveis.

Não é possível separar os menores destas tecnologias, ou pelo menos, não é fácil. O uso da Internet tornou-se crucial na esfera profissional e mesmo no nosso quotidiano. A necessidade de ensinar os mais novos a usar dispositivos tecnológicos tornou-se um facto e, por conseguinte, a necessidade de integrar essas tecnologias no sistema educativo também se fez sentir. As tecnologias são, sem dúvida, um pilar fundamental na educação e são muito úteis na procura de informação e na execução de tarefas escolares. Muitos espaços de ensino já desenvolveram plataformas através das quais oferecem recursos *online* aos seus alunos, enviam-lhes trabalhos de casa e, inclusive, requisitam que os alunos submetam as suas tarefas através de plataformas *online*. Neste ponto em que mantê-los afastados das tecnologias de informação é tão difícil, e até contraproducente, parece apropriado ponderar qual a melhor forma de proteger os menores.

Existem múltiplos perigos que podem afetar crianças, adolescentes e jovens na Internet, começando pelo ciberbullying ou *sexting* que pode ocorrer com pessoas que eles conhecem e que estão à sua volta (na sua escola ou na vizinhança, por exemplo), ou até sob a forma de ameaças externas, que são aquelas que vêm de estranhos. Pessoas desconhecidas têm a capacidade de recolher informações sobre menores e de os contactar, nem sempre com as melhores intenções. Além disso, ferramentas tecnológicas como telemóveis, portáteis ou computadores dão aos menores acesso a uma grande quantidade de conteúdos da Internet que podem ser completamente inapropriados, tais como conteúdos violentos, pornográficos ou extremistas. Um dos aspetos que mais preocupa os pais e que pode conduzir os menores a qualquer uma das ameaças anteriormente mencionadas são as redes sociais. As redes sociais permitem o acesso de jovens menores e, além disso, alguns jovens abaixo da idade estipulada para utilizar determinadas plataformas conseguem aceder à mesma, dado que conseguem mentir facilmente, definindo para o seu perfil uma idade que lhes permita aceder ao conteúdo de cada plataforma uma vez que não existe qualquer tipo de verificação dos dados introduzidos.

Antes da emergência de novas tecnologias, todo o processo de curiosidade, experimentação, estabelecimento de novas relações, etc. pelo qual os menores passam, acontecia diante dos olhos de todos os que os rodeavam. É por isso que o exercício do controlo parental era muito mais simples e não havia tanta dificuldade em manter os perigos afastados. É também por isso que, hoje em dia, a definição de controlo parental adquire novas particularidades e novos meios de comunicação, ainda que mantenha a sua essência. O controlo parental pode ser, portanto, definido como:

Definição
Controlo Parental ...a forma como os pais supervisionam e intervêm, se necessário, para assegurar que as experiências e processos de socialização e crescimento pessoal dos seus filhos ocorrem de forma adequada e sem riscos para eles.

Os riscos enfrentados pelos menores não mudaram na sua essência, mudou sim a forma e os meios através dos quais estes chegam às crianças e jovens. A existência de diferentes tipos de riscos conduzem a novas formas e métodos de controlo parental de forma a garantir a segurança dos menores.

Exemplo
Por exemplo, as crianças podem sofrer *bullying* sob a forma de insultos, rejeições, ameaças, ridicularização ou disseminação de mentiras, quer cara a cara, quer através da Internet, espalhando-se mais rapidamente e com um maior alcance.

Um sistema de controlo parental é uma ferramenta que permite aos pais controlar e/ou limitar o conteúdo *online* ao qual os seus filhos podem aceder a partir dos seus dispositivos, sejam eles computadores, telemóveis ou tablets. Existem muitas ferramentas parentais diferentes e podem ser utilizadas nos dispositivos dos menores para impedir algumas ações, bloquear páginas ou conteúdos ou para controlar a sua atividade a partir do mesmo dispositivo ou até a partir do dispositivo dos adultos.

Exemplo
Se os pais estiverem preocupados com a segurança dos seus filhos, devem considerar quais os dispositivos que a criança usa tendo em conta a sua idade. Existem aplicações e *softwares* para controlar a utilização da Internet, mas nem todos estes mecanismos de controlo estão disponíveis em todos os dispositivos. A idade da criança também orientará os pais a escolher uma ou outra ferramenta, uma vez estas respondem a diferentes necessidades, consoante a idade. Para os mais pequenos, pode ser útil possuir uma ferramenta implantada no dispositivo que bloqueie o conteúdo que não é feito para crianças, enquanto para os adolescentes, pode ser mais adequado uma ferramenta que permita monitorizar o tempo de uso ou o conteúdo acedido a partir dos dispositivos dos pais. As ferramentas de controlo parental estão disponíveis na maioria dos dispositivos, mas existem ferramentas mais específicas, em lojas *online* ou lojas de *apps* ou ferramentas oferecidas por companhias de seguros e de segurança e fornecedores de Internet.

Em geral, os sistemas de controlo parental que temos hoje são usados para garantir a segurança dos menores *online*, evitando assim possíveis ameaças e más experiências. Mais especificamente, os sistemas de controlo parental são ferramentas que foram concebidas para bloquear e filtrar o acesso a determinados espaços da Internet e para monitorizar a presença *online*. Estas ferramentas oferecem cada vez mais funcionalidades e podem ser personalizadas e adaptadas aos requisitos dos pais. As funcionalidades mencionadas podem ser divididas da seguinte forma:

- **Monitorização:** Para acompanhar a atividade *online*. Permite ao utilizador analisar a navegação efetuada pela criança, gerando avisos se esta entrar em *websites* não recomendados.

- **Controlar o contacto com outras pessoas:** Esta funcionalidade permite ao utilizador evitar o contacto dos filhos com estranhos o que, segundo o INCIBE (Instituto Nacional de Cibersegurança espanhol), ocorre em 40% dos menores.
- **Limitar o tempo de utilização:** Permite controlar tanto o tempo máximo em que a criança tem acesso à Internet como o tempo durante o qual tem permissão para manter o dispositivo ligado.
- **Controlar o acesso a sítios inadequados:** Permite ao utilizador controlar ou bloquear o acesso a *websites* cujo conteúdo seja impróprio para faixas etárias mais novas ou que comprometam os seus dados.
- **Aplicações restritivas:** Esta funcionalidade impede a utilização ou o *download* de certas aplicações.
- **Evitar as compras *online*:** É possível desativar a compra, intencional ou não, de aplicações ou outros artigos *online*.
- **Geolocalização:** Permite saber a localização exata da criança.
- **Autenticação em dois fatores:** Para além da palavra-chave para desbloquear o dispositivo, é necessário um código que é enviado aos pais para que o desbloqueio do dispositivo seja possível. Desta forma, são sempre os pais que dão acesso aos menores.
- **Bloqueio de chamadas**.

Todas estas formas de controlo parental são utilizadas para garantir a segurança dos menores, protegendo-os de estranhos e de conteúdos ou páginas inapropriadas. Este tipo de mecanismos ajudam também a proteger as crianças e adolescentes da utilização imprópria da Internet, pelos próprios ou por terceiros, seja esta intencional ou não. Esta proteção pode ser levada a cabo através do controlo da utilização da Internet por crianças ou através do bloqueio e controlo de diferentes funções.

