



Unidade de conteúdo

Proteção contra conteúdos impróprios

Projeto: B-SAFE

Número: 2018-1CZ01-KA204-048148

Nome do autor: bit cz training

Última data de processamento: 28.10.2020

Funded by the
Erasmus+ Programme
of the European Union



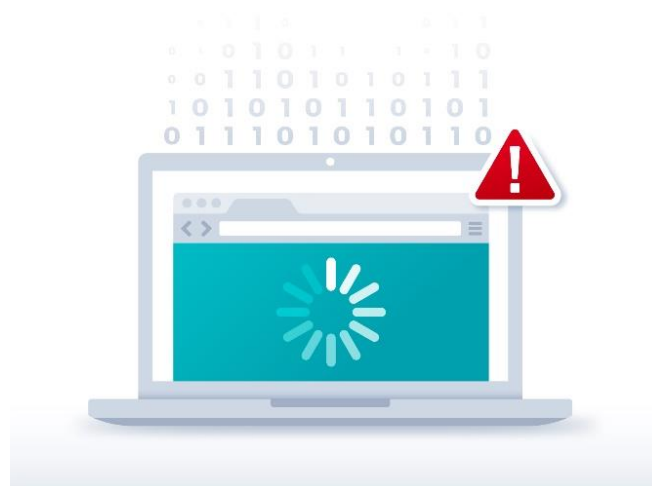
"The European Commission support for the production of this publication does not constitute an endorsement of the contents which reflects the views only of the authors, and the Commission cannot be held responsible for any use which may be made of the information contained therein."



Proteção contra conteúdos impróprios

Introdução

Nesta época digital, a Internet oferece imensas maneiras de explorar um mundo virtual sem as limitações do mundo real. O conteúdo da Internet não é dividido em áreas apropriadas à idade ou ao desenvolvimento. E esse é o problema! Alguns conteúdos podem ser ilegais, inapropriados, ofensivos ou impróprios para determinadas faixas etárias. Sem supervisão ou orientação, qualquer pessoa, mesmo uma criança pequena, pode encontrar conteúdos que sejam perturbadores, explícitos ou inapropriados. Muitos *websites* perturbadores não são 'ilegais', o que significa que ninguém os controla ou gere. A visualização acidental de conteúdos *online* pode ter um efeito traumático, especialmente em crianças. Alguns exemplos de conteúdos inapropriados são a promoção do ódio com base na raça, religião, deficiência, preferência sexual, o extremismo violento, conteúdo sexualmente explícito e violência real ou simulada. É importante que os pais protejam e orientem os seus filhos quando estes dão os seus primeiros passos na Internet, e educá-los para que se tornem utilizadores responsáveis e independentes da Internet.



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

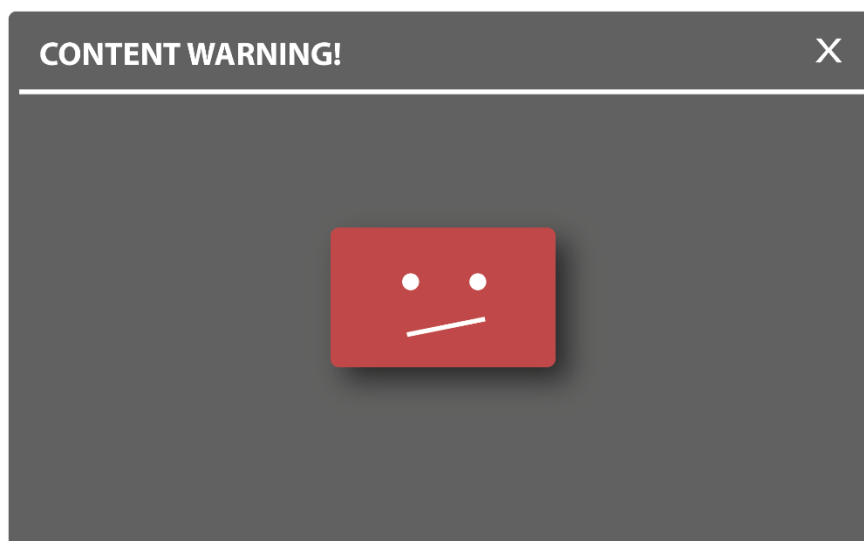
Depois de aprenderes os conteúdos desta unidade, saberás o que é conteúdo impróprio, o que este abrange e como te protegeres contra o mesmo.

Além disso, aprenderás mais sobre métodos de difusão de conteúdos inapropriados e sobre o seu impacto na vida quotidiana.



1. O que é conteúdo impróprio?

Conteúdo impróprio é um termo usado para caracterizar um vasto e cada vez maior número de diferentes tipos de conteúdo problemático *online*.



Geralmente, conteúdo impróprio é tudo o que viola os direitos das crianças, como definidos na Convenção sobre os Direitos da Criança, e tudo o que viola os direitos humanos, como definidos na Declaração Universal dos Direitos Humanos, em particular o direito à vida, à privacidade, à informação, à proteção, e o direito de participar na sociedade, de ser protegido contra abusos e violência. Este tipo de conteúdo pode compreender qualquer coisa desde o discurso de ódio até às imagens de autoflagelação ou *websites* 'pró-ana' (promotores da anorexia). O conteúdo inapropriado pode incluir os seguintes tópicos:

- Pornografia
- Comportamentos violentos ou extremistas
- Produtos perigosos
- Racismo ou ódio
- *Websites* pró-anorexia ('pró-ana')
- *Websites* com conteúdo extremista

De maneira a melhor caracterizar estes subtópicos, vamos explorá-los em pormenor:

Pornografia

A pornografia caracteriza-se por ser uma descrição explícita ou uma imagem destinada a estimular sentimentos sexuais. No entanto, a pornografia pode ou não ser obscena; pode não ser obscena se se argumentar que a obra tem valor literário, artístico, político ou científico. Contudo, a falta de consenso dificulta as tentativas objetivas de estipular uma só definição de pornografia.

