Instituto de Apoio à Criança

infoCEDI

Boletim do Centro de Estudos, Documentação e Informação sobre a Criança do Instituto de Apoio à Criança

CEDI CENTRO DE ESTUDOS, DOCUMENTAÇÃO E INFORMAÇÃO SOBRE A CRIANÇA

InfoCEDI setembro-outubro 2017 N.º 72

Ficha Técnica

Direcção de Publicação:
Ana Tarouca
Pedro Pires

Revisão de texto:
José Brito Soares

Edição:
Instituto de Apoio à Criança
Largo da Memória, 14
1349-045 Lisboa

Periodicidade: Bimestral

ISSN: 1647-4163

Distribuição gratuita

Endereço Internet:
www.iacrianca.pt
Blogue:
Crianças a torto e a Direitos

Serviço de Documentação:
Tel.: (00351) 213 617 884
Fax: (00351) 213 617 889
E-mail:iac-cedi@iacrianca.pt

Atendimento ao público, mediante marcação:
-De 2ª a 5ª feira, entre as 9.30h e as 16.00h
-6ª feira entre as 9.30h e as 12.00 horas

Para subscrever este boletim digital envie-nos uma mensagem para
iac-cedi@iacrianca.pt

International Telecommunication Union

Definições sobre Segurança Infantil na Internet

Violência online

É qualquer tipo de comportamento de agressão, ameaça ou intimidação efetuado pela internet e/ou pelas novas tecnologias, através de sms, mms, email, chatroom, messenger, website, youtube, redes sociais, com a intenção de nos magoar, envergonhar, assustar ou ofender.

Uma das formas mais comuns de violência online é o **cyberbullying**.

Cyberbullying

É uma forma de **bullying** cometido através da internet e das novas tecnologias, em que alguém (normalmente uma pessoa/grupo que conheces da vida "real") procura ofender, envergonhar e humilhar outra pessoa.

Qualquer jovem pode ser vítima de **cyberbullying** através de, por exemplo:

- emails ou mensagens recebidas (no telemóvel, no facebook, em chats) com ofensas, insultos ou ameaças;
- emails ou mensagens recebidas (no telemóvel, no facebook, em chats) contendo vídeos e/ou fotos que causam desconforto ou embaraço;
- emails recebidos contendo vírus;
- uso das passwords para entrar no email e/ou na conta do facebook para enviar emails insultuosos ou para publicar informação ofensiva ou falsa (sobre nós ou sobre pessoas que conhecemos); emails, mensagens ou comentários partilhados com outras pessoas (pelo telemóvel, no facebook, em chats), que contenham informação falsa ou humilhante sobre nós, tais como comentários, fotos, imagens ou vídeos, para envergonhar e prejudicar.

Embora um caso de cyberbullying possa ser ultrapassável, alguns casos podem ganhar tais dimensões, que deixam a vítima em estado de desespero. Nestas circunstâncias e, dependendo da sua inteligência emocional, uma vítima pode adotar comportamentos de risco, encarando o suicídio, como uma opção de fuga. Por esta razão, nunca devemos encarar este problema de ânimo leve.

O que pode correr mal?

Este fenómeno tem-se tornado cada vez mais comum, assumindo proporções variadas. O que geralmente ocorre é um utilizador anónimo (recorrendo a perfis falsos, contas sem informação ou até roubo da identidade de outros utilizadores), através das redes sociais, emails, SMS, serviços de IM, fóruns ou quaisquer outros mecanismos de comunicação, transtornar outro utilizador.
O agressor pode fazê-lo de diferentes formas – através de ameaças, – denegrir a sua imagem, causando sempre períodos de sofrimento e/ou stress. E enquanto que no bullying "tradicional" o bully é geralmente o elemento com maior poder (tamanho, idade, força) dentro de um grupo local, na Internet, o agressor pode ter os mais variados perfis.

Existem algumas redes sociais/aplicações que foram sinalizadas como propícias ao Cyberbullying nomeadamente aplicações que permitem o anonimato como é o caso do Ask.FM e Snapchat.
Seguem-se alguns exemplos de cyberbullying:

Ameaça e Perseguição
Através do computador e smartphones, os agressores enviam sistematicamente mensagens ameaçadoras ou de ódio aos seus alvos. Os bullies podem inclusivamente adotar nomes ou nicks de outros utilizadores, para envolver outras vítimas no processo.

Humilhação pública

Grande parte das vezes, este fenómeno baseia-se na humilhação pública, recorrendo às redes sociais ou ao envio de mensagens de correio eletrónico em massa para outros utilizadores, contendo imagens ou outros conteúdos que coloquem em causa a reputação da vítima.

Envio de malware

Caso o agressor possua conhecimentos suficientes, poderá efetuar o envio de vírus e malware como forma de prejudicar a vítima. Note-se que estes vírus poderão ser veículos para alcançar outros objetivos como o roubo de informações pessoais.

Roubo de Identidade

Ao obter acesso às palavras-passe da vítima, o agressor entra nas várias contas da vítima, acedendo ilicitamente a várias informações sobre a vítima em questão e causando vários problemas, como o envio de mensagens de conteúdo inapropriado para os contactos da vítima. Através do acesso a estas informações é possível ao agressor criar perfis em vários websites, muitas vezes com o objetivo de manchar a reputação online da vítima.

Cyberstalking

É outra forma de violência online.

Stalking significa um **conjunto de comportamentos de assédio persistente e de contactos indesejados** efetuados por uma pessoa contra outra, com o objetivo de conhecer, seduzir, começar (ou reatar) uma relação mais íntima com essa pessoa (por exemplo, namoro). Esses contactos e aproximações são feitos de uma forma que causa desconforto, assusta e intimida a outra pessoa.

O **Cyberstalking** é uma forma de stalking que envolve o **uso da Internet e das novas tecnologias para comunicar e tentar o contacto ou a (re)aproximação a alguém**.
A pessoa que realiza este tipo de comportamentos pode ser:

- desconhecida;
- conhecida (ex.: ex-namorados/as; amigos; colegas).

O stalking pode começar por contatos que parecem inofensivos e românticos como, por exemplo:

- ligar constantemente para dizer 'olá' ou para perguntar 'como estás?';
- enviar várias mensagens escritas ou e-mails com juras de amor.

Estes contactos podem evoluir para **situações cada vez mais incómodas e reais**, por exemplo:

- aparecer nos sítios que a pessoa frequenta, por exemplo, no café;
- vigiar os passos da pessoa, acompanhado as atividades e percursos que esta vai fazendo;

Os contactos e aproximações podem mesmo chegar a envolver **violência física ou verbal e ameaças**.

Seguranet

Discursos de ódio

Os **discursos de ódio através da internet** também podem ser uma forma de violência e representam uma violação dos direitos humanos.

São manifestações que procuram afirmar, encorajar ou incitar o ódio contra uma pessoa ou grupo de pessoas em razão da sua cor da pele, etnia, nacionalidade, ascendência, língua, religião, sexo, orientação sexual, identidade de género, condição física, ou outros fatores discriminatórios ou xenófobos.

Estes discursos têm como objetivos injuriar, ameaçar, intimidar e desumanizar uma pessoa ou grupo, diferenciando-o/a da restante população e, ao mesmo tempo, disseminar estas mensagens junto de outras pessoas, promovendo a sua aceitação e a violência.

Podem ser manifestados através de qualquer meio de comunicação e estão cada vez mais presentes nas redes sociais e na internet, atingindo, por este meio, uma difusão muito alargada junto de um elevado número de pessoas.