Para os mais pequenos, os instrumentos de controlo parental geralmente escolhidos são aqueles que limitam e impedem o acesso a certos conteúdos inadequados para a sua idade ou limitam o tempo de utilização das diferentes aplicações e dispositivos. Estas ferramentas usam diferentes técnicas para conseguir este objetivo. A maioria deles recorre a 'listas negras', que nomeiam os sítios que não devem ser vistos ('*blacklists*') e filtram os mesmos ou permitem o acesso apenas aos conteúdos que estão nas listas brancas ('*whitelists*'), que são listas de conteúdos adequados para os mais pequenos. Também é possível bloquear o acesso a conteúdos com determinadas palavras-chave (pornografia, drogas, compras, etc), o que pode resultar no bloqueio de páginas adequadas para menores devido a falsos positivos. Além disso, este tipo de ferramentas de controlo parental também permite bloquear o acesso a aplicações específicas, permitir a sua utilização apenas *offline* (sem acesso à Internet), desativar a função de *chat* ou controlar o tempo e o horário em que lhes é dado acesso.

Por outro lado, e pensando nos adolescentes, foram também criadas ferramentas de controlo parental que permitem a utilização de dispositivos eletrónicos e a monitorização de atividades. Chega a um ponto em que as crianças precisam de uma maior liberdade no seu contacto com os dispositivos, uma vez que o seu conhecimento destes instrumentos aumenta, e têm curiosidade em saber mais e em interagir outras pessoas. Com recurso a estas ferramentas de controlo parental que permitem aos pais monitorizar a atividade dos filhos, é possível conhecer os serviços a que os adolescentes têm acesso, o que fazem, as pessoas que contactam e onde estes se ligam. O último é possível graças ao sistema de navegação GPS e a outras técnicas de localização que todos os dispositivos móveis possuem.

Este controlo parental pode ser exercido a partir de diferentes pontos:
- **Router e servidores DNS (*Domain Name System*):** O router é o acesso digital de uma casa e, através deste, é possível gerir as restrições de navegação de todos os dispositivos que se ligam a ele. A partir do router é possível controlar e filtrar os conteúdos a que os dispositivos conectados têm acesso e aos quais estes já acederam, definir os limites de tempo da ligação e aplicar filtros nos *websites*. Os servidores DNS também servem este propósito de filtração.

Análise
Esta é uma boa opção para controlar todos os dispositivos da casa, mas pode não ser a melhor opção se o objetivo é estabelecer restrições específicas para cada dispositivo. Além disso, não é possível controlar dispositivos quando estes não estão ligados ao servidor.

- **O próprio dispositivo:** Todos os dispositivos que temos em casa (computadores, tablets, telemóveis e até brinquedos) incluem mecanismos de controlo parental e permitem bloquear o acesso a conteúdos que não são adequados e controlar a atividade *online*.

Análise
Como está incluído no dispositivo, não é preciso procurar outros sistemas de controlo parental e evita-se assim o pagamento extra por este tipo de serviço. Além disso, permite aplicar o controlo em cada dispositivo individualmente. Contudo, normalmente não é possível personalizar e adaptar o serviço às necessidades individuais.

- ***Software*:** Para além de programas de controlo de computadores que protegem contra vários perigos que podemos encontrar na Internet, tais como vírus e *malware*, é também possível bloquear *websites*, marcar limites de tempo ou controlar a atividade *online*, receber relatórios sobre utilização ou informações sobre *chat*s.

Análise
Pode ser menos intuitivo do que outras ferramentas mas permite o controlo tanto do conteúdo visitado na Internet como da utilização do próprio dispositivo.

- **Navegador da Internet:** Através do navegador, é possível definir filtros, impedir a abertura de certos *websites* e até selecionar os domínios que se pretende bloquear.

Análise
É muito útil bloquear endereços que contenham certas palavras, páginas específicas ou todas as páginas que pertencem a certas categorias. Embora esta ferramenta seja vantajosa para controlar a utilização da Internet, não serve para controlar o próprio dispositivo em si.

- ***Apps*:** São adequadas para qualquer dispositivo móvel, que tendem a ser os dispositivos mais usados pelos menores para se ligarem à Internet. Com estas aplicações é possível controlar os *sites* que visitam e o tempo de uso, limitar os *downloads* de outras aplicações, evitar o contacto com estranhos e impedir a divulgação dos seus dados.

Análise
Esta é uma ferramenta poderosa existindo, atualmente, um leque bastante diversificado de aplicações fáceis de instalar e utilizar. O único problema é que estas aplicações estão normalmente disponíveis para telemóveis e, por vezes para tablets, mas nem sempre para outros dispositivos, tais como computadores ou portáteis.

O nível de supervisão que estes mecanismos oferecem, especialmente os últimos apresentados, é muito elevado, o que pode significar que podem ser vistas como intrusivas. Além disso, tal como os menores têm o direito de ser protegidos contra todas as formas de abuso *online*, eles também têm direitos de privacidade. É, portanto, aconselhável não fazer um uso abusivo deste tipo de instrumentos de controlo parental, avaliar a sua utilização e privilegiar sempre a construção de relações de confiança com crianças, promovendo o diálogo.

1. Aplicar conhecimentos

Exercício de ESCOLHA ÚNICA

Objetivo específico associado: OE_Controlo Parental_01_01: Saber quais as ameaças tecnológicas que afetam os menores.

Situação: Que ameaças tecnológicas afetam os menores?
Tarefa: Escolher a opção certa usando o princípio de escolha múltipla: apenas uma frase é verdadeira.

- Só existe o ciberbullying
- Existem múltiplos perigos que podem afetar crianças, adolescentes e jovens na Internet (ciberbullying, *sexting*,...)
- Não há nenhuma ameaça tecnológica que afete os menores.

Exercício de ESCOLHA ÚNICA

Objetivo específico associado: OE_Controlo Parental_01_02: Saber a definição do termo controlo parental.

Situação: Qual é a definição do termo controlo parental?
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira.

- O "controlo parental" corresponde à forma como os pais supervisionam e intervêm se necessário, para assegurar que as experiências e processos de socialização e crescimento pessoal dos seus filhos ocorrem de forma adequada e sem riscos para eles.
- O "controlo parental" é uma ferramenta que permite aos pais controlar e/ou limitar o conteúdo ao qual os seus filhos têm acesso *online,* a partir dos seus dispositivos, sejam eles computadores, telemóveis ou tablets.
- O "controlo parental" é uma ameaça tecnológica que pode afetar menores.

Exercício de ESCOLHA ÚNICA

Objetivo específico associado: OE_Controlo Parental_01_03: Ser capaz de explicar para que serve o controlo parental

Situação: Para que serve o controlo parental?
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira.

- Para controlar e/ou limitar o conteúdo a que as crianças têm acesso na Internet a partir dos seus dispositivos, sejam eles computadores, telemóveis ou tablets.
- Para dar às crianças a oportunidade de navegar na Internet como desejarem.

- Para controlar as contas das redes sociais das crianças.

Exercício de ESCOLHA ÚNICA

Objetivo específico associado: OE_Controlo Parental_01_04: OE_Controlo Parental_01_04: Perceber como funciona o controlo tecnológico parental

Situação: Como funciona o controlo tecnológico parental?
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira.

- O controlo tecnológico parental previne que uma criança aceda a conteúdo impróprio através de um bloqueio no roter da internet.
- O controlo tecnológico parental evita a utilização de dispositivos eletrónicos em casa através do uso de passwords online.
- O controlo tecnológico parental pode ser exercido a partir de diferentes pontos: servidores externos e DNS, a partir do próprio dispositivo, *software*, browser de Internet ou *apps*.

2. Desenvolver conhecimento – O que é o *sexting*?

O *sexting* consiste no envio de imagens ou vídeos sexuais, produzidos pelo próprio remetente, normalmente através do telemóvel ou de outros dispositivos tecnológicos. O termo resulta da junção da palavra sexo (*sex*, em inglês) e do verbo inglês que denomina o ato de enviar mensagens de texto (*texting*, em inglês). Esta prática teve orignem nos países anglo-saxónicos em 2005 e, gradualmente, espalhou-se pelo resto do mundo.