Definição
As definições de pornografia variam consoante a época e o local: algo rotulado como pornografia há uns anos pode ser agora considerado apenas erótico. A pornografia na Internet é qualquer pornografia acessível pela Internet, primariamente via <i>websites</i> , partilha de ficheiros <i>peer-to-peer</i> (entre pares), ou através de grupos de notícias da Usenet. A disponibilidade do acesso público generalizado à <i>World Wide Web</i> no final dos anos 90 levou ao crescimento da pornografia na Internet.



Seguem-se alguns exemplos de Pornografia na Internet:

- Representações de nudez em que o sujeito está nu ou minimamente vestido, e em que a roupa não seria aceitável num contexto público apropriado.
- Representações, animações ou ilustrações de atos sexuais ou poses sexualmente sugestivas.
- Conteúdos que retratam fetiches sexuais.
- Conteúdo obsceno ou profano.
- Conteúdo que retrata, descreve ou encoraja a bestialidade.
- Aplicações que promovem entretenimento relacionado com o sexo, serviços de *escort* ou outros serviços que possam ser interpretados como proporcionando atos sexuais em troca de compensações.

Comportamentos violentos ou extremistas

A violência não é apenas da esfera dos jogos de computador ou dos filmes. A Internet também lhe dá algum palco, especialmente em portais de partilha de vídeos, onde aparecem vídeos brutais de ação ao vivo, bem como ataques ou eventos reais com um fim trágico. Existem mesmo portais especializados na recolha de *links* com fotos ou vídeos cruéis.

O conteúdo violento comum na Internet refere-se a representações gráficas ou descrições de violência realista ou ameaças de violência a qualquer pessoa ou animal. Também existem aplicações que incluem manifestações de violência. Estas aplicações podem promover automutilação, suicídio, distúrbios alimentares, jogos aparentemente inofensivos, ou outros atos que possam resultar em ferimentos graves ou morte.

Em casos extremos, pode encontrar-se conteúdo relacionado com terrorismo, inclusive conteúdo que promove atos terroristas, incita a violência ou celebra ataques terroristas.

Não esquecer

O conteúdo relacionado com o terrorismo ou a violência pode server um propósito educacional, documental, científico ou artístico. Para esse tipo de propósito, é necessário considerar cuidadosamente a utilização do conteúdo e explicar consistentemente a nocividade desses comportamentos.

Produtos perigosos

Muitas pessoas não compreendem que a Internet é um meio capaz de oferecer e facilitar a venda de explosivos, armas de fogo, munições ou acessórios para armas de fogo. Outras possibilidades incluem componentes que servem para o fabrico de explosivos, armas de fogo, munições, acessórios de armas restritos ou outras armas, bem como instruções para transformar uma arma de fogo numa arma com capacidades de disparo automáticas ou automáticas simuladas.

O “*darknet market*” ou “*cryptomarket*” é um *website* comercial ilegal alojado num *website* privado não-público chamado “*darknet*”, o qual só pode ser acedido com *software*, configurações ou autorização específica. Funciona principalmente como um Mercado negro, para a venda ou intermediação de transações envolvendo drogas, armas cibernéticas, armas físicas, dinheiro falso, dados de cartões de crédito roubados, documentos falsificados, drogas ilícitas, esteroides e outros bens ilícitos, mas também bens legais.

Racismo ou ódio

A promoção ou incitação de ódio direcionada a indivíduos ou grupos, com base na raça ou origem étnica, religião, deficiência, idade, nacionalidade, estatuto de veterano, orientação sexual, género,



identidade de género, ou qualquer outra característica também é um tipo comum de conteúdo impróprio associado à discriminação ou marginalização sistémica. As afirmações feitas nesse sentido pretendem provar que estes indivíduos ou grupos são desumanos, inferiores ou dignos de serem odiados. As manifestações de racismo ou ódio incluem características negativas (por exemplo, maliciosas, corruptas, perversas, etc.), declarações de que o grupo é uma ameaça ou discurso que objetiva encorajar outros a acreditar que as pessoas devem ser odiadas ou discriminadas por serem membros de um grupo específico.

A Internet concede espaço ilimitado para a publicação de praticamente qualquer conteúdo, texto, vídeo, fotografia ou música. Adicionalmente, qualquer pessoa – seja um indivíduo ou um grupo de pessoas, uma organização ou uma empresa – pode afirmar a sua presença na Internet através de um *blog*, *website* ou perfil numa rede social. Apesar de todos os esforços feitos no sentido de regular o conteúdo impróprio, as pessoas encontram sempre novas formas e oportunidades para obter esse conteúdo na Internet. As formas mais comuns de divulgação incluem:

Websites pró-anorexia

Os *websites*, *blogs*, fóruns e grupos de redes sociais ‘pró-ana’ representam um movimento que entende a anorexia como um estilo de vida, não uma doença. Os anoréticos não vêm nada de errado com o seu estilo de vida, mas compreendem que o seu meio não vê a questão da mesma maneira e oferece resistência, pelo que estes indivíduos reúnem-se e procuram apoio uns nos outros. Através desta validação da sua experiência patológica e dos seus comportamentos em *websites* e redes sociais, estes garantem um sentido de *feedback* positivo. As opiniões sobre os espaços ‘pró-ana’ variam – há quem acredite que estes *sites* são ambientes seguros para as pessoas anoréticas discutirem a sua doença e apoiarem aqueles que optam pela recuperação, mas também há quem argumente que os *sites* ‘pró-ana’ dão mais força à opinião de que a anorexia nervosa não é uma doença mas uma opção de vida que deve ser respeitado pelos médicos e pelas famílias.

Websites com conteúdo extremista

Os *websites* com conteúdo extremistas muitas vezes parecem inocentes à primeira vista: fornecem informações atrativas sobre tópicos como eventos históricos, mas distorcem os factos e referem outras fontes de informação já manipuladas por uma perceção alterada do mundo. Do mesmo modo, os extremistas tendem a fazer uso, por exemplo, de apresentações de grupos musicais, escondendo conteúdo extremista em textos publicados por esses grupos.