Os discursos de ódio através da internet podem consistir em:

- e-mails enviados a uma pessoa ou grupo com manifestações de ódio racial ou de ódio motivado por outros fatores discriminatórios;
- comentários e mensagens publicadas em redes sociais que manifestem ódio contra uma pessoa ou grupo em razão da sua cor, orientação sexual, nacionalidade ou religião;
- fotografias ou vídeos que incitem o ódio ou a discriminação;
- *memes* que possuam mensagens e imagens com conteúdo hostil ou malicioso relacionado com a orientação sexual, identidade de género ou outros fatores discriminatórios;
- jogos que contenham atos de violência ou outras manifestações de ódio relacionadas com a discriminação ou a xenofobia.

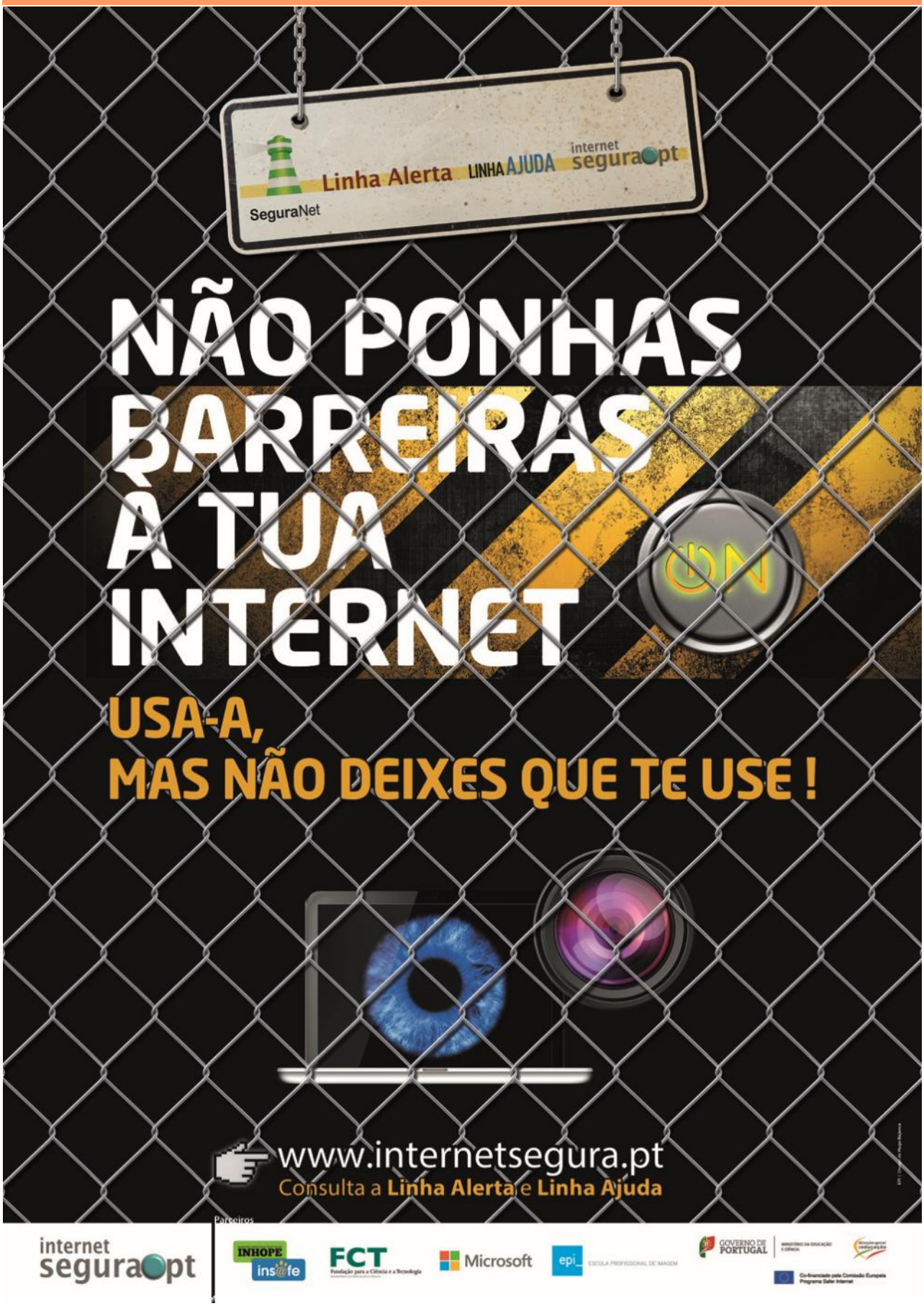
Podem surgir muitas **inseguranças e receios quando estas formas de violência acontecem**, por exemplo:

- a pessoa alvo de violência pode não perceber que o que lhe está a acontecer é uma forma de violência;
- a pessoa pode não saber que atitude tomar quando está a ser vítima de violência online;
- a vítima pode até conhecer da vida "real" a pessoa que a está a agredir ou humilhar, mas não sabe que é ela que o está a fazer naquele momento;
- o/a agressor/a pode fazer-se passar por outra pessoa para que a sua verdadeira identidade não seja revelada;
- muitas agressões são anónimas, ou seja, não vêm "assinadas" por ninguém;
- a vítima receia que as agressões ou humilhações que alguém está a cometer sejam partilhadas ou enviadas a outras pessoas, principalmente às pessoas que conhece.

Em Portugal, esta questão é abordada em profundidade pelo Movimento contra o Discurso de Ódio (http://www.odionao.com.pt/).

Site da APAV para Jovens e Site da Internet Segura

O Instituto de Apoio à Criança é parceiro da Internet Segura.pt.



Seguranet

CONSELHOS SOBRE NAVEGAR COM SEGURANÇA NA INTERNET

O QUE NUNCA DEVES FAZER:

- Fornecer dados pessoais (teus, de membros da tua família ou de amigos) a pessoas que conheces na internet - nome completo, número do documento de identificação (bilhete de identidade, cartão de cidadão), número de telefone/telemóvel, morada, número/informações das tuas contas bancárias ou das dos teus pais.
- Preencher informação com dados pessoais, sem verificar anteriormente o endereço do website que os solicitou, o motivo do pedido e a credibilidade da entidade que o regula.
- Expor demasiada informação sobre ti em blogues ou redes sociais.
- Abrir ou responder a emails de destinatários que não conheces.
- Abrir links ou consultar páginas que te pareçam duvidosas ou com conteúdos estranhos.
- Partilhar a tua password com alguém (mesmo com alguém em quem confies totalmente).
- Fazer compras online, sem o consentimento e ajuda dos teus pais.
- Combinar encontros com pessoas que conheceste online.
- Responder a mensagens ou contactos desagradáveis, humilhantes ou provocadores (mesmo que sejam de uma pessoa que até conheces)
- Usar a internet para magoar, prejudicar ou humilhar alguém.

Quanto mais informação colocares sobre ti online, maior é o risco da alguém a usar para te prejudicar.

O QUE DEVES SEMPRE FAZER:

- Fornecer o teu email apenas a pessoas que conheces e a entidades que sejam legítimas.
- Atualizar regularmente o antivírus do teu computador.
- Proteger o teu email com um filtro de spam/lixo eletrónico, para evitares receberes emails ou publicidade indesejada ou de destinatários que não te interessam.
- Alterar regularmente as tuas passwords.
- Efetuar sempre logout quando queres sair do teu email ou de uma página da web em que tenhas efetuado login.
- Falar com um adulto em quem confies quando tiver acontecido alguma coisa que te tenha incomodado ou quando tens alguma dúvida.
- Contactar o administrador da página da web em que estás se perceberes que o conteúdo do website é inadequado ou impróprio.
- Não responder a qualquer mensagem provocatória ou desagradável e guardar essa informação para a enviar ao administrador do website ou fórum.