Para diferenciar o *sexting* do aliciamento de menores, é importante notar que no primeiro caso, as imagens ou vídeos são feitos pelo mesmo remetente voluntariamente ou por outra pessoa, sendo que a participação dos intervenientes é consentida. Quando os menores são ludibriados ou coagidos a fazer *sexting* com o assediador, não é considerado *sexting*, uma vez que, embora em alguns casos pareça ser voluntário, os menores estão a ser manipulados. O *sexting* faz a distinção entre dois papéis, nomeadamente aqueles que realizam o ato de filmar, o chamado *sexting* ativo, e aqueles que recebem as imagens, ou seja, *sexting* passivo.

Alguns jovens fazem-no como um presente para os seus parceiros, como um elemento de *flirt* ou para atrair atenção. Esta prática comporta principalmente o risco de que o recetor possa partilhar as mensagens que recebe, ou usá-las para coagir e chantagear a outra pessoa para que envie mais imagens ou faça outras ações. Também é possível que ocorra uma distribuição inadvertida devido a descuido ou erro.

Definição
Sexting ...consiste no envio (pelo remetente) de imagens ou vídeos de conteúdo sexual via telemóvel aos seus pares (os recetores). A pessoa que protagoniza estes vídeos ou imagens é a mesma que os envia e fá-lo voluntariamente.

O *sexting* ativo ocorre quando a pessoa tira fotografias ou vídeos com poses sugestivas ou sexuais e os envia para outra pessoa.
O *sexting* passivo acontece quando as pessoas recebem fotografias tiradas por outras pessoas.
Porque é que o *sexting* é uma potencial ameaça para crianças e jovens adultos? Esta prática é um perigo grave na Internet porque, depois de enviar estas imagens, o remetente perde todo o controlo sobre elas. Desta forma, este conteúdo pode chegar a muito mais pessoas, de várias maneiras:

- O destinatário envia intencionalmente esse conteúdo a outras pessoas, que o reencaminham infinitamente até ser visto por uma audiência muito vasta.
- O remetente das imagens envia-as por engano à pessoa errada, que as partilha com outras pessoas.
- Alguém rouba o telemóvel, tablet ou o computador a um dos proprietários das imagens e publica as mesmas na Internet.
- Alguém acede sem autorização aos conteúdos do dispositivo móvel ou do computador de um dos proprietários das imagens, enviando-as para mais pessoas, publicando-as na Internet ou encaminhando-as para o seu protagonista para iniciar um processo de chantagem ou extorsão.

Essas imagens podem ir parar a múltiplos lugares:

- Nos dispositivos móveis dos conhecidos do remetente como, por exemplo, os seus próprios pais.
- Nas redes sociais, que podem ser de acesso público.
- Nas páginas de conteúdo sexual e/ou pornografia.
- Nas mãos dos aliciadores, que vêm nestes menores as presas perfeitas para acederem aos seus pedidos.

As consequências para a vítima são:

- Humilhação e linchamento social para o protagonista das imagens.
- O menor enfrenta o insulto público, afetando primeiramente a sua autoestima, numa idade em que a sua personalidade está a ser formada e depende em grande parte da imagem que projeta para os outros, pois a opinião dos outros é importante.
- Há também sentimentos de impotência, principalmente quando o caso é reportado aos pais ou educadores, bem como sentimentos de culpa por estar nessa situação.
- Estes sentimentos podem levar a uma profunda tristeza, ansiedade, depressão, diminuição ou aumento do apetite ou, em situações mais extremas, a tentativas de suicídio.

Importante
A descoberta da distribuição da imagem leva à perda de confiança em terceiros. Problemas de relacionamento no ambiente escolar contribuem para um isolamento social para evitar olhares, comentários insultuosos, etc.

A prevenção do *sexting* pode ser realizada por pais, mães, tutores e também pelos próprios menores.

Os pais ou tutores:

- Devem ensinar aos menores que o que partilham na Internet tem as suas consequências, e que mesmo que o partilhem em privado com uma pessoa muito próxima, isto pode conduzir a muitos problemas mais tarde.
- Incutir neles o respeito pelo seu corpo e pela sua intimidade e sublinhar que ninguém pode forçá-los a fazer nada que não queiram.
- Sempre que possível, estar a par da localização do computador e incentivar o uso de dispositivos móveis em espaços partilhados com a família.

Os menores devem evitar enviar qualquer tipo de fotos, mas sabe-se que à medida que crescem, começam também a fazer uso dessa funcionalidade nos dispositivos. Mesmo nesta transição para se tornarem adultos, é importante tomar algumas medidas:

- Não trocar fotografias íntimas, muito menos com estranhos.
- Não publicar imagens comprometedoras nas redes sociais ou na Internet - estas fotos são muito difíceis de apagar mais tarde e podem chegar a muitas pessoas.
- Se se enviar uma imagem, é mais seguro enviá-la sem a possibilidade de se ser identificado, sem mostrar o rosto, tatuagens, ou marcas que possam identificar facilmente a pessoa.
- Não enviar imagens com coordenadas de geolocalização - alguns telemóveis ou dispositivos têm a opção de marcar na imagem o sítio onde a foto foi tirada. Isto pode ser um perigo adicional em caso de divulgação da foto ou roubo do dispositivo, uma vez que terceiros podem saber onde foi tirada e localizar o menor.
- Se tirarmos uma fotografia que não queremos que seja divulgada, a melhor opção é apagá-la do dispositivo.

2. Aplicar conhecimentos

Exercício de ESCOLHA ÚNICA

Objetivo específico associado: Controlo Parental_02_01: Conhecer a definição para o termo *sexting*

Situação: O *Sexting* consiste no...
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira.

- Envio de mensagens sexuais ameaçadoras para uma criança ou um adolescente.
- Envio de imagens ou vídeos sexuais, produzidos pelo próprio remetente.
- Envio de conteúdos sexuais, tais como imagens ou vídeos produzidos pelo assediador.

Exercício de ESCOLHA ÚNICA

Objetivo específico associado: Controlo Parental_02_02: Saber a diferença entre o *sexting* ativo e passivo

Situação: O *sexting* ativo é quando...
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira.

- A pessoa tira fotografias ou vídeos com poses sugestivas ou sexuais e envia-os a outra pessoa.
- O assediador pede à outra pessoa para enviar imagens com poses sugestivas ou sexuais.
- O assediador ameaça a outra pessoa para que envie imagens com poses sugestivas ou sexuais.

Exercício de ESCOLHA ÚNICA

Objetivo específico associado: Controlo Parental_02_03: Conhecer os riscos associados à prática e disseminação do *sexting*

Situação: Depois de enviar estas imagens, o remetente perde todo o controlo sobre elas, porque...
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira.

- Há muitas consequências para a vítima.
- O assediador acumula mais poder.
- O conteúdo pode chegar a mais pessoas do que o pretendido.

Exercício de ESCOLHA ÚNICA

Objetivo específico associado: Controlo Parental_02_04: Conhecer os riscos associados à prática e disseminação do *sexting*

Situação: Para evitar o *sexting*:
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira.

- Os pais e tutores devem ensinar aos menores que tudo o que é partilhado na Internet tem as suas consequências.
- Os pais e tutores devem monitorizar tudo o que os menores fazem na Internet.
- Os pais e os tutores devem ensinar os menores a ter respeito pelo seu corpo.

3. Desenvolver conhecimento – O que é o aliciamento de menores?

O aliciamento é definido como o ciberbullying deliberadamente levado a cabo por um adulto com o intuito de estabelecer uma relação e controlo emocional sobre um menor, a fim de preparar terreno para o abuso sexual.

Em alguns casos é realizado entre menores, mas geralmente com uma diferença de idade entre ambas as partes, em que o interveniente mais velho é geralmente o assediador.