Redes sociais

Tal como acontece com os jornais e as televisões, não é permitida a distribuição de conteúdo ilegal – tal como pornografia infantil ou conteúdo violento – na Internet. Apesar de todos os esforços para regulamentar estas situações, este tipo de conteúdo continua a aparecer na Internet. Além disso, a Internet providencia espaço para a distribuição de conteúdo legal mas impróprio, tal como pornografia normal ou conteúdo com teor violento, o que pode interferir com o desenvolvimento saudável das crianças.

No contexto da comunicação *online*, está a tornar-se cada vez mais comum o envio voluntário de mensagens sexualmente sugestivas e imagens ou vídeos íntimos. E com o *boom* das redes sociais, a distribuição de tais conteúdos é ainda mais fácil.

Por vezes, é muito difícil dizer o que é e o que não é um conteúdo impróprio.

A pornografia é muitas vezes confundida com o termo erotismo.

Qual é a diferença?



Aquilo que constitui pornografia e erotismo varia consoante a perspetiva de diferentes grupos e diferentes indivíduos. Esta categorização é também muito passível de variar com o tempo – aquilo que era considerado pornográfico no início dos anos 1900 pode, agora, ser considerado erótico.

O critério usado para distinguir entre erótico e pornográfico está intimamente relacionado com os valores morais, estéticos e religiosos de cada um. Ainda que muitas pessoas pensem nestas duas orientações da sexualidade humana como coincidentes, existe uma diferença significativa entre elas. Ao contrário da pornografia, o erotismo não apela exclusivamente aos nossos sentidos ou apetites carnis, mas envolve também o nosso sentido estético e o nosso julgamento sobre como a figura ilustra um ideal de beleza humana. O erotismo é uma questão mais artística e estética, ao passo que a pornografia está mais orientada para a satisfação instintiva das necessidades sexuais.

Classificação da pornografia em termos de psicologia:

- *soft* = tudo o que é erótico, desde um ato artístico até um indício de um ato sexual
- *hard* = representação direta de um ato sexual, incluindo detalhes dos genitais, a sua estimulação, ereção, penetração e ejaculação
- desviante = representação direta de desvios e práticas sexuais que não ocorrem numa vida sexual comum e geralmente aceite numa dada cultura (sociedade) – por exemplo, práticas com crianças, práticas sadomasoquistas, etc.

Pornografia *versus* pornografia infantil

Nem todas as representações do corpo nu constituem pornografia. Para serem consideradas pornografia, as obras em questão devem ter o propósito de induzir ou aumentar a excitação sexual (a representação de um órgão genital num livro de biologia, por exemplo, não é pornografia). Por conseguinte, a determinação de uma obra como pornográfica, baseia-se, por si própria, no sentimento moral dominante.

A pornografia infantil é aquela que retrata ou usa uma criança ou uma pessoa que parece ser uma criança. Atualmente, a pornografia infantil inclui imagens de crianças retratando posições de relações sexuais reais ou fingidas (em casos extremos, pode nem sequer ser possível ver os órgãos genitais expostos). As leis europeias e nacionais proíbem a produção, distribuição, importação, receção ou posse de qualquer imagem de pornografia infantil. A violação das leis de pornografia infantil é um crime grave, e os infratores condenados enfrentam penas legais severas.

1. Aplicar conhecimento

Exercício de ESCOLHA MÚLTIPLA

Objetivo específico associado: OE_ Saber caracterizar conteúdo impróprio.01_01: Saber nomear tipos de conteúdo impróprio.

Situação: Quais tópicos podem ser considerados conteúdo impróprio?

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

- Arte com imagens eróticas
- *Websites* com conteúdo racista ou de ódio
- Filmes de ação em geral
- Venda de produtos perigosos
- Filmes documentais sobre guerras com violência extrema



2. Como reconhecer *websites* com conteúdo impróprio?

Já existem várias instituições que supervisionam a disposição dos conteúdos *online*. É positivo ser capaz de distinguir a qualidade e credibilidade da informação e saber como lidar com material ameaçador.

Common Sense Media

A *Common Sense Media* é uma organização que classifica filmes, séries, livros, aplicações e outros conteúdos consoante a sua adequação para diferentes faixas etárias. Também permite aos utilizadores da sua plataforma que avaliem esses conteúdos, nomeando a idade para a qual são adequados.

Kids-In-Mind

A *Kids-In-Mind* é uma plataforma que providencia resumos detalhados de filmes, descrevendo o que a criança poderá ver no filme, ainda que não faça recomendações específicas sobre a adequação do conteúdo a uma determinada faixa etária.

Outras opções

A base de dados cinematográfica do IMDb também fornece informação bastante útil. Na secção de “detalhes do filme” de qualquer obra, encontra-se o “guia dos pais” (“*Parents Guide*”) e, clicando no link “ver informações sobre o conteúdo” (“*view content advisory*”), é possível aceder a informação detalhada, incluindo as recomendações de idade específicas para cada país, consoante os critérios nacionais (toda esta informação é exclusivamente em inglês).

Existem também variadas plataformas que permitem perceber se um determinado conteúdo é adequado para crianças – muitas destas usam uma escala de classificação baseada no nível de violência e teor explícito contido num meio de comunicação.

Em baixo apresentam-se algumas das questões a ter em mente para fazer uma escolha informada sobre a adequação de uma aplicação, *website* ou conteúdo:

Classificações de videoclipes musicais *online*

Estas classificações aparecem nas duas maiores plataformas de partilha de vídeo, o VEVO e o YouTube. No YouTube, é possível encontrar a etiqueta ‘*Partner Rating*’ por baixo do vídeo em questão, a qual revelará se o mesmo se destina a maiores de 12, 15 ou 18 anos (*PG12*, *PG15*, *PG18*). No VEVO é possível encontrar o símbolo da classificação no canto superior esquerdo do vídeo. Também é possível clicar no botão ‘I’ para mais informações sobre a classificação.