Site da APAV para Jovens

OUTROS RISCOS NA INTERNET

Sexting

O termo sexting resulta das palavras 'sex ' (sexo) e 'texting' (envio de SMS) e significa a troca de mensagens eróticas com ou sem fotos via telemóvel, chats ou redes sociais. O maior perigo de sexting é que essas fotos ou mensagens acabem espalhadas pela Net ou nas mãos de pessoas erradas! O fenómeno do sexting é especialmente comum entre adolescentes e jovens adultos. Na grande maioria das vezes as imagens ou mensagens íntimas são enviadas no contexto de uma relação de namoro, mas as motivações são diversas:

- Fornecer uma "prova de amor "pelo envio de fotos eróticas;
- Desejo de afirmar audácia e autoconfiança exibindo o corpo de forma sedutora;
- Solicitação do parceiro(a) para fazê-lo sob chantagem emocional;
- Ser convencido por alguém a fazê-lo durante uma conversa online;
- Envio por vingança de fotos ou mensagens de terceiros;
- Envio por erro (em especial a partir de um telemóvel).

O que pode correr mal?

Duas pessoas envolvidas num relacionamento sério que trocam fotos ou mensagens eróticas não é uma novidade. O que mudou na era digital é a velocidade com que estas imagens podem ser enviadas e também copiadas e partilhadas em várias plataformas online e, por conseguinte, a probabilidade de se tornarem acessíveis a milhares de pessoas. Uma imagem que saiu das nossas mãos para a web por via de um telemóvel ou de um computador, fica fora do nosso controlo. Quando as relações acabam em conflito, muitas vezes as mensagens e fotografias que eram do foro privado acabam publicadas.

Depois disso o resultado dessa gravação pode ser utilizado para fazer chantagem, para prejudicar a reputação da pessoa visada e/ou para fazer cyberbullying (com efeitos traumáticos para os envolvidos).

O que fazer para estar mais seguro?

- Deves pedir imediatamente à pessoa a quem enviaste a foto ou mensagem que a apague. Alguém que gosta de nós ou que nos respeita irá acatar a decisão. Se não for o caso, a pessoa pode e deve ser punida por lei (ao abrigo do art.º192 do código penal que pune a devassa da vida privada).
- Não se deve esperar muito tempo a reagir, quanto mais rápido mais depressa se recupera o controlo da situação. Deve pedir-se ajuda a alguém em quem se confia, um amigo, um familiar ou ao Centro Internet Segura para se receber orientações sobre como agir.
- Graças aos direitos de imagem, a foto não pode ser difundida sem a autorização do próprio (ou sem a autorização dos pais se fores menor). É ilegal. Se tomares conhecimento de que alguém abusivamente publicou fotos tuas sem o teu conhecimento, podes e deves agir legalmente, com a ajuda dos teus pais.
- Utilize vários motores de busca para encontrar as tuas fotos na Internet. Digita o teu nome e/ou o nome que usas para os teus perfis em redes sociais. Também podes programar os Alertas do Google para fazer este trabalho (uma foto que ainda não está online pode vir a estar).
- Deves remover as tuas fotos dos lugares onde aparecem. Regra geral as redes sociais possuem botões para denunciar fotos que não cumprem as regras de utilização do serviço. Num website deves contactar os responsáveis pela gestão do mesmo ou os prestadores do serviço de alojamento onde a foto está publicada. Se não resultar de imediato deves avisar a polícia.

Pornografia Vingativa (Revenge Porn)

Este termo é utilizado para descrever a distribuição de imagens sexualmente explícitas sem o consentimento do(s) individuo(s) representado(s) nas imagens. Esta situação é classificada como uma forma de assédio grave e um tipo de violência doméstica.

Este problema assume uma carga social e emocional muito grande para as vítimas e pode causar situações constrangedoras e até ameaçadoras, caso a informação pessoal das vítimas esteja associada aos conteúdos em causa. As vítimas são geralmente perseguidas, ameaçadas e podem ver-se obrigadas a abandonar a sua vida "normal" como resultado da sobre-exposição da sua imagem. Alguns países já tratam este problema como um crime e, como tal, punido judicialmente.

Existem ainda poucos estudos que revejam este assunto com a profundidade necessária, no entanto as Linhas de Apoio do Centro Internet Segura do Reino Unido afirmam que esta situação está cada vez mais presente, lidando com um crescimento do número de queixas. No relatório publicado pela **EU Kids Online, "The meaning of online problematic situations for children",** é reportado que o fenómeno ocorre também na faixa etária dos 9 aos 16 anos. Para além das situações evidenciadas, as crianças revelaram ainda que tinham conhecimento de incidentes que envolviam os seus pares a partilhar imagens de foro sexual dos seus parceiros românticos anteriores, como forma de vingança.

Internet Segura e Acreditar, 2016

Proteja os seus filhos

Controlo parental

Um sistema de controlo parental determina que conteúdo está disponível ou indisponível num computador ou rede de computadores. Estes sistemas são utilizados pelos pais para controlar o acesso dos filhos a material que considerem inapropriado para a idade destes ou por administradores de sistemas de instituições públicas ou privadas que pretendam igualmente bloquear o acesso a conteúdos – conteúdos que violem a lei ou sejam inapropriados para serem visionados na rede, como é o caso das escolas ou bibliotecas públicas.

Os conteúdos normalmente filtrados por estes sistemas são:

- Conteúdo sexualmente explícito como pornografia, erotismo, discussões sobre sexo e sexualidade em todas as suas vertentes;
- Conteúdo violento;
- Promoção ou discussão sobre vícios: jogos de apostas *online*, drogas, álcool, etc.
- Promoção ou discussão de racismo e xenofobia;
- Conteúdos ilegais;
- Promoção ou discussão de pirataria, técnicas criminais ou outros atos ilegais;
- Conteúdos que não estão dentro do âmbito das funções destinadas ao computador ou rede de computadores;
- Redes sociais (com o intuito de proteger as crianças de pedófilos ou predadores sexuais).

Os sistemas de controlo de conteúdos por *software* consistem em programas que se instalam no computador, para que o acesso a determinados conteúdos seja controlado.

Dentro deste conceito existem vários produtos muito diferentes entre si. Alguns produtos apenas filtram conteúdos consultados na Internet (protocolo http), com base no endereço dessa mesma página ou através de determinadas expressões ou palavras; enquanto, que outros controlam também correio eletrónico (protocolo pop e smtp), ou ainda outras aplicações como programas de mensagens instantâneas (por ex. *MSN Messenger*), ou até todo o sistema (documentos abertos, explorador de ficheiros, etc.), igualmente com base em palavras ou expressões que encontrem em algum destes sítios ou ferramentas.

Existem ainda programas de controlo de conteúdos que têm apenas a funcionalidade de filtrar conteúdo. Existem, por outro lado, filtros incluídos em programas de segurança mais abrangentes como *suites* de segurança que incluem *firewall*, filtros de SPAM, filtros de *phishing*, etc.

Para controlar o acesso a páginas da Internet com base no seu endereço, os sistemas de controlo recorrem a *listas negras* (*blacklist*) e/ou *listas brancas* (*whitelist*).