O objetivo do assédio é ganhar a confiança do menor, obter imagens ou vídeos de conteúdo sexual e até mesmo combinar encontros em pessoa. Estes atos podem constituir crimes de perversão, prostituição e abuso sexual de menores.

Este tipo de ciberbullying está intimamente relacionado com a pedofilia, uma vez que muitos assediadores também tiram partido das imagens que obtiveram para manipular e extorquir as vítimas, sob a ameaça que divulgarão as imagens se os menores não aceitarem as condições impostas pelo infrator.

Definição
Aliciamento de menores ...práticas levadas a cabo por adultos com o intuito de ganhar a confiança dos menores, geralmente para fins sexuais. Isto acontece maioritariamente na Internet mas, por vezes, o assediador tenta estabelecer contacto físico.

Normalmente, a conduta dos "*groomers*", isto é assediadores, segue as seguintes fases:

- **Gancho:** O perseguidor faz questões à vítima para a conhecer, pergunta a sua idade e localização geográfica. Depois, tenta conhecer os seus gostos e preocupações, adaptar-se a eles, apresentar pontos em comum com a vítima e ganhar a sua confiança. Aqui, o assediador não faz qualquer pressão ao menor e evita perguntas que possam assustar ou afastar a criança, mas tenta antes reforçar os laços de amizade com eles.
- **Lealdade:** Depois de fazer amizade com a vítima e de se mostrar amigável, interessante e com muitas semelhanças, o assediador certifica-se de que o seu novo amigo quer continuar a falar com ele. Para o conseguir, aborda temas de interesse mútuo, como desporto, música, escola, etc e depois introduz questões familiares, como com quem vive, como é a sua família, o que fazem os pais, etc.
- **Sedução:** Com toda a informação e confiança construídas até agora, o assediador dedica-se à sedução, incluindo tópicos sexuais nas conversas e tenta trocar imagens sexuais com a vítima. Através do elogio procura estimular no menor um sentimento de "dívida" levando a que o menos faça aquilo que o assediador pede.
- **Assédio:** Neste momento, o assediador já tem uma ideia próxima do que pode obter da criança. Ele tem a sua informação privada e familiar, conhece os seus gostos e receios e tem fotografias dele ou dela. O objetivo agora torna-se mais claro: estabelecer uma relação sexual, ainda que de modo virtual, numa primeira fase. É possível que nesta fase o assediador se mostre como é e use a chantagem, ameaças e manipulação para alcançar os seus objetivos.

Em alguns casos, as fases iniciais podem começar por ocorrer fisicamente, cara-a-cara, se o assediador for uma pessoa previamente conhecida da criança.

Em algumas situações, podem ocorrer duas fases adicionais:

- **Procura:** Numa primeira fase, graças a toda a informação que os menores colocam nas redes sociais não supervisionadas, em salas de *chat* e fóruns, o assediador procura as suas vítimas tendo em conta fatores como vulnerabilidade, necessidade emocional, baixa autoestima, solidão e pouca atenção dos pais.
- **Isolamento:** Nesta fase intermédia que envolve a fase de engate e sedução, o agressor aproveita a confiança que ganhou com a criança e a informação que reuniu sobre a vítima para tentar isolá-la dos amigos e da família, a fim de conseguir exercer um maior controlo, tornar-se a pessoa mais próxima do menor e evitar que partilhe o que está a acontecer com alguém.

As mudanças ou sintomas que a vítima sofre podem ser divididos em quatro grupos diferentes:

Mudanças de hábitos em relação a diferentes aspetos:

- Na utilização de dispositivos ou na própria Internet
- Na comparência às aulas, por exemplo, recorrendo a justificações falsas para as ausências
- Abandono ou ausência de atividades extracurriculares
- Oscilações nos tempos de estudo e no desempenho escolar
- Alterações das atividades de lazer
- Modificação dos hábitos alimentares
- Diminuição da concentração e da capacidade de subsistência
- Omissão nas comunicações através da Internet ou do telemóvel

Mudanças de humor:

- Mudança de humor
- Momentos de tristeza, apatia ou indiferença
- Atitudes pouco habituais de relaxamento e de tensão, inclusive reações agressivas
- Explosões momentâneas de agressividade

Mudanças nas suas relações:

- Mudanças estranhas nos grupos de amigos e/ou ausência súbita de relacionamento com amigos e outras interações sociais
- Falta de defesa ou reação exagerada a determinadas piadas ou observações públicas podem ser comentários aparentemente inofensivos mas, para a vítima, têm outro significado/impacto
- Medo ou oposição à saída de casa
- Reservas excessivas na comunicação
- Mudanças, por vezes radicais, nos grupos de amigos
- Mudanças na relação com os adultos, em termos da sua frequência e da sua dependência
- Mudanças nos grupos e ídolos ou modelos a seguir/imitar

Alterações e sintomas físicos e psicossomáticos, tais como:

- Modificações na linguagem corporal quando na presença de certas pessoas, evitando o contacto ou praticando o autoisolamento
- Quando em espaços escolares, existe um medo de frequentar o recreio ou estar em locais visíveis a outras pessoas
- Manifestações de doenças ou enfermidades frequentes
- Lesões físicas frequentes sem explicação razoável, perda ou deterioração do vestuário
- Tonturas frequentes entre outros sintomas incomuns
- Dores de cabeça ou de estômago que obrigam o menos a ausentar-se de atividades escolares

As principais recomendações para evitar situações de aliciamento são:

No núcleo familiar, é importante promover uma comunicação intrafamiliar fluida, que facilite o diálogo com as crianças acerca da Internet, das redes sociais e dos perigos potenciais relacionados com o seu uso, perigos esses que tornam essencial alertar os menores sobre os dados que não devem fornecer *online*.

É também aconselhável educar os menores para a utilização segura da Internet, ferramentas, serviços e redes sociais, enfatizando os conselhos que foram dados anteriormente relacionados com o não fornecimento de dados pessoais nem aceitar contactos por parte de estranhos. A ideia é formá-los, oferecendo-lhes os conhecimentos e ferramentas necessárias para que estes sejam cada vez mais

autónomos na utilização das redes. As medidas de supervisão e controlo devem ser adaptadas à idade dos meninos, meninas ou jovens que se pretende supervisionar.

Os centros educativos podem levar a cabo ações concretas contra o aliciamento, procurando ter, entre o pessoal docente, especialistas que canalizem e facilitem a informação e o funcionamento técnico de mecanismos e dispositivos.

Podem também adotar metodologias que facilitem a inserção e abordagem de problemas de aliciamento e medidas de prevenção no currículo escolar.

No caso dos menores, devem evitar fornecer imagens e informações comprometedoras a qualquer pessoa ou torná-las acessíveis a terceiros. Devem também rejeitar mensagens sexuais ou pornográficas e, em qualquer caso, pedir ajuda em situações novas ou delicadas, especialmente se envolverem insegurança ou angústia emocional.

3. Aplicar conhecimentos

Exercício de ESCOLHA ÚNICA

Objetivo específico associado: OE_Controlo Parental_03_01: Conseguir definir o termo aliciamento de menores

Situação: O aliciamento de menores é definido como…
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira

- Ciberbullying realizado deliberadamente por um adulto.
- Ciberbullying levado a cabo deliberadamente por um amigo da mesma idade.
- Ciberbullying realizado deliberadamente por um colega de turma na Internet.

Exercício de ESCOLHA ÚNICA

Objetivo específico associado: OE_Controlo Parental_03_02: Conhecer as fases e características do aliciamento

Situação: A preparação segue fases diferentes, sendo que a fase de engate é quando...
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira

- O assediador certifica-se de que o seu novo amigo quer continuar a falar com ele.
- O assediador faz perguntas à vítima a fim de as conhecer.
- O assediador procura as suas vítimas e informação acerca destes na Internet.