Classificações PEGI de jogos *online*

As Informações Pan-Europeias sobre Jogos (ou PEGI, na sigla em inglês) são usadas para aconselhar quais os videojogos adequados para adolescentes, jovens ou adultos, consoante o tipo de conteúdo apresentado. As classificações PEGI foram introduzidas em 2003 e vão desde o PEGI! (Controlo Parental Recomendado), passado pelo PEGI 3, PEGI 7, PEGI 12, PEGI 16, até ao PEGI 18, sendo que o número está relacionado com a idade para a qual o jogo é apropriado. Assim, se um jogo tiver uma classificação PEGI 7, é adequado para crianças a partir dos 7 anos. Estas classificações são legalmente vinculativas, pelo que é ilegal vender um jogo PEGI 18 a uma criança. Sublinhe-se que estas classificações não estão relacionadas com o nível de dificuldade do jogo, apenas com a adequação do conteúdo.



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



Plataformas On-demand

Em plataformas como a Netflix, BBC iPlayer e Amazon Prime, é possível encontrar as classificações etárias exibidas no próprio conteúdo presente nos respetivos catálogos. O modo de apresentação e as escalas de classificação podem variar entre plataformas mas as classificações alertam sempre para a presença de teor para adultos ou 'linguagem forte' em qualquer conteúdo.

Idade mínima de utilização de redes sociais

Os termos e condições da maioria das redes sociais recomendam que crianças com menos de 13 anos não devem fazer uso dessas plataformas. A razão por detrás desta idade mínima não está afeta ao facto de que o conteúdo na plataforma é impróprio para menores de 13 anos, mas está sim ligada ao COPPA (*Children's Online Privacy Act*), uma lei Americana aprovada para proteger a privacidade de menores de 13 anos na Internet.

Classificações etárias das aplicações

Tanto a Google Play Store como a Apple App Store utilizam classificações de aplicações para realçar o nível de conteúdo sexual, palavrões, temáticas para adultos e abuso de substâncias que podem estar presentes numa *app*.

Abreviaturas relacionadas com acessibilidade que podem ser encontradas na Internet (fonte: Classificação da Motion Picture Association):

- G: filme infantil, completamente seguro
- PG: Pais podem considerar a possibilidade de deixar os filhos ver
- PG-13: Menores de 13 só devem ver se acompanhados pelos pais
- R: Menores de 17 só devem ver se acompanhados pelos pais
- NC-17: Não adequado a menores de 18 anos

Não esquecer

Os controlos parentais, as definições de privacidade e variadas classificações são ferramentas úteis para ajudar a minimizar os riscos que as crianças podem enfrentar na Internet, mas estes não são 100% eficazes. É muito importante incutir nas crianças competências como pensamento crítico e resiliência, de modo a que estes saibam o que fazer face aos riscos. É crucial encorajá-los sempre a falarem com um adulto se encontrarem alguma coisa que os perturbe quando navegam *online*.

Quando as crianças começam a usar a Internet, deve conversar-se com elas sobre o que podem encontrar no espaço digital. É essencial ajudá-los a compreender que, por vezes, podem contactar com coisas que preferiam não ver, ou que os pais preferiam que elas não vissem. Estas conversas devem ser frequentes.

As medidas recomendadas para evitar o contacto com conteúdo inadequado são:

- Explicar os limites de idade e os sites impróprios para certas idades;
- Falar com outros pais e com a escola;



- Chegar a acordo sobre regras basilares;
- Manter a calma e uma postura tranquilizante;
- Proceder à verificação da idade em *websites* pornográficos comerciais;
- Encorajar o pensamento crítico;
- Falar sobre o que é falso e o que é real;
- Explicar os benefícios do uso consciente da tecnologia.

Não esquecer

É importante criar um ambiente de diálogo contínuo e interessar-se sempre pelo que as crianças estão a fazer *online*.

2. Aplicar conhecimento

Exercício de ESCOLHA MÚLTIPLA

Objetivo específico associado: OE_ Saber caracterizar conteúdo impróprio.01_02: Saber nomear métodos de difundir conteúdo inapropriado e obter informação sensível.

Situação: Qual é o conteúdo debatido em *websites* 'pró-ana'?

Tarefa: Escolher a opção certa usando o princípio de escolha múltipla: apenas uma frase é verdadeira.

- Materiais obscenos
- Vídeos e fotos com teor violento
- Promoção de automutilação, suicídio ou jogos violentos
- Anorexia

3. O que é conteúdo impróprio para crianças?

Sem supervisão, os jovens têm acesso a um mundo praticamente sem limites, pelo que os pais devem estar cientes dos riscos. A Internet dá liberdade a qualquer pessoa para publicar e criar quaisquer conteúdos, pelo que é possível que as crianças contactem com conteúdo que prefeririam não ter visto, ou acedam a *websites* que são inapropriados para a sua idade. O termo impróprio significa coisas diferentes para pessoas diferentes, desde palavrões até imagens ou vídeos pornográficos, e o que é inadequado para as crianças também se altera à medida que estas crescem e se desenvolvem. Há uma série de coisas na Internet que pode perturbar as crianças, e afetar o que devia ser uma experiência saudável *online*. É importante lembrar que o conteúdo impróprio inclui materiais pornográficos, mas também pode incluir conteúdo relacionado com ódio racial, distúrbios alimentares ou *sites* de jogos de azar.



Que conteúdo é impróprio para crianças?

Conteúdo impróprio inclui, na maioria dos casos, informações ou imagens que perturbem as crianças, ou informações que possam conduzir a criança a comportamentos ilegais ou perigosos. Isto pode incluir:

- Material pornográfico;
- Conteúdo que contenha palavrões;
- *Websites* que encorajem o vandalismo, crime, terrorismo, racismo, distúrbios alimentares ou até o suicídio;
- Imagens, vídeos ou jogos que exibam imagens de violência ou crueldade para com outras pessoas ou animais;
- *Sites* de jogos de azar;
- *Chatrooms* não moderados – espaços onde não há ninguém a supervisionar a conversa e a banir comentários impróprios;
- Conteúdo sexista ou *sites* que retratem as mulheres em papéis muito tradicionais que não refletem valores e expectativas contemporâneas.