As *listas negras* são listagens com vários endereços, que foram previamente catalogados, referentes a um determinado tema indesejado. Nestes sistemas é permitido o acesso a qualquer página exceto aquelas que constam dessa *lista negra*. Existem várias listas atualizadas frequentemente e divididas em várias categorias (pornografia, jogos, *chat's*, etc...) disponíveis aos utilizadores comuns, sendo que algumas são completamente gratuitas e outras pressupõem o pagamento de uma mensalidade/anuidade para que possam ser descarregadas/consultadas. Alguns sistemas atualizam-se automaticamente sendo transparente para o utilizador a utilização destas listas. O capítulo seguinte enumera algumas dessas listas.

As *listas brancas* são o oposto das *listas negras*. Neste caso também se recorre a uma lista de endereços, mas apenas se permite o acesso aos endereços que constam nessa lista, sendo que todos os outros endereços são bloqueados.

Para além destes sistemas, existem outros que permitem a definição de várias palavras-chave. Ou seja, quando um utilizador pretende aceder a uma página na Internet, é feita uma pesquisa pelas palavras-chave definidas na página a disponibilizar. Se for encontrada alguma das palavras-chave definida, o conteúdo dessa página não é disponibilizado ao utilizador. Estes sistemas apresentam algumas vantagens em relação aos anteriores, uma vez que, quando uma nova página com conteúdo indesejável é colocada *online*, há um intervalo de tempo em que a página não foi catalogada e adicionada à respetiva lista negra - o que faz com que esta esteja acessível durante esse período de tempo. Apresentam ainda vantagens ao nível da abrangência, uma vez que não restringem as capacidades de controlo à navegação em páginas da Internet e ao protocolo HTTP, podendo desta forma ser utilizados para controlar o uso de outras aplicações. No entanto, apresentam também uma desvantagem, já que a pesquisa pelas palavras-chave tem custos em termos de tempo, tornando a navegação na Internet sensivelmente mais lenta do que no caso de controlo por endereço.

Que produtos existem nesta categoria?

Os produtos aqui apresentados, bem como a ordem pela qual são apresentados, não representam nenhuma preferência da nossa parte e apenas se pretende indicar quais as opções existentes no mercado. De notar ainda que grande parte destes sistemas não foi testada pela nossa equipa e, assim sendo, não podemos testemunhar a eficácia dos produtos mencionados.

Filtros de Conteúdo Comerciais:

- BitDefender Internet Security 2008 (Windows)
- BSecure (Windows)
- ContentBarrier (Mac & Windows)
- Cyber Patrol (Windows)
- Cyber Sentinel (Windows)
- CyberSieve (Windows)
- Cybersitter (Mac & Windows)
- F-Secure Internet Security (Windows)
- TrendMicro Internet Security (Windows)
- Intego Security Barrier (Mac)
- Internet Filter / Integrity online (Windows)
- Kidsnet Light (Windows)
- Magic Desktop (Windows)
- McAfee Total Protection (Windows)
- McAfee Internet Security (Windows)
- Net Nanny - antigo ContentProtect (Windows)
- Norton Internet Security (Windows & Mac)
- Optenet PC Content Filter (Windows)
- Panda Internet Security (Windows)
- Parents Carefree (Windows)
- Safe Eyes (Windows & Mac)
- Websense Web Filter (Windows)

Filtros de Conteúdo Grátis:

- CensorNet (Linux)
- DansGuardian (Linux)
- K9 Web Protection (Windows)
- Naomi (Windows)
- We-blocker (Windows)

Outros:

- Microsoft Internet Explorer 6 Content Advisor (Windows)
- Glubble: Extensão para o browser Mozilla Firefox (Windows, Mac & Linux)

Listas Negras (blacklists):

- URLBlacklist (gratuita)
- MESD (gratuita)
- Shalla's Blacklist (gratuita)
- Websense (paga)

Quais as principais vantagens?

Permitem o bloqueio efetivo a sítios com conteúdos não desejáveis;
Nos filtros por palavra-chave, permitem o bloqueio de uma página com conteúdos desadequados, logo a partir do momento em que esta é colocada *online*;
Alguns filtros permitem o controlo de conteúdos noutras aplicações como correio eletrónico, sistemas de mensagens instantâneas (msn, yahoo, etc.), explorador de ficheiros do computador, etc.;
Alguns sistemas estão integrados em aplicações de segurança geral;
Facilidade de utilização de alguns sistemas;
Alguns sistemas permitem a criação de perfis, possibilitando, por exemplo, que as regras de acesso de um utilizador menor de idade não se apliquem a um adulto;
Proteção contra páginas perigosas que exploram vulnerabilidades do sistema operativo, evitando assim alguns ataques à segurança do computador;
Proteção contra páginas que contêm esquemas de roubo de identidade (*phishing*) e fraude;
Armazenamento dos dados sobre cada bloqueio, permitindo saber quem e quando tentou aceder a uma página com conteúdo indesejável;
Permite estabelecer horários de ligação à Internet, bem como monitorizar o tempo que um utilizador esteve *online*.

International Telecommunication Union

Quais as principais desvantagens?

Com alguns conhecimentos, estes sistemas podem ser desativados pelos utilizadores do computador;
Existem páginas na Internet que explicam como ultrapassar este tipo de filtros;
Apenas bloqueia o acesso no computador em que está instalado. No caso de necessidade de controlar vários computadores, necessita de instalação em cada um deles;
Pode bloquear "sítios positivos", ou seja, bloquear o acesso a sítios que não têm conteúdo considerado indesejável;
Podem criar uma falsa sensação de segurança em que o utilizador, ao ver que o sítio não está bloqueado, considera que o conteúdo deste é adequado para si (podendo não ser o caso);
Alguns sistemas apenas controlam o conteúdo em páginas da Internet, filtrando as comunicações através do protocolo HTTP, não filtrando as outras aplicações (mensagens instantâneas, correio eletrónico, outros programas do computador...) e protocolos (FTP, *telnet*, ligações através de um *proxy*...);
Alguns sistemas apenas suportam uma ou duas línguas. Usando o mesmo termo noutra língua pode ser suficiente para "enganar" o filtro;

Alguns motores de pesquisa armazenam informação de páginas pesquisadas em *cache*, tornando o conteúdo de uma página, que possa estar inacessível no sistema de controlo de conteúdos, disponível ou parcialmente disponível.

Guia de Boas Práticas de Segurança – Página Web da Internet Segura, acedida em 4 de Outubro 2017.

International Telecommunication Union

Sobre Segurança Infantil na Internet recomendamos

Manual de ação para jovens - Dá a tua opinião sobre os teus direitos online! (2017)

Publicação da Insight, Miúdos Seguros na Net e Telefono Azzurro, tendo o Instituto de Apoio à Criança como um dos parceiros: "Este Manual de Ação Para Jovens não pretende apenas fazer-te pensar sobre os teus direitos na Internet, mas também te dá a possibilidade de garantires que a tua voz seja ouvida pelas entidades que decidem e que legislam em Portugal. Como? Publica as tuas criações e comentários sobre as atividades deste manual na tua plataforma de redes sociais favorita (que aceita hashtags, como o Facebook, Google+, Instagram, Pinterest, Tumblr ou Twitter) antes de 15 de dezembro de 2017. O teu trabalho será enviado para os decisores nacionais e da Comissão Europeia e contribuirá para a construção de um livro e de uma carta de Direitos e Deveres da Criança e Adolescente na Internet, os quais serão lançados publicamente em janeiro e fevereiro de 2018.