Exercício de ESCOLHA ÚNICA

Objetivo específico associado: OE_Controlo Parental_03_03: Ser capaz de identificar os sintomas de uma vítima de aliciamento

Situação: As mudanças que a vítima sofre podem ser divididas em quatro áreas diferentes:
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira

- Hábitos, humor, passatempos e saúde.
- Hábitos, estado de espírito, relações e saúde.
- Hábitos, humor, relações e psicossomático.

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

Exercício de ESCOLHA ÚNICA

Objetivo específico associado: OE_Controlo Parental_03_04: Conseguir explicar três estratégias de prevenção do aliciamento

Situação: De modo a evitar que os menores sofram de aliciamento, é aconselhável:
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira

- Controlar o que veem, não os deixar usar dispositivos quando estão sozinhos e colocar os aparelhos numa área partilhada.
- Estimular a comunicação, ensiná-los a utilizar diferentes ferramentas, dispositivos e redes sociais.
- Deixá-los usar a Internet apenas quando forem suficientemente autónomos.

4. Desenvolver conhecimento - O que é o ciberbullying?

Definição
Ciberbullying Ciberbullying é qualquer tipo de bullying que tem lugar com recurso a dispositivos digitais como computadores portáteis, tablets ou smartphones.

O infrator causa danos à vítima (também conhecida como 'ciber-vítima') na Internet, prejudicando a sua reputação *online* ao divulgar mensagens através das redes sociais como o Facebook, Instagram, Twitter, etc, publicando em blogs ou enviando informações via *email*, SMS, aplicações de *smartphones* como o WhatsApp ou o We*Chat*.

Um dos primeiros passos do ciberbullying tende a envolver um infrator que insulta ou ameaça a vítima, ameaçando vazar informações que podem prejudicar a sua reputação. A informação enviada pelo agressor sobre a pessoa que está a ser alvo de assédio pode ser verdadeira, sendo, neste caso, divulgada propositadamente pelo facto de ser negativa ou prejudicial aos interesses da pessoa alvo de assédio ou pode ser efetivamente falsa. Se assim for, pode ser categorizada como desinformação.

Exemplo
Por exemplo, uma rapariga recebe uma mensagem através do WhatsApp com um *link* para um *web*site que inclui algumas imagens da própria, nua. Um infrator pede à vítima que faça os seus trabalhos de casa ou enviará este *link* aos seus amigos e família.

Algumas das táticas regulares de ciberbullying que o predador irá fazer à vítima são:

- Insultar ou ofender outros pessoas através da Internet
- Pedir às vítimas que pratiquem automutilação ou que se suicidem
- Ameaçar
- Criar um *website* ou um blogue que inclua informações embaraçosas sobre a vítima
- Hacking de perfis de redes sociais, muitas vezes chamados *'sockpuppet'*
- Divulgação de dados privados da vítima
- Partilha de fotos de nudez
- Bullying por ciúmes
- Assédio com base na religião, raça ou orientação sexual

Em geral, o perseguidor, também conhecido como *cyberstalker*, será alguém próximo da vítima: um colega de classe, algum companheiro de atividades culturais ou desportivas e, na maioria das vezes, haverá um grupo de infratores e não apenas um indivíduo. Este tipo de comportamento é muito doloroso para a vítima, devido às características seguintes:

1. Persistência: Vivemos num mundo conectado 24 horas/7 dias por semana, onde a comunicação nunca para.
2. Permanência: A maior parte da informação publicada na Internet permanece para sempre na Internet e é pública. Além disso, uma vez iniciado o ciberbullying, os infratores não tendem a parar, mas aumentam os seus ataques.
3. Ocultação: As vítimas não querem falar sobre as agressões devido ao medo, por isso é difícil para os pais, os professores e outras autoridades perceberem o que ocorre.

Normalmente, quando os menores sofrem de assédio *online*, retraem-se para dentro de si próprios e isso afeta não só as suas condutas *online*, mas também a sua forma de viver no mundo real.

As vítimas de ciberbullying não querem continuar a ir aos lugares onde estas experiências traumáticas ocorrem. Estas vítimas deixam frequentemente de frequentar as atividades que costumavam gostar muito de fazer, começam inclusive a faltar às aulas, fingindo sentir-se doentes, o que compromete os seus resultados escolares e, por vezes, ficam mesmo doentes devido a distúrbios alimentares ou depressões.

Adicionalmente, estes aumentarão ou diminuirão a utilização dos dispositivos e tornar-se-ão mais protetores da sua privacidade, não deixando que ninguém em casa veja o que estão a fazer nas redes sociais em particular e na Internet em geral. Por vezes até eliminam os seus perfis e criam novas contas.

A fim de prevenir o ciberbullying existem algumas estratégias que podemos implementar:

- Os pais e professores devem falar com as crianças sobre o ciberbullying, reforçando e recompensando o bom comportamento para com os outros e concentrando-se não só no infrator mas também em terceiros.
- Os adultos devem ter regras claras sobre o conteúdo que deve ser visto e partilhado e a quantidade de tempo gasto nas redes sociais. Além disso, devem ser estabelecidas expectativas relativas a um comportamento digital correto.
- Na escola, os professores podem criar uma "caixa de correio de bullying" anónima, para que os alunos possam utilizar a mesma para dizer que estão a passar por este problema e para desencadear os protocolos de ciberbullying.

- Os pais e professores devem estar sempre atentos a qualquer mudança de humor das crianças, por mais ligeira que seja.

4. Aplicar conhecimento

Exercício de ESCOLHA ÚNICA

Objetivo específico associado: OE_Controlo Parental_04_01: Ser capaz de definir o termo ciberbullying

Situação: Qual das afirmações seguintes melhor descreve o ciberbullying?
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira

- Insultar ou ameaçar outros, tanto fisicamente como através da Internet.
- Assediar outras pessoas nas redes sociais, *websites*, aplicações ou utilizando qualquer outro canal digital.
- Assistir a qualquer comportamento negativo na Internet.

Exercício de ESCOLHA ÚNICA

Objetivo específico associado: OE_Controlo Parental_04_02: Conhecer os perfis envolvidos no ciberbullying e as suas características

Situação: Qual é a definição de ciber-vítima?
Tarefa: Escolha a opção correta de acordo com o princípio de escolha única: apenas uma frase é verdadeira.

- Aquele que insulta, ameaça ou vaza qualquer informação nociva ou má sobre outra pessoa.
- A pessoa que sofre os processos e muitas vezes retira-se para dentro de si mesma.
- O termo "ciber-vítima" é incorreto.

Exercício de ESCOLHA ÚNICA

Objetivo específico associado: OE_Controlo Parental_04_03: Conhecer as consequências do ciberbullying para o infrator e para a vítima

Situação: Qual dos pontos seguintes não é um indicador de que um menor sofre de ciberbullying?
Tarefa: Escolha a opção correta de acordo com o princípio de escolha única: apenas uma frase é verdadeira

- Prefere concentrar-se no estudo e geralmente melhora as suas notas.
- As vítimas normalmente eliminam os seus perfis nas redes sociais e começam novos perfis.
- As pessoas que sofrem de ciberbullying mudam o seu estado de espírito e retraem-se para dentro de si próprios.

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

Exercício de ESCOLHA ÚNICA

Objetivo específico associado:OE_Controlo Parental_04_04: OE_Controlo Parental_01_04: É possível explicar três estratégias de prevenção do ciberbullying.

Situação: Qual a melhor opção para evitar o ciberbullying?
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira

- Chamar a polícia assim que existir uma situação que se considere suspeita.
- Evitar a utilização de dispositivos eletrónicos em casa.
- Estabelecer regras claras sobre o que fazer e não fazer quando se utiliza a Internet.