Geralmente quase todas as pessoas são afetadas pelo conteúdo impróprio, e é possível estipular diferentes categorias para definir as questões específicas da proteção:

- Pré-escolar (0-5 anos)
- Idade escolar mais jovem (6-11 anos)
- Idade escolar mais velha (12-15 anos)
- Juventude (15-18 anos)
- Adultos

Pré-escolar

Cada vez mais crianças em idade pré-escolar têm acesso aos computadores, *smartphones* e *tablets* dos pais para jogar jogos, usar diversas aplicações e ver os seus programas de televisão preferidos. Há algumas medidas simples que se podem implementar para garantir que este uso da Internet é seguro. É necessário construir uma relação saudável com o conteúdo adequado, através da exploração do mesmo com a criança, da instalação de proteções de controlo parental, do uso de senhas que restrinjam a sua admissão e do estabelecimento de limites/regras para a vivência *online*.



Idade escolar mais jovem

A utilização precoce da tecnologia digital tem demonstrado algumas vantagens, como a melhoria dos conhecimentos linguísticos e a promoção do desenvolvimento social e da criatividade das crianças. Contudo, os contactos com a tecnologia não estão imunes de riscos para as crianças pequenas, que podem ter contacto com conteúdo impróprio ou começar a copiar o que as crianças mais velhas fazem *online*. Neste caso podem aplicar-se as mesmas medidas de proteção recomendadas para as crianças em idade pré-escolar, e complementá-las com as seguintes sugestões: usar o “modo avião” (que impede a comunicação com outras pessoas através do dispositivo em questão); falar com crianças mais velhas sobre os seus comportamentos *online* e aquilo que mostram a crianças mais novas; e monitorizar as classificações etárias para perceber o que se adequa a esta idade.

Idade escolar mais velha

As crianças nesta faixa etária são o grupo que corre mais riscos, devido a variados fatores, tais como o enorme aumento da utilização da tecnologia moderna, sem instrução ou supervisão relevantes, a ingenuidade que pode dar aso a abusos, a tendência para o desafio à autoridade e a procura por uma identidade própria que, se não for satisfatória no mundo real, pode ser procurada no mundo virtual. É normal, para determinados grupos etários que a sua vida virtual esteja sujeita a um controlo parental mínimo, superficial ou nulo, sendo que estes jovens têm, frequentemente, maior literacia informática do que os seus próprios pais, que muitas vezes percecionam a tecnologia moderna como sendo hostil e permitem que as crianças a usem livremente para os próprios poderes relaxar. Portanto, uma grande porção destes jovens utilizadores desenvolveu a sensação de que podem fazer qualquer coisa no mundo virtual, sem grande sentido de responsabilidade e respeito pelos outros.

Juventude

Os estudantes do ensino secundário destacam-se pelo seu intenso uso das tecnologias modernas, especialmente a Internet e as redes sociais, as quais originam perigos. É importante que estes jovens estipulem definições de privacidade na maioria das redes sociais, de maneira a que apenas os amigos próximos possam procurá-los, identificá-los em fotografias ou partilharem as suas publicações. Deves dizer aos jovens desta idade que tudo o que divulgarem na internet, todos os *emails* e todas as mensagens enviadas poderão ficar *online* para sempre. É crucial enfatizar que, na Internet, só devem fazer coisas que não se importem que os pais, professores e futuros empregadores vejam, bem como lembrar que é fulcral não ceder à pressão dos colegas para enviar comentários ou imagens inapropriados. Recomenda-se que se incite junto dos jovens a criação de uma pegada digital positiva. Para este grupo-alvo, o mais importante é a confiança: tens de estar interessado nas suas necessidades, falar com eles e ser mais amigo do que pai/mãe.

Adultos

O conteúdo direcionado para adultos também pode ser afetado por conteúdo impróprio *online*. Muitos *websites* contêm vírus. Estes são mais frequentemente colocados em páginas com materiais impróprios. Na maioria dos casos, trata-se de um *download* por engano de vírus informáticos espalhado por *sites* de conteúdo pornográfico. Esses *websites* são muito apelativos para os cibercriminosos porque têm um grande número de utilizadores. Além disso, as vítimas destes ataques ficam frequentemente relutantes em denunciar um ataque cibernético ou uma contaminação no seu dispositivo, se estes forem originários de uma visita a um *website* pornográfico. Os vírus digitais que são descarregados de *websites* com conteúdo impróprio mais comumente incluem *trojans*, *clickjacking*, *tinder bots*, *cat-phishing*, *ransomware*, *worms*, *pornware*, ou *spyware*.



3. Aplicar conhecimento

Exercício de ESCOLHA MÚLTIPLA

Objetivo específico associado: OE_ Reconhecer as ameaças de abuso de informação sensível e o seu impacto.02_02: Conseguir caracterizar os grupos-alvo que podem ser vítimas de contacto com conteúdo impróprio.

Situação: Qual é o grupo-alvo grupo mais vulnerável a conteúdos impróprios?

Tarefa: Escolher a opção certa usando o princípio de escolha múltipla: apenas uma frase é verdadeira.

- Idosos
- Crianças entre os 12 e os 18 anos
- Todas as crianças com menos de 15 anos
- Todas as crianças com mais de 15 anos

4. Como posso proteger-me e aos meus filhos de conteúdos impróprios?

Ferramentas como o controlo parental podem ajudar a proteger as crianças dos conteúdos impróprios, mas não é possível verificar tudo o que eles vêm na Internet. É preciso ajudá-los a evitar conteúdos impróprios, e a lidar com eles se o contacto for inevitável. O primeiro passo é falar com eles sobre isso.

A maioria destes *websites* perturbadores não são 'ilegais', o que significa que se manterão *online* e cabe aos pais controlar e gerir o seu acesso. Ninguém se sentiria seguro a permitir que uma criança vagueasse sem rumo no meio de uma grande cidade, sozinha, no meio da noite, por isso devemos lembrar-nos que a Internet é como uma grande cidade, cheia de coisas boas e más, um lugar onde uma criança requer supervisão.

O que posso fazer quando reconheço *websites* com conteúdo impróprio?