Disponível on-line »

Coleção de livros infantis "O Pisca faz Faísca" (2017)

No âmbito do projeto SeguraNet, a Direção-Geral da Educação enviou, durante o mês de maio de 2017, aos Jardins de Infância, do ensino público, uma coleção de três histórias infantis "O Pisca faz Faísca!". Com este recurso, pretende-se alcançar, o público em idade pré-escolar, abordando temáticas prementes para esta faixa etária no que respeita à cidadania digital.
Sugere-se a visita guiada ao *website* "O Pisca faz Faísca": http://pisca.seguranet.pt/, um espaço *online* que disponibiliza a coleção das histórias em formato digital e onde poderão ainda ser exploradas diversas atividades (adivinhas, sopa de letras, correspondências, pinturas, entre outras).
A autora dos livros é Cristina de Carvalho e a ilustração ficou a cargo de Ana Fonseca.

Disponível on-line »

Parenting in the Digital Age (2017)

Publicação da Save the Children România: "At national level, a real phenomenon has occurred around the connection of tragic events to the online challenge that targets children and adolescents, called "Blue Wale". Although these situations are not officially linked by the authorities, the impact at social level is very high and there is a feeling of fear especially among those with children in their care. The general appeal seems to be blaming the parents, the teachers, or even the children. Our proposal is not to follow this provocation but to stop for a few moments to look in depth. We can transform this national context into an opportunity to open up more authentic discussions with children, to help them connect with life, the natural enjoyments of their age, the alternatives they have to socialize and, most importantly, to remind ourselves as adults that the relationships we cultivate with children are the basis for their development. We invite you to ask your child or pupil what he or she understands from this massive promotion of the existence of dangerous challenges in the online environment. From our experience, this is the easiest way to understand how this information reaches children and how they relate to it. Regardless of his or her answer, you can use this discussion to get to a closer level with your child with more openness, curiosity and gentleness and to understand what his or her personal experience is".

Disponível on-line »

Estudo Crescendo entre Ecrãs. Usos de meios eletrónicos por crianças (3-8 anos) (2017)

Livro editado pela ERC - Entidade Reguladora para a Comunicação Social. Disponível on-line »

Recommendation CM/REC(2018)x of the Committee of Ministers to Member States on Guidelines to promote, protect and fulfill children's rights in the digital environment (revised draft, 25 July 2017)

Documento da responsabilidade do Conselho da Europa:
"34 - States should ensure that children have the right to have their personal data erased when they withdraw their consent or object to the processing of personal data concerning them, especially where this compromises their dignity, security and privacy.
(…)
90 - States should encourage the production by business enterprises of parental controls that can mitigate risks for children in the digital environment and, where appropriate, monitor standards applied so that they are not unduly restrictive or give a false sense of security".

Disponível on-line »

A influência dos estilos parentais na utilização da Internet por crianças e adolescentes (2016)

Tese de Mestrado de Sandra Mendonça: "O presente estudo tem por objetivo compreender de que forma os estilos parentais influenciam a utilização da Internet por crianças e adolescente. Por sua vez, pretende-se perceber como as famílias de baixo contexto socioeconómico e condição de imigrante acompanham e medeiam a utilização da Internet pelos filhos. A amostra utilizada envolveu 119 crianças e adolescentes e respetivo pai ou mãe. Os dados foram recolhidos mediante a aplicação de um questionário construído para o efeito. De acordo com os resultados, a utilização da internet é elevada entre as crianças e adolescentes, verificando-se o mesmo nos pais. A casa é o local de maior acesso e o recurso mais utilizado é o telemóvel. Os pais revelam-se mais confiantes na utilização da internet, comparativamente aos filhos. O estilo autoritativo na utilização da internet é o mais evidente entre os pais em estudo. Quanto às estratégias de mediação parental, todas evidenciam uma correlação positiva com os estilos parentais. A mediação ativa da segurança é a mais utilizada entre os pais em estudo, sendo que falar com a criança/adolescente sobre o que faz na internet e nas redes sociais são as práticas mais realizadas. Em relação aos riscos, a sua expressão entre as crianças e adolescentes em estudo é relativamente baixa, não se verificando diferenças a nível de sexo. Face aos estilos parentais, estes não parecem ter influência na redução dos riscos. Contrariamente às pesquisas de Valcke et al (2010) os que estilos parentais não parecem influenciar significativamente a utilização da internet pelas crianças e adolescentes".

Disponível on-line »

International Telecommunication Union

Em Portugal, no que concerne à exposição aos riscos, de acordo com as informações do estudo Net Children, Go Mobile (2014), apenas 10% das crianças e adolescentes reportaram sentir-se incomodado, por algo que tenha encontrado na internet, com maior incidência entre as raparigas, sobretudo as mais velhas (13-14 anos), e crianças de famílias de meios socioeconómicos baixos. Em relação aos tipos de risco encontrados, considerando o Bullying, uma em 10 crianças refere ter experienciado esta situação, sobretudo as raparigas (13%) tanto as mais novas (9-10 anos) como as adolescentes de idade intermédia (13-14 anos). Quanto às mensagens sexuais, também designado por Sexting, apenas 5% das crianças e adolescentes portugueses mencionaram ter experienciado esta situação, situando-se abaixo da média europeia (11%). Relativamente aos encontros com alguém que conheceram na internet, 11% das crianças e adolescentes portugueses revelaram ter tido esta experiência, com forte incidência entre os adolescentes acima dos 12 anos. Não se registam diferenças significativas a nível do género e estatuto socioeconómico. Estes valores situam-se abaixo da média europeia (26%). A nível da visualização de imagens sexuais, 27% das crianças e adolescentes portugueses declaram ter visto imagens sexuais nos últimos 12 meses, sobretudo os adolescentes entre 15-16 anos e crianças e adolescentes baixo estatuto socioeconómico.

Relativamente à exposição a outros conteúdos inapropriados, nomeadamente distúrbios alimentares, conteúdos de incentivo à automutilação ou ao consumo de drogas, materiais que promovem discriminação e violência contra certos grupos 10% das crianças e adolescentes portugueses viram um ou mais destes tipos de conteúdos.

As percentagens mais elevadas são referentes a publicação de mensagens que atacam certos grupos (8%), conteúdos que falam sobre ou sugerem formas de automutilação (6%) e conteúdos que incentivam distúrbios alimentares (5%). Estes valores encontram-se abaixo da média europeia (20%, 11% e 13% respetivamente).

Foram ainda mencionados outros riscos, sendo os valores mais elevados referentes a vírus no computador (15%), uso indevido da sua password/telemóvel para aceder à informação do próprio ou para se passar por este (4%) e uso da sua informação pessoal de uma forma que não gostou (2%). No que respeita à forma como as criança e adolescentes lidam com os riscos com os quais se deparam na internet, a procura de apoio junto dos pais é a situação mais mencionada, sendo a mãe mais solicitada (68%), em comparação ao pai (53%). Os irmãos (36%) e amigos (32%) surgem posteriormente.

MENDONÇA, 2016: 15

É bom saber: um guia para se manter seguro e protegido online (2016?)