5. Desenvolver conhecimento – O que é a dependência da Internet? Características como a curiosidade, ausência de conhecimento sólido, tempo livre e um lugar chamado Internet onde se podem encontrar todas as respostas a qualquer pergunta ou contactar com qualquer pessoa são terreno fértil para se passar a maior parte do tempo nesse lugar. Os menores têm todas essas características em comum.

A Internet expandiu o mundo para os adolescentes e crianças, permitindo-lhes socializar e expressar-se, aumentando os seus recursos para estudar introduzindo, simultaneamente, uma interação e aprendizagem única. Estes são os aspetos positivos da Internet, a qual também tem um lado negro, que não podemos ignorar.

Existem dois tipos de vícios: Pode-se ficar viciado numa substância, mas também se pode ficar viciado num comportamento. Este tipo de dependência classifica-se frequentemente como "novos vícios", " vícios não-químicos" ou "vícios comportamentais". Por vezes, quando se passa muito tempo a fazer algo, pode-se desenvolver um vício a este processo. Quando se é viciado em passar o tempo na Internet, isso tem um nome: dependência da Internet.

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

Definição
Dependência da Internet A dependência da Internet é um transtorno de dependência, também referido como um uso compulsivo da Internet. Não consiste apenas em passar muito tempo na Internet, mas também em deixar que isto interfira com a vida quotidiana devido a um vício na sua utilização.

Este distúrbio tem aumentado profusamente devido ao facto de se viver numa sociedade permanentemente conectada. O que quer que precises pode ser encontrado na Internet: se não encontrares o tamanho certo de uma camisa numa loja, podes comprá-la na Internet; se não quiseres cozinhar, podes encomendar comida para ser entregue à tua porta; se não tiveres um irmão com quem jogar consola, podes jogar com um estranho *online*; se precisares de estudar, todos os livros, artigos e outros recursos estão disponíveis para acesso via Internet.

Nestas circunstâncias, é muito difícil distinguir se um menor está a experimentar qualquer tipo de distúrbio de dependência da Internet. No entanto, existem algumas formas de descobrir este tipo de vício. Para tirar as dúvidas, é responsabilidade dos pais fazerem a si próprios algumas perguntas:

- O menor é incapaz de parar de utilizar as redes sociais quando lhe é pedido?
- O menor está compulsivamente a fazer compras *online*?
- Ele/Ela está a jogar jogos de vídeo *online* em excesso?
- Ele/Ela está a jogar na Internet?
- O menor passa o dia inteiro em frente ao computador?
- O menor tem problemas com as relações sociais fora da Internet?
- Ele/Ela está a experienciar algum problema por não fazer os seus trabalhos de casa/as suas notas escolares estão a diminuir?

Se a resposta a qualquer uma destas perguntas for sim, devemos olhar profundamente para o comportamento do menor porque ele ou ela pode sofrer de um vício na Internet ou ser dependente da Internet.

No entanto, estes indicadores são apenas possíveis indicadores. Como dissemos acima, vivemos num mundo conectado ininterruptamente e a linha entre o uso normal da rede e o uso abusivo da mesma é muito ténue. Assim, é necessário aferir se este tipo de comportamento tem ou não qualquer impacto negativo na vida do menor. Se o menor não for capaz de dar prioridade aos seus deveres e tarefas em vez de estar *online* é absolutamente claro que este tem um problema.

Exemplo
À hora do jantar, o filho é chamado para se juntar à família à mesa, mas ele não vem. Os pais chegam ao ponto de o chamar três vezes, mas ele tem o *smartphone* na mão e não está disposto a parar o que está a fazer. Mesmo à mesa, ele continua a verificar as histórias no seu perfil do Instagram. O pai pega no *smartphone* e guarda-o no seu bolso deixando a criança literalmente em sofrimento porque não pode continuar a fazer o que estava a fazer.

Outra forma de descobrir se o menor sofre deste distúrbio é analisar a quantidade de tempo gasto a usar dispositivos digitais, a frequência e as manifestações emocionais de não estar ligado à rede. Se o menor parece estar deprimido, ansioso ou agitado quando não está *online*, ou se passa por mudanças de humor frequentes, a dependência da Internet pode ser a razão pela qual o menor se sente deprimido, ansioso ou agitado.

A dependência da Internet também pode ter manifestações físicas, tais como má nutrição, dor no pescoço, insónias, olhos secos ou má higiene.

A fim de evitar a dependência da Internet, há algumas medidas úteis a serem implantadas:

- Limitar a quantidade de tempo gasto com a utilização de dispositivos digitais, não só através da estipulação de um número fixo de horas, mas também a altura do dia em que se pode aceder aos dispositivos. Por exemplo, definir a proibição do computador após o jantar.
- Organização de debates na escola sobre a utilização correta da Internet.
- Dar prioridade aos momentos familiares em detrimento do uso das tecnologias.
- As crianças devem usar sempre a Internet sob a supervisão de um adulto.
- Os instrumentos de controlo parental (ver capítulo 1) devem ser instalados a fim de evitar a entrada de crianças e adolescentes em *sites* de jogo ou pornográficos.

5. Aplicar conhecimentos

Exercício de ESCOLHA ÚNICA

Objetivo específico associado: OE_Controlo Parental_05_01: Conhecer a definição do termo dependência da Internet

Situação: Qual é a afirmação mais adequada para definir a dependência da Internet?
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira.

- Desordem que consiste em passar muito tempo na Internet.
- Vício que impossibilita que a vítima viva uma vida normal devido à dependência da utilização da Internet.
- Perseguição de uma vítima através da ameaça de divulgação de fotos nuas num *website*.

Exercício de ESCOLHA ÚNICA

Objetivo específico associado: OE_ Controlo Parental_05_02: Conseguir identificar sinais de alarme sobre a utilização abusiva da Internet

Situação: Qual/quais das seguintes afirmações não constitui um sinal de alarme sobre a utilização abusiva da Internet?
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira.

- O menor não quer estar *online* porque tem medo de um *cyberstalker*.
- O menor joga excessivamente videojogos *online*.
- O menor tem problemas com as relações sociais fora da Internet.

Exercício de ESCOLHA ÚNICA

Objetivo específico associado: OE_Controlo Parental_05_03: Conhecer três formas de prevenir a dependência da Internet.

Situação: Qual é a melhor estratégia para evitar a utilização abusiva da Internet?
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira.

- Limitar os momentos de utilização da Internet durante o dia.
- Dar às crianças a oportunidade de navegar na Internet como desejarem.
- Controlar as contas das redes sociais das crianças.

6. Desenvolver conhecimento - O que é a divulgação de informação?

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

Hoje em dia, quase toda a nossa vida está exposta na Internet. Se formos pirateados, o *hacker* encontrará as nossas palavras-passe de cartão de crédito, terá acesso aos nossos perfis de redes sociais, às nossas contas de correio eletrónico e ao nosso histórico de navegação.

Devido a este excesso de exposição, devemos cuidar dos nossos dados e evitar a sua divulgação. No entanto, mesmo que estejamos empenhados numa utilização responsável da Internet, devemos assegurar que os menores estão tão empenhados como nós, porque eles fazem uso dos dispositivos familiares, bem como dos seus próprios dispositivos.

Uma vasta gama de crimes envolve a extração de dados, ou o vazamento de dados e os adolescentes e crianças são um dos grupos mais prováveis de partilhar os seus dados, devido a duas principais razões:
1. Eles, como nativos digitais, passam mais tempo *online*.
2. Eles não experienciam uma sensação de perigo ao navegar na Internet.

Várias técnicas podem ser utilizadas para divulgar dados secretamente a partir de um dispositivo digital. Por vezes, os infratores 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 senhas dos utilizadores para que estes possam desfrutar de um serviço *online*. Contudo, na maioria das vezes, os menores partilham os seus dados porque estes não estão conscientes do perigo, pelo que é vital incitar um comportamento mais responsável na Internet.