- Informar o respetivo administrador, diretamente na aplicação (*web browser*, redes sociais, etc.)
- Informar a polícia ou outras instituições de relevo
- Usar ferramentas de software para bloquear o conteúdo inapropriado (controlo parental)
- Falar com as crianças sobre esse tema

É possível informar o gestor de aplicação quando se identifica conteúdo apropriado em aplicações comuns (*Google*, *Facebook*, etc.). Normalmente, é possível encontrar o botão em questão nas definições da aplicação.



Outra opção é informar a polícia sobre o conteúdo impróprio através da especificação detalhada da fonte.

Os controlos parentais são opções presentes em *softwares* ou dispositivos que permitem aos pais controlar a utilização da Internet dos seus filhos. Estas opções impedem as crianças de acederem a conteúdos impróprios ou inapropriados *online*. Podem ser implementados junto dos fornecedores dos serviços de Internet, nos motores de busca, nos *sites* de transmissão de vídeo e muito mais. As ferramentas de controlo parental mais comuns na Internet são:

- A configuração de controlos parentais comuns a toda a rede, no *router*
- O uso de aplicações de monitorização da quantidade de tempo passado pelas crianças na Internet
- A restrição do acesso à Internet no WiFi
- A instalação de filtros de controlo parental nos *browsers*

Para evitar o acesso a *sites* problemáticos não só das crianças mas também de funcionários – por forma a restringir distrações no trabalho –, em particular aqueles que contêm pornografia, tópicos extremistas, entre outros, é possível recorrer a variados métodos de proteção.

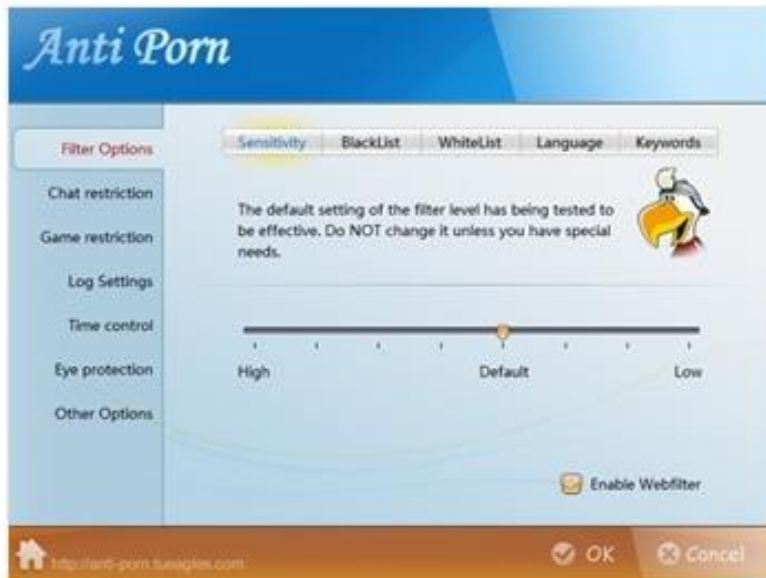
Quais programas, filtros ou suplementos (*add-on*) são os melhores para restringir o acesso a *sites* impróprios?

Anti-Porn

Um dos programas mais conhecidos e amplamente usados para proibir visitas a *websites* pornográficos. A sua popularidade deve-se principalmente à sua fácil maneabilidade e facilidade de ajuste. A aplicação reconhece e marca automaticamente o conteúdo como erótico e proíbe de imediato o acesso a esse espaço. Também tem uma base de dados de vários milhares de *websites* maliciosos, que é regularmente atualizada.



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



K9 Web Protection

Outro programa de filtragem desenvolvido para proteger contra as armadilhas da Internet. Funciona tanto como um protetor de *malware* e um filtro de conteúdo impróprio. É gratuito e pode ser usado tanto em *Windows* como *MAC OS X*. Adicionalmente, é fácil de configurar e operar. Os *sites* maliciosos são categorizados por tipo de conteúdo, como pornografia, redes sociais, conteúdos violentos, etc.



Kurupira Web Filter

Não é um programa particularmente conhecido ou difundido, mas é perfeitamente capaz de cumprir a sua função, contando com um ambiente agradável, orientado para principiantes. Uma das grandes vantagens é que a sua licença é gratuita. Para aceder ao programa, é necessário definir uma palavra-passe.



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



iWebFilter

Esta aplicação contém uma vasta base de dados de páginas, palavras e conteúdos problemáticos, sendo que o utilizador pode estendê-la. Pode definir-se um bloqueio a ser aplicado em *browsers*, plataformas de mensagens instantâneas (*IM*) e de correio eletrónico, e outras aplicações. Há também um horário de acesso à Internet, limite de transferência de dados e registo detalhado de eventos.



Na eventualidade de a criança encontrar conteúdo censurável, o adulto não deve permitir que se continue a ver, deve sim desligar ou abandonar o ecrã. O adulto não deve repreender a criança por navegar em locais inapropriados na Internet. Quando uma criança procura propositadamente material impróprio como pornografia, violência, etc., é necessário pensar na causa que o leva a fazer tal. É necessário considerar a idade e o contexto, ou procurar apoio profissional, por exemplo, junto de profissionais de aconselhamento pedagógico-psicológico relevante.

A Insafe e a INHOPE trabalham em conjunto através da rede de Centros de Internet Mais Segura (Safer Internet Centres – SICs) dispersos pela Europa – compreendendo normalmente centros de sensibilização, linhas de apoio, linhas diretas, entre outros, dedicados à remoção de conteúdo ilegal



online. Os Centros de Internet Mais Segura operam em 30 países da Europa, com a missão de manter crianças e jovens seguros na Internet. Através de uma variada gama de serviços, os SICs respondem às mais recentes problemáticas relacionadas com a Internet, ajudando a promover as muitas oportunidades que o mundo *online* oferece, a par de abordarem os desafios que daí também surgem.