Uma edição conjunta da Google com a Internet Segura. Disponível on-line »

Jogar online em segurança (2016)

Publicação para jovens, da Internet Segura. Disponível on-line »

Privacidade no Facebook (2016)

Publicação para jovens, da Internet Segura. Disponível on-line »

Redes sociais é bom estar seguro: para filhos (2016)

Brochura para jovens, da Internet Segura e da Acreditar. Disponível on-line »

Dicas de segurança para crianças e jovens: PROTEGE-TE (2016)

Conselhos do Instituto de Apoio à Criança. Disponível on-line »

Será que sabes tudo sobre smartphones? (2016)

Publicação para jovens, da Internet Segura: "Um smartphone, tal como os computadores, é vulnerável a certos perigos, como os do Phishing, SPAM, Malware, roubo de informação pessoal e/ou de identidade e também cyberbullying. Assim, a maioria das regras de segurança que se aplicam para os primeiros aplicam-se aqui também. Tal como no computador, quando um smartphone fica infetado é possível detetar uma diminuição na sua performance, o aparecimento de aplicações estranhas que não foram instaladas pelo utilizador, a alteração de configurações no telemóvel, bem como uma diminuição drástica no tempo de vida útil da bateria. Alguns dos vírus que se encontram nos telemóveis têm como objetivo o roubo de palavras-passe dos utilizadores, autenticações bancárias, ou mesmo envio de mensagens e chamadas para números de valor acrescentado. Neste sentido, é importante que os utilizadores estejam atentos ao registo de chamadas e mensagens, à interrupção de chamadas sem motivo aparente ou a aumentos inexplicáveis do tráfego de dados". p. 3

Disponível on-line »

Estudo de avaliação de impacto do Projeto Seguranet (2016)

Publicação da responsabilidade do Ministério da Educação - Direção Geral de Educação: "O projeto Seguranet faz parte integrante do "Internet Segura", o programa nacional dedicado à segurança na Internet e é da responsabilidade de um consórcio de entidades públicas e privadas portuguesas, entre estas, o Ministério da Educação e Ciência - a Fundação para a Ciência e a Tecnologia (que coordena), a Direção-Geral de Educação/ ERTE, a Fundação para a Computação Científica Nacional - a Microsoft Portugal e outros parceiros da sociedade civil, como associações, empresas e universidades, entre outras. O Programa Internet Segura tem como objetivo combater a existência de conteúdos ilegais na Internet, minimizar os efeitos de conteúdos ilegais e lesivos nos cidadãos, promover a utilização segura da Internet e a consciencialização da sociedade para os riscos associados à utilização da Internet. O consórcio coopera ativamente com organizações internacionais e em particular com a INHOPE (International Association of Internet Hotlines) e com a rede europeia INSAFE. Recorde-se que o INSAFE é a uma rede europeia de centros de consciencialização que promovem o uso seguro e responsável da Internet e dos dispositivos móveis por jovens. As ações a desenvolver pelo consórcio organizam-se em projetos estruturantes, projetos de intervenção transversal e projetos de intervenção focalizada. O projeto Seguranet enquadra-se na estratégia geral do consórcio que é responsável pelo Programa Internet Segura em Portugal. O projeto Seguranet constitui-se como um projeto focalizado, centra-se em particular nas populações escolares e tem como missão promover o uso seguro e crítico da Internet por parte dos alunos/alunas portugueses e é coordenado pela Direção Geral da Educação – Equipa de Recursos e Tecnologias Educativas. Tendo em vista alcançar os objetivo da sua missão, o projeto Seguranet promove, junto das escolas, dos professores, dos alunos e da comunidade, um conjunto de ações, atividades e iniciativas que contribuem para a aquisição de conhecimentos acerca dos benefícios e dos riscos da Internet e a adoção de comportamentos seguros e atitudes responsáveis por parte das crianças e dos jovens. O estudo de avaliação que se apresenta abrange especificamente os seguintes vetores de ação do projeto Seguranet:

1. Portal Seguranet - que fornece conteúdos e propostas de atividades para cada um dos diferentes grupos-alvo;
2. Os Desafios - que constituem propostas de trabalho educativo em torno da temática do uso seguro da Internet bem como envolvem a criação e produção de conteúdos;
3. Intervenções e atividades - tais como ações de sensibilização destinadas a alunos, professores, pais e comunidade educativa e especificamente as ações promovidas pelos Centros de Competência TIC da DGE-RTE.
4. Semana da Internet Mais Segura - uma proposta anual de iniciativa europeia desenvolvida e promovida em Portugal pelo Centro de Internet Segura e pelo Projeto Seguranet durante o mês de Fevereiro de cada ano.
5. Escola eSafety Label - uma iniciativa que permite a distinção das escolas com o Selo de Segurança Digital, como aquelas escolas que promovem a segurança online da comunidade educativa e que por isso se envolvem em atividades relacionadas com a segurança de crianças e jovens e promovem elevados padrões de segurança na instituição.
6. Painel de jovens - que é constituído por jovens pertencentes a escolas participantes no projeto Seguranet que se reúnem e participam ativamente nas sua atividades, sendo as suas opiniões e perspetivas consideradas quando do planeamento de novas ações, novos materiais ou atividades.
7. Equipa Seguranet – corresponde à estrutura do Ministério da Educação e Ciência - DGE-ERTE – e que é responsável pela implementação do projeto em Portugal. Cada uma das dimensões assinaladas concorre para os objetivos do projeto Seguranet e, neste sentido, corresponde a diferentes propostas de trabalho educativo, com diferentes atores, recursos, tecnologias, contextos e intervenientes pelo que são de esperar formas de intervenção e ação muito diferenciadas".

Disponível on-line »

Guidelines for Child Online Protection (2016)

Edição da International Telecommunication Union (ITU): "This manual contains Guidelines for children and young people in all parts of the world on how to keep themselves and others safe online. However, a young internet user of seven years of age is very unlikely to have the same needs or interests as a 12 year old just starting at High School or a 17 year old on the brink of adulthood. At different points in the Guidelines, the advice or recommendations fits these different contexts".

Disponível on-line »

Dependências online - o poder das tecnologias (2016)

Publicação da responsabilidade da Seguranet. Disponível on-line »

Internet Safety for Kids (2015)

Curso gratuito de segurança da criança na internet em inglês, da responsabilidade da Goodwill Community Foundation: "In this free Internet Safety for Kids tutorial, learn Internet safety tips for keeping kids safe from online predators and cyberbullies."

Disponível on-line »

A segurança na internet: utilização da internet como recurso educativo no 1º ciclo do ensino básico (2015)

Comunicação de Carina Félix e Henrique Gil: "As TIC passam a ser elemento constituinte da aprendizagem e os professores devem proporcionar, a todos os alunos, as mesmas oportunidades e condições a nível de literacia digital, nomeadamente através de novas e diferentes abordagens dos conteúdos. Neste sentido, este projeto teve como principal objetivo averiguar se a Internet é segura para as crianças do 1º Ciclo do Ensino Básico e quais os procedimentos preventivos mais adequados para melhorar essa segurança. Para o efeito, foi realizada uma investigação no âmbito da Prática de Ensino Supervisionada tendo-se envolvido uma turma do 1º Ciclo do Ensino Básico. (…) Em termos gerais, pode-se afirmar que os resultados permitiram verificar que ainda há muito a fazer na prevenção para uma utilização segura da Internet. A grande maioria dos participantes, apesar de ter consciência dos perigos que a utilização da Internet poder vir a promover, desconhece as principais ferramentas digitais que permitem uma utilização segura. E, por outro lado, verificou-se também que os pais desconhecem, em larga escala, o tipo de utilização que os seus filhos fazem da Internet".

Disponível on-line »

International Telecommunication Union

Internet segura no 1º ciclo do ensino básico: a internet como recurso educativo na prática de ensino supervisionada (2015)

Comunicação de Carina Félix e Henrique Gil: "Na escola, as TIC passam a ser um elemento constituinte do processo de ensino, de aprendizagem e os professores devem proporcionar, a todos os alunos, as mesmas oportunidades e condições a nível de literacia digital, nomeadamente através de novas e diferentes abordagens dos conteúdos. Neste sentido, esta investigação teve corno objetivo principal averiguar se a Internet é segura para as crianças do 1º ciclo e quais os procedimentos preventivos mais adequados para melhorar essa segurança.