Definição
Divulgação de informação Divulgar significa expor, involuntariamente, informação privada que não deve ser revelada a outras pessoas. Pode acontecer através de hacking ou porque a fonte não se apercebe da importância de manter a privacidade dos dados privados.

Podemos dizer que há divulgação de informação quando alguém cede a sua informação pessoal ou a coloca numa circunstância em que esta pode ser descoberta por pessoas que a podem utilizar de forma prejudicial, arriscando a privacidade ou segurança do proprietário dos dados.

Este problema tem aumentado de forma significativa com o aprimoramento e sofisticação do hacking: o *malware* e o *spyware* são apenas alguns dos problemas mais comuns. Mas, como dissemos acima, um dos principais problemas é a tendência das pessoas para partilharem tanta informação sobre eles

próprios. Isto constitui um problema crescente, muito por causa das aplicações de *smartphones*, que nos pedem acesso a informações como localização, contactos, etc, a fim de usufruirmos dos seus serviços. Esta é uma mudança de paradigma que provem da Internet. Na televisão, os conteúdos são exibidos em troca da atenção dos espectadores. Na Internet, as aplicações e serviços são acedidos em troca de dados pessoais.

Isto não constituiria um problema em si se os dados revelados não fossem sensíveis. Mas, será que uma criança sabe se a informação exposta é sensível e potencialmente arriscada ou não? Mesmo os adultos, por vezes, não conseguem perceber esta diferença. Para descobrir se os menores estão a divulgar informação, os pais devem fazer-lhes algumas perguntas:

- Em que *sites* anda a navegar?
- Quais as aplicações que está a descarregar?
- Alguém lhe pediu para partilhar algum dado pessoal para usufruir de um serviço, tal como endereço de correio eletrónico ou número de cartão de crédito?

Exemplo
O Paul quer descarregar uma aplicação no seu *smartphone* para falar com os seus amigos. Apesar de a aplicação ser gratuita, ele é obrigado a preencher um formulário que inclui o cartão de crédito e o código de verificação do cartão.

Se uma aplicação ou serviço *online* pedir qualquer informação para o seu funcionamento que não costumava pedir anteriormente, ou se alguém estiver a pedir informações privadas pouco normais, como uma morada de casa, é provável que exista o risco de divulgação de informações sensíveis.

Por vezes, a fuga de dados ocorre devido a uma infeção por um vírus 'Cavalo de Tróia' (*Trojan Horse*). Se tiver qualquer suspeita relativamente a um *software*, não deve fazer download do mesmo. Deve suspeitar de *software* que permita assistir a filmes ou programas em *streaming* gratuitamente, bem como *web*sites e aplicações de jogos. A melhor maneira de proceder é descarregar serviços apenas após passarem por uma verificação parental.

A fim de evitar a divulgação acidental de informação, existem algumas estratégias que podem ser implementadas pelos pais:

- Dizer ao menor para não dar quaisquer dados pessoais sem autorização
- Nunca manter palavras-passe ou códigos PIN no *browser* de um dispositivo partilhado com crianças
- Instalar programas de controlo parental como, por exemplo, Qustodio, Secure Kids ou Parental Click
- Falar com os menores sobre não colocar nenhuma foto que permita a estranhos saberem o endereço exato onde vivem ou a escola onde estudam.
- A melhor tática de prevenção é falar frequentemente com os menores sobre os riscos de divulgação de informação e sobre a importância de uma utilização responsável da Internet.

6. Aplicar conhecimentos

Exercício de ESCOLHA ÚNICA

Objetivo específico associado: OE_ Controlo Parental_06_01: Saber dar a definição de divulgação de informação

Situação: Qual é a afirmação mais correta para definir a divulgação de informação?
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira.

1. Vício por dispositivos digitais.

2. Vazamento de informação de conteúdo sensível.
3. Lançamento de informações falsas na Internet.

Exercício de ESCOLHA ÚNICA

Objetivo específico associado: OE_ Controlo Parental_06_02: Ser capaz de identificar quando as crianças estão a divulgar informação

Situação: Qual das próximas não é um sinal de alarme relativamente à divulgação de informação?
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira.

1. O menor pede permissão para descarregar uma aplicação para *smartphone*.
2. O menor é coagido a enviar o número do cartão de crédito.
3. Os menores publicam algumas fotografias tiradas à porta de casa.

Exercício de ESCOLHA ÚNICA

Objetivo específico associado: OE_ Controlo Parental_06_03: Saber explicar três formas de prevenir a fuga de informação

Situação: Qual seria a melhor estratégia para evitar a fuga de informação?
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira.

1. Não manter as senhas e códigos PIN no *browser*.
2. Permitir que os menores descarreguem qualquer aplicação que desejem.
3. Divulgar fotografias pessoais nas redes sociais.

Fontes

Garaigordobil, M. (2019). Prevención del cyberbullying: variables personales y familiares predictoras de ciberagresión.. Obtido em: https://dialnet.unirioja.es/servlet/articulo?codigo=7041022

Garcia Ganchon, J. O. Seguridad y riesgos: Ciberbullying, grooming y sexting. Obtido em: http://openaccess.uoc.edu/*web*apps/o2/handle/10609/72526

Stuttgen, K., McCague, A., Bollinger, J., Dvoskin, R., & Mathews, D. (2020). Whether, when, and how to communicate genetic risk to minors:'I wanted more information but I think they were scared I couldn't handle it'. Journal of Genetic Counseling. Obtido em: https://*online*library.wiley.com/doi/abs/10.1002/jgc4.1314

Villanueva-Blasco, V. J., & Serrano-Bernal, S. (2019). Patrón de uso de internet y control parental de redes sociales como predictor de sexting en adolescentes: una perspectiva de género. Revista de Psicología y Educación. Journal of Psychology and Education, 14(1), 16-26. Obtido em :https://www.almendron.com/tribuna/wp-content/uploads/2020/05/patron-de-uso-de-internet.pdf

Para relembrar

Resumo

Este módulo centra-se na importância do controlo parental para proteger crianças e adolescentes de situações perigosas quando usam a Internet ou dispositivos tecnológicos.

Uma vez que estamos num mundo em mudança, onde a tecnologia evolui dia após dia, os perigos que os menores sempre enfrentaram no passado podem agora entrar nas suas vidas através de novas vias. Estes riscos podem também propagar-se e ampliar-se facilmente através da Internet.

Por forma a cumprir com a tarefa de manter os menores em segurança enquanto estes interagem e expandem o seu círculo, é necessário conhecer os riscos e as formas de os evitar. Para tal, é importante definir as formas como os perigos podem atingir os mais jovens (redes sociais, jogos, plataformas de vídeo, etc) e as ferramentas disponíveis para os deter ou detetar.

Tendo exposto as diferentes maneiras como os perigos atingem as crianças e adolescentes e as ferramentas e funções para os manter sob controlo, torna-se necessário especificar quais são estes riscos e as suas consequências. Alguns dos perigos que os menores enfrentam são o *sexting*, o aliciamento, o ciberbullying, a dependência da Internet e a divulgação de informação. Estes perigos devem ser compreendidos para melhor se lidar com eles e, inclusive, para os detetar.

Algumas destas consequências podem afetar diretamente a saúde emocional e até física dos menores. Se prestarmos atenção, há efeitos visíveis que podem atacar o problema pela sua raiz.

Contudo, a melhor opção, sempre que possível, é evitar situações de *sexting*, aliciamento de menores, ciberbullying, dependência da Internet, e divulgação de dados, em vez de lidar com eles após se tornarem realidade. Para o fazer, serão expostas formas de exercer o controlo parental na Internet, bem como dispositivos tecnológicos e algumas ferramentas. Também será possível encontrar algumas dicas para manter os menores afastados de cada um dos perigos supramencionados.