Se tu ou o teu filho se depararem com algum conteúdo inapropriado que incite à violência ou ao ódio, eis o que podem fazer:

- Na eventualidade do conteúdo ser ou expor alguma ilegalidade (que viole as leis), deves contactar a polícia
- Contactar as organizações/instituições dedicadas ao tópico da segurança na Internet (por exemplo, as SICs: <https://www.betterinternetforkids.eu/web/portal/policy/unsafe-inhope>) para que te ajudem com a remoção/bloqueio do conteúdo
- Reportar o conteúdo ao administrador da página/plataforma
- Alterar as configurações do computador
- Contactar peritos para ajudarem a criança com a situação traumática
- Falar com o teu filho
- Manter a calma

Em baixo encontram-se alguns guias rápidos em vídeo de como proceder para definir as definições mais indicadas nas plataformas mais populares, entre outras medidas que podes tomar:

Verificador de Privacidade do Facebook

https://www.youtube.com/watch?v=wN3iz2Mv_ME&feature=emb_title

Modo restrito do YouTube

https://www.youtube.com/watch?v=XuXnatkASTQ&feature=emb_title

Google SafeSearch

https://www.youtube.com/watch?v=LK-MlwjQz20&feature=emb_title

Segurança e spyware

Alguns computadores, especialmente em locais públicos (bibliotecas, cafés, escolas, etc.) podem conter *software* de monitorização que consegue captar o ecrã e, assim, constituir uma ameaça à informação sensível no ecrã. Estas ferramentas de vigilância do PC conseguem monitorizar todo o tipo de atividade no computador. *Software* antivírus e *firewalls* não protegem totalmente o sistema contra a maioria dos *spywares* e ameaças à privacidade. O *spyware* é normalmente integrado em *downloads* de *software*, anexado a *emails*, ou transmitido através de redes, pelo que parece ser legítimo, mas uma vez instalado pode ser quase impossível detetá-lo e removê-lo sem a ajuda de uma ferramenta dedicada à eliminação de *spyware*. A proteção e prevenção de *spyware* são essenciais para garantir a privacidade contra olhares curiosos e invasores virtuais. Essas medidas também podem ser instaladas nos computadores privados para proteger pais e filhos de conteúdos inadequados, monitorizando toda a atividade *online*. Exemplos de ferramentas semelhantes podem ser encontrados no texto em cima.

Em baixo, encontram-se algumas dicas para identificar *websites* e aplicações duvidosas:

- Verificar se o URL de um *website* é o URL principal que normalmente usas para aceder a essa página.
- Desconfiar de quaisquer *emails* de pessoas que não conheças. Em caso de dúvida, não clicar em ligações ou abrir anexos em *emails*.



- Verificar se as imagens da marca (por exemplo, o logotipo) são fiáveis – se são iguais em todas as plataformas da marca – e se não estão desfocadas.
- Há erros ortográficos flagrantes no *website* ou em *emails* que pedem que inicies sessão e atualizes os teus dados? Se sim, então é provável que se trate de um esquema.
- Verificar a *app store* (onde se encontram as aplicações) antes de fazer *download* de alguma aplicação. Se uma *app* tiver boas críticas e muitos utilizadores, é pouco provável que seja um esquema. Se não tiver críticas, é boa ideia fazer mais alguma pesquisa *online* – os golpes são normalmente identificados com bastante rapidez e as pessoas muitas vezes publicam *online* sobre eles.
- Uma aplicação está a solicitar muitas informações pessoais ou dados de *login* para quaisquer contas de redes sociais? Então, é provável que se trate de um golpe.

Informação pessoal

Uma outra questão que devemos ter em atenção relativamente a conteúdos inapropriados tem a ver com a publicação de informação pessoal. Toda a gente pode ver e descarregar tudo o que publicamos *online* e utilizá-lo noutro contexto ou indevidamente essa informação.

Choo (2008) delineou três categorias de grupos organizados no ciberespaço:

1. Grupos de crime organizado tradicionais que fazem uso da tecnologia de informação para potencializar as suas atividades criminosas terrestres;
2. Grupos cibercriminosos organizados que operam exclusivamente *online*;
3. Grupos organizados de indivíduos com motivações ideológicas e políticas que fazem uso da tecnologia de informação para facilitar a sua conduta criminosa.

Estes tipos de crime organizado procuram explorar o ciberespaço de várias maneiras diferentes, cometendo uma grande variedade de crimes que podem ser conduzidos ou reforçados por computadores ou dispositivos digitais.

O tipo de informação mais importante para manter a privacidade é a informação pessoal identificável (em inglês, *personally identifiable information* - PII).

Definição
De acordo com a Administração dos Serviços Gerais dos EUA, PII é “informação que pode ser usada para distinguir ou rastrear a identidade de um indivíduo, quer isoladamente ou quando combinada com outra informação pessoal ou informação identificativa que esteja ligada ou possa ser associada a um indivíduo específico”.

Alguns exemplos de informação pessoal identificável são:

- Nomes: O teu nome completo, o teu apelido, o nome de solteira da tua mãe
- Números de identificação pessoal: O teu número da segurança social, o número da carta de condução, o número do passaporte, o número de utente, o número de contribuinte, o número da conta bancária, ou o número da conta financeira
- Endereços: A morada e o endereço de *email*
- Biometria: Digitalização da retina, impressões digitais, geometria facial, ou assinaturas de voz
- Identificação da matrícula ou do veículo
- Números de telefone
- Informação sobre bens tecnológicos: Endereços MAC (*Media Access Control*) e IP (*Internet Protocol*).



Porque é que esta informação pessoal deve manter-se privada? Proteger informações pessoais pode ser útil na prevenção de roubos de identidade, na proteção das informações financeiras, para se evitar ser roubado, para proteger a empregabilidade e reputação dentro de uma empresa, e muito mais...

Seguem-se algumas dicas para manter a segurança das contas e garantir controlo da privacidade *online*. Também podes ler mais sobre como proteger a tua identidade.