Disponível on-line »

App Internet Segura – Fundação para a Ciência e Tecnologia (2015)

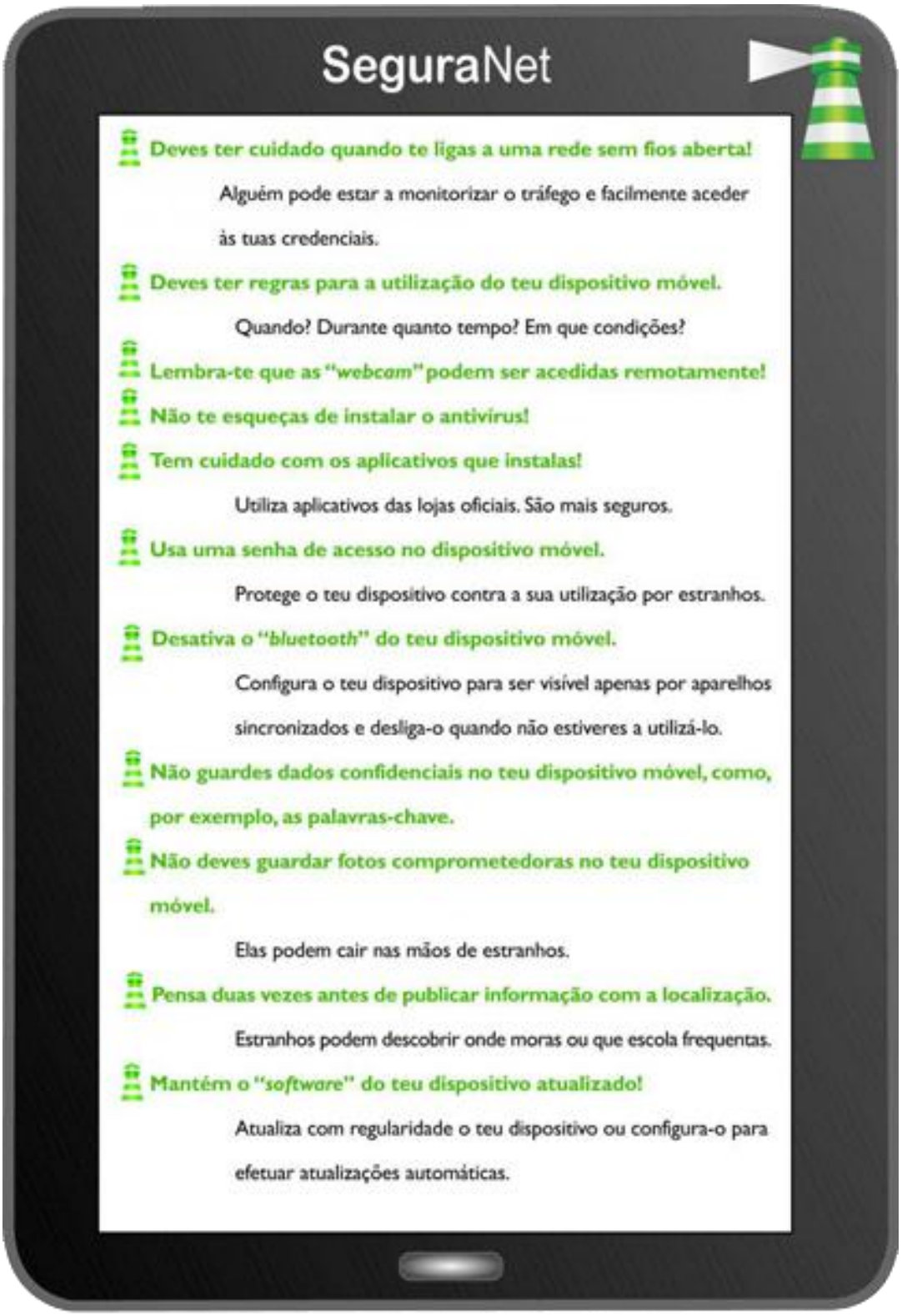
Esta aplicação está disponível para download gratuito e é compatível com todos os dispositivos: "A segurança online nunca foi tão importante e a app Internet Segura, da Fundação para a Ciência e Tecnologia, vem dar resposta a todas as dúvidas e incertezas que navegar online pode trazer. Através do seu Centro Internet Segura, a FCT pretende contribuir proativamente no combate às condutas e aos conteúdos online maliciosos ou ilegais, minimizando os potenciais riscos que podem advir do uso das tecnologias da informação e da comunicação. Assim, tem como principal missão promover uma utilização segura da Internet, juntamente com a consciencialização da sociedade para os riscos associados ao uso da mesma.

Disponível on-line »

App Internet Segura

Indicações para a utilização segura dos dispositivos móveis (2015)

Documento disponibilizado pela Seguranet. Disponível on-line »


SeguraNet
Deves ter cuidado quando te ligas a uma rede sem fios aberta!
Alguém pode estar a monitorizar o tráfego e facilmente aceder às tuas credenciais.
Deves ter regras para a utilização do teu dispositivo móvel.
Quando? Durante quanto tempo? Em que condições?
Lembra-te que as "webcam" podem ser acedidas remotamente!
Não te esqueças de instalar o antivírus!
Tem cuidado com os aplicativos que instalas!
Utiliza aplicativos das lojas oficiais. São mais seguros.
Usa uma senha de acesso no dispositivo móvel.
Protege o teu dispositivo contra a sua utilização por estranhos.
Desativa o "bluetooth" do teu dispositivo móvel.
Configura o teu dispositivo para ser visível apenas por aparelhos sincronizados e desliga-o quando não estiveres a utilizá-lo.
Não guardes dados confidenciais no teu dispositivo móvel, como, por exemplo, as palavras-chave.
Não deves guardar fotos comprometedoras no teu dispositivo móvel.
Elas podem cair nas mãos de estranhos.
Pensa duas vezes antes de publicar informação com a localização.
Estranhos podem descobrir onde moras ou que escola frequentas.
Mantém o "software" do teu dispositivo atualizado!
Atualiza com regularidade o teu dispositivo ou configura-o para efetuar atualizações automáticas.

Seguranet

A segurança na internet no 1º ciclo do ensino básico: utilização da internet como recurso educativo na prática supervisionada (2014)

Tese de Mestrado de Carina Félix: "Atualmente as Tecnologias de Informação e Comunicação (TIC) têm vindo a fazer parte de uma realidade, onde os indivíduos trabalham, comunicam, interagem, investem, aprendem e ocupam os seus tempos livres. Deste modo, a escola, enquanto instituição social, não poderia ficar indiferente às TIC. Na escola, as TIC passam a ser elemento constituinte de aprendizagem e os professores devem proporcionar, a todos os alunos, as mesmas oportunidades e condições a nível de literacia digital, nomeadamente através de novas e diferentes abordagens dos conteúdos. A Internet também tem vindo a transformar a maneira como as crianças vivem, as formas de lazer e novas formas de interação social. As crianças deparam-se com mudanças constantes que geram novos problemas e novas necessidades, tornando-se necessário que sejam capazes de pensar por si mesmos e de resolver esses problemas. Neste sentido, este projeto teve como objetivo principal averiguar se a internet é segura para as crianças do 1º ciclo e quais os procedimentos preventivos mais adequados para melhorar essa segurança".

Disponível on-line »

De acordo com um estudo sobre jovens e as tecnologias realizado por Ferreira, Mendes e Pereira (2001), referido por Baltazar (2004), é em casa e na escola que os jovens mais consultam e utilizam as tecnologias, nomeadamente, a Internet. Assim, reforça-se a ideia de que os pais e professores devem ter um papel marcante no auxílio e na educação dos jovens utilizadores deste meio. O facto de existir um adulto presente para ajudar, explicar e alertar é fundamental e pode marcar a diferença. Segundo Papert (1997), os pais sentem-se muito orgulhosos da relação e da facilidade com que os seus filhos usam a Internet para poderem adquirir novas aprendizagens, mas muitos sentem-se distante dessa realidade que eles próprios desconhecem. As crianças ao mostrarem tão grande facilidade de aprendizagem no que diz respeito às tecnologias não significa que estes estejam conscientes dos perigos que existem na Internet e dos riscos que correm ao utilizá-la. Ainda para Thierry De Smedt (2003), referido por Baltazar (2004), os jovens têm tendência a não atribuir importância aos riscos, considerando-os sempre afastados da sua própria realidade. Os utilizadores da Internet por se encontrarem em ambientes familiares (casa e escola), por vezes sentem-se confortáveis, protegidos e despreocupados. Assim, os educadores têm um papel central: aconselhar, alertar e, especialmente dialogar com os jovens sobre os perigos que existem na Internet, tal como os devem aconselhar sobre os perigos que existem nas suas vidas quotidianas e que devem evitar.

FÉLIX, 2014: 55-56

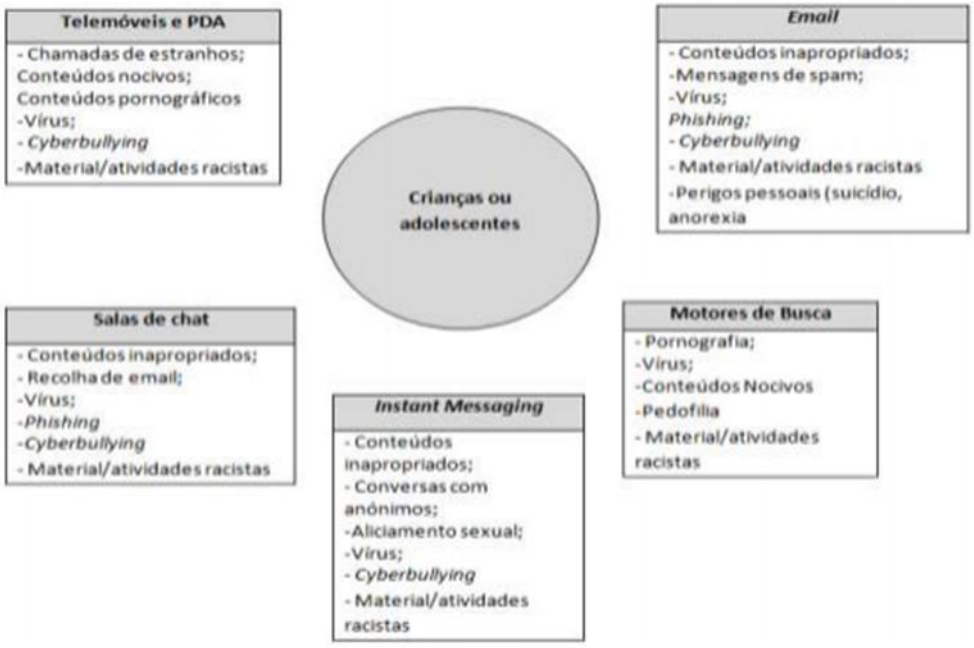


Figura 14 - Tecnologias e serviços disponibilizados na Internet que são utilizados pelas crianças (Adaptado de Santos & Manteigas, 2010 e Livingstone (2003)

FÉLIX, 2014: 71

Tipologias de riscos online

De acordo com a figura 14 apresentada anteriormente, serão agora analisados os vários tipos de riscos online:

1. Fishing

De acordo com a informação disponibilizada no site da Internet Segura "phishing" (trocadilho com fishing, ou ir à pesca, consiste em utilizar métodos para que o cibernauta revele os seus dados pessoais e confidenciais. O phishing é uma "vigarice" que utiliza SPAM ou mensagens de pop-up para as pessoas revelarem os seus números pessoais do cartão de crédito, informações bancárias, números de segurança social, passwords ou outro tipo de informação confidencial. O phishing segundo Whitby, 2013, traduz-se no roubo de dados pessoais financeiros, como o número de cartão de crédito, o código do cartão de débito, ou elementos pessoais de acesso a contas bancárias. O phishing pode envolver os mais novos na qualidade de participantes, quando estes estão em contacto com terceiros.

(continua)

2. Aliciamento

O aliciamento, é uma "conduta de um suspeito de pedofilia que dê a uma pessoa racional motivos de preocupação de qualquer encontro pessoal com uma criança, derivado dessa conduta, se pode destinar a fins ilícitos". Para podermos perceber o que é o aliciamento deve-se primeiro compreender a diferença entre pedófilo e predador sexual. O pedófilo interessa-se por crianças que estão na fase dos 6-10 anos e o predador interessa-se por jovens com mais de 10 anos. (Whitby, 2013). Conforme foi analisado no Centro de Proteção Online (CEOP), contra a Exploração de Crianças no Reino Unido, entre fevereiro de 2009 e março de 2010 registaram-se 6291 denúncias de suspeitas de abuso sexual de crianças, 25% pertencente ao aliciamento (Whitby, 2013).

De acordo com Martellozzo citada por Whitby (2013), criminologista do Reino Unido, o aliciamento pode assumir várias formas, as quais se passam a apresentar:

- *Os aliciadores mostram interesse na vida das crianças mostrando compreendê-las;*
- *Grande abertura, confiança e a máxima cautela na abordagem do assunto. Têm um comportamento passivo, estudando primeiro o comportamento da criança;*
- *Os aliciadores mais confiantes podem declarar abertamente um desejo «pervertido» de relações pedófilas;*
- *Os mais cautelosos colocam figuras de banda desenhada ou brinquedos como foto de perfil;*
- *Os "hipercautelosos" são os mais perigosos, porque sabem como não deixar rasto sendo os mais difíceis de identificar;*
- *Muitos aliciadores não pretendem encontrar-se com uma criança, eles procuram imagens para partilhar com outros aliciadores;*
- *Alguns obtêm essas imagens para com elas poderem vir a chantagear;*
- *Crianças mais vulneráveis ao aliciamento veem de famílias disfuncionais.*

No entanto os números de casos denunciados deve-se à campanha ClickCEOP, no primeiro mês de lançamento desta aplicação, mais de 200 utilizadores do Facebook no Reino Unido denunciaram comportamentos suspeitos (Whitby, 2013). Em Portugal, pode-se utilizar o site da Linha Aberta da Internet Segura que também denuncia conteúdos ilegais. A Linha Aberta faz parte de um projeto denominado Internet Segura e co-financiado pela Comissão Europeia ao abrigo do programa Safer Internet Plus.

(continua)

3. Pornografia Infantil

A pornografia infantil, através da Internet, é uma realidade infelizmente incontornável, tornando-se numa nova modalidade online, que atrai adultos, adolescentes e crianças através de enunciados sobre a pedofilia virtual. Hoje, a pornografia infantil online constitui também uma forma rentável de exploração de