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

As respostas corretas estão assinaladas a negrito

Situação: Que ameaças tecnológicas afetam os menores?
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira.

- Só existe o ciberbullying
- **Existem múltiplos perigos que podem afetar crianças, adolescentes e jovens na Internet (ciberbullying, *sexting*,...)**
- Não há nenhuma ameaça tecnológica que afete os menores.

Situação: Qual é a definição do termo controlo parental?
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira.

- **O "controlo parental" corresponde à forma como os pais supervisionam e intervêm se necessário, para assegurar que as experiências e processos de socialização e crescimento pessoal dos seus filhos ocorrem de forma adequada e sem riscos para eles.**
- O "controlo parental" é uma ferramenta que permite aos pais controlar e/ou limitar o conteúdo ao qual os seus filhos têm acesso *online,* a partir dos seus dispositivos, sejam eles computadores, telemóveis ou tablets.
- O "controlo parental" é uma ameaça tecnológica que pode afetar menores.

Situação: Para que serve o controlo parental?
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira.

- **Para controlar e/ou limitar o conteúdo a que as crianças têm acesso na Internet a partir dos seus dispositivos, sejam eles computadores, telemóveis ou tablets.**
- Para dar às crianças a oportunidade de navegar na Internet como desejarem.
- Para controlar as contas das redes sociais das crianças.

Situação: Como funciona o controlo tecnológico parental?
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira.

- O controlo tecnológico parental previne que uma criança aceda a conteúdo impróprio através de um bloqueio no roter da internet.
- O controlo tecnológico parental evita a utilização de dispositivos eletrónicos em casa através do uso de passwords online.
- **O controlo tecnológico parental pode ser exercido a partir de diferentes pontos: servidores externos e DNS, a partir do próprio dispositivo, *software*, browser de Internet ou *apps*.**

Situação: O *Sexting* consiste no...
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira.

- Envio de mensagens sexuais ameaçadoras para uma criança ou um adolescente.
- **Envio de imagens ou vídeos sexuais, produzidos pelo próprio remetente.**
- Envio de conteúdos sexuais, tais como imagens ou vídeos produzidos pelo assediador.

Situação: O *sexting* ativo é quando...
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira.

- **A pessoa tira fotografias ou vídeos com poses sugestivas ou sexuais e envia-os a outra pessoa.**
- O assediador pede à outra pessoa para enviar imagens com poses sugestivas ou sexuais.
- O assediador ameaça a outra pessoa para que envie imagens com poses sugestivas ou sexuais.

Situação: Depois de enviar estas imagens, o remetente perde todo o controlo sobre elas, porque...
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira.

- Há muitas consequências para a vítima.
- O assediador acumula mais poder.
- **O conteúdo pode chegar a mais pessoas do que o pretendido.**

Situação: Para evitar o *sexting*:
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira.

- **Os pais e tutores devem ensinar aos menores que tudo o que é partilhado na Internet tem as suas consequências.**
- Os pais e tutores devem monitorizar tudo o que os menores fazem na Internet.
- Os seus pares devem ensinar-lhes a ter respeito pelo seu corpo.

Situação: O aliciamento de menores é definido como…
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira

- **Ciberbullying realizado deliberadamente por um adulto.**
- Ciberbullying levado a cabo deliberadamente por um amigo da mesma idade.
- Ciberbullying realizado deliberadamente por um colega de turma na Internet.

Situação: A preparação segue fases diferentes, sendo que a fase de engate é quando...
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira

- O assediador certifica-se de que o seu novo amigo quer continuar a falar com ele.
- **O assediador faz perguntas à vítima a fim de as conhecer.**
- O assediador procura as suas vítimas e a sua informação na Internet.

Situação: As mudanças que a vítima sofre podem ser divididas em quatro áreas diferentes:
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira

- Hábitos, humor, passatempos e saúde.
- Hábitos, estado de espírito, relações e saúde.
- **Hábitos, humor, relações e psicossomático.**

Situação: De modo a evitar que os menores sofram de aliciamento, é aconselhável:
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira

- Controlar o que veem, não os deixar usar dispositivos quando estão sozinhos e colocar os aparelhos numa área partilhada.
- **Estimular a comunicação, ensiná-los a utilizar diferentes ferramentas, dispositivos e redes sociais.**
- Deixá-los usar a Internet apenas quando forem suficientemente autónomos.

Situação: Qual das afirmações seguintes melhor descreve o ciberbullying?
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira

- Insultar ou ameaçar outros, tanto fisicamente como através da Internet.
- **Assediar outras pessoas nas redes sociais, *websites*, aplicações ou utilizando qualquer outro canal digital.**
- Assistir a qualquer comportamento negativo na Internet.

Situação: Qual é a definição de ciber-vítima?
Tarefa: Escolha a opção correta de acordo com o princípio de escolha única: apenas uma frase é verdadeira.

- Aquele que insulta, ameaça ou vaza qualquer informação nociva ou má sobre outra pessoa.
- **A pessoa que sofre os processos e muitas vezes retira-se para dentro de si mesma.**
- O termo "ciber-vítima" é incorreto.

Situação: Qual dos pontos seguintes não é um indicador de que um menor sofre de ciberbullying?
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira

- **Prefere concentrar-se no estudo e geralmente melhora as suas notas.**
- As vítimas normalmente eliminam os seus perfis nas redes sociais e começam novos perfis.
- As pessoas que sofrem de ciberbullying mudam o seu estado de espírito e retraem-se para dentro de si próprios.

Situação: Qual a melhor opção para evitar o ciberbullying?
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira

- Chamar a polícia assim que existir uma situação que se considere suspeita.
- Evitar a utilização de dispositivos eletrónicos em casa.
- **Estabelecer regras claras sobre o que fazer e não fazer quando se utiliza a Internet.**

Situação: Qual é a afirmação mais adequada para definir a dependência da Internet?
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira.

- Desordem que consiste em passar muito tempo na Internet.
- **Vício que impossibilita que a vítima viva uma vida normal devido à dependência da utilização da Internet.**
- Perseguição de uma vítima através da ameaça de divulgação de fotos nuas num *website*.

Situação: Qual das afirmações não constitui um sinal de alarme sobre a utilização abusiva da Internet?
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira.

- **O menor não quer estar *online* porque tem medo de um *cyberstalker*.**
- O menor joga excessivamente videojogos *online*.
- O menor tem problemas com as relações sociais fora da Internet.

Situação: Qual é a melhor estratégia para evitar a utilização abusiva da Internet?
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira.

- **Limitar os momentos de utilização da Internet durante o dia.**
- Dar às crianças a oportunidade de navegar na Internet como desejarem.
- Controlar as contas das redes sociais das crianças.

Situação: Qual é a afirmação mais correta para definir a divulgação de informação?
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira.

- Vício por dispositivos digitais.
- **Vazamento de informação de conteúdo sensível.**
- Lançamento de informações falsas na Internet.

Situação: Qual das próximas não é um sinal de alarme relativamente à divulgação de informação?
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira.

- **O menor pede permissão para descarregar uma aplicação para *smartphone*.**
- O menor é coagido a enviar o número do cartão de crédito.
- Os menores publicam algumas fotografias tiradas à porta de casa.

Situação: Qual seria a melhor estratégia para evitar a fuga de informação?
Tarefa: Escolher a opção certa usando o princípio de escolha única: apenas uma frase é verdadeira.

- Não manter as senhas e códigos PIN no *browser*.
- Permitir que os menores descarreguem qualquer aplicação que desejem.
- Divulgar fotografias pessoais nas redes sociais.