- Fazer uma verificação de privacidade, passando pelas definições de todas as contas de redes sociais;
- Definir palavras-passe fortes e atualizar senhas antigas
- Não partilhar *passwords*
- Garantir que descarregas e instalas novos sistemas operativos e *software* no telemóvel, tablet ou computador logo que estejam disponíveis
- Não adicionar nas redes sociais pessoas que não conheces *offline*
- Quando os *websites* ou *apps* pedem informações pessoais, verificar se são legítimos

A Comissão Europeia adotou uma recomendação sobre medidas para combater eficazmente os conteúdos ilegais *online*. Questões como o incitamento ao terrorismo, discurso de ódio ilegal, ou conteúdo relacionado com abuso sexual de crianças, bem como a violação de direitos de Propriedade Intelectual e proteção dos consumidores *online*, necessitam de uma abordagem forte e coordenada a nível da UE. A abordagem é completamente alinhada e consistente com a Diretiva de Direitos de Autor, incluindo aspetos amplamente debatidos sobre a responsabilidade das plataformas *online*. É também completamente coerente com a revisão da Diretiva dos Meios de Comunicação Audiovisuais.

As plataformas *online* precisam de ser mais responsáveis pela gestão do conteúdo. A recomendação propõe uma abordagem comum para detetar rápida e proativamente, remover e prevenir o reaparecimento de conteúdos *online*:

- Procedimentos mais claros de 'aviso e ação';
- Ferramentas mais eficazes e tecnologias mais proativas;
- Salvaguardas mais rígidas para garantir os direitos fundamentais;
- Especial atenção às pequenas empresas;
- Cooperação próxima com as autoridades.

4. Aplicar conhecimento

Exercício de ESCOLHA MÚLTIPLA

Objetivo específico associado: OA_ Proteção contra conteúdos impróprios_03: Saber proteger-se contra conteúdo impróprio. OE_05: Ser capaz de indicar as razões pelas quais algumas informações pessoais não devem ser publicadas *online*.

Situação: Quais são as maneiras básicas para evitar propagar conteúdo impróprio?

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

- Não enviar fotografias a ninguém desconhecido.
- Manter as palavras-passe secretas e não as dizer nem a um amigo próximo.
- Não abrir o anexo de uma mensagem vinda de um endereço desconhecido.
- Não usar nenhuma rede social.



Fontes

Internet matters.org: <https://www.internetmatters.org/issues/inappropriate-content/learn-about-it/#age-ratings>

CNET.com: https://download.cnet.com/Anti-Porn/3000-27064_4-10207334.html

K9 Web Protection: <https://www.downloadsource.net/1771222/k9-web-protection/>

Soft free download (Soft 32): <https://kurupira-web-filter-and-parental-control.soft32.com/>

Softpedia: <https://www.softpedia.com/get/Internet/Other-Internet-Related/iWebFilter.shtml>

Para relembrar

Resumo

Existem variadas formas de conteúdo impróprio. As mais comuns incluem:

- Pornografia
- Comportamentos violentos/extremistas
- Produtos perigosos
- Racismo ou ódio
- *Websites* pró-Ana
- *Websites* com conteúdo extremista

Frequentemente, o conteúdo é indesejável e prejudicial, mas pode não ser ilegal. Isso depende de como é publicado na Internet, respetivamente, de como se evita a sua acessibilidade. No entanto, tanto o conteúdo ilegal como o conteúdo legal nocivo podem ter um impacto indesejável sobre aqueles que encontram esse tipo de conteúdo.

Em geral, é aconselhável contactar a polícia quando se trata de atos ilegais. Contudo, por vezes é essencial, acima de tudo, impedir rapidamente a distribuição de tais conteúdos, e é possível fazê-lo sem recorrer às instituições policiais. Não obstante, se te deparares com pornografia ilegal ou *websites* extremistas, não hesites em reportar à polícia.

Em primeiro lugar, as crianças (dependendo da idade) não devem encontrar conteúdo perigoso de todo. Os **filtros no browser da Internet**, por exemplo, podem ser úteis para restringir esse acesso (por exemplo, é possível desativar a exibição de uma página contendo o termo “pornografia”, etc.).

Os **controles parentais** são opções de *software* ou configurações em dispositivos que permitem que os pais monitorizem o uso da Internet dos seus filhos. Estes impedem as crianças de acederem a conteúdos impróprios ou inapropriados *online*. Podem ser implementados junto do fornecedor de serviços de Internet, nos motores de busca, nos sites de transmissão de vídeo, e muito mais. As ferramentas de controlo parental mais usadas na Internet são:

- A configuração dos controlos parentais na rede do router;
- O recurso a aplicações que monitorizam o tempo de Internet da criança;
- A restrição do acesso à Internet no Wi-Fi;
- A imposição de controlos parentais nos navegadores *web*.

O instrumento de proteção contra o conteúdo impróprio mais importante é a **discussão e cuidado com as nossas crianças**, de forma a sabermos o que estas fazem na Internet e mostrarmos interesse nas



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

suas necessidades e hobbies. Podemos usufruir das ferramentas de proteção que existem, como as leis, os controlos parentais, as configurações de *software* e as instituições de apoio, mas a chave é a confiança entre ti e a criança.



As respostas corretas estão assinaladas a negrito

Situação: Quais tópicos podem ser considerados conteúdo impróprio?

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

- Arte com imagens eróticas
- **Websites com conteúdo racista ou de ódio**
- Filmes de ação em geral
- **Venda de produtos perigosos**
- Filmes documentais sobre guerras com violência extrema

Situação: Qual é o conteúdo debatido em *websites* 'pró-ana'?

Tarefa: Escolher a opção certa usando o princípio de escolha múltipla: apenas uma frase é verdadeira.

- Materiais obscenos
- Vídeos e fotos com teor violento
- Promoção de automutilação, suicídio ou jogos violentos
- **Anorexia**

Situação: Qual é o grupo-alvo grupo mais vulnerável a conteúdos impróprios?

Tarefa: Escolher a opção certa usando o princípio de escolha múltipla: apenas uma frase é verdadeira.

- Idosos
- **Crianças entre os 12 e os 18 anos**
- Todas as crianças com menos de 15 anos
- Todas as crianças com mais de 15 anos

Situação: Quais são as maneiras básicas para evitar propagar conteúdo impróprio?

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

- **Não enviar fotografias a ninguém desconhecido.**
- **Manter as palavras-passe secretas e não as dizer nem a um amigo próximo.**
- **Não abrir o anexo de uma mensagem vinda de um endereço desconhecido.**
- Não usar nenhuma rede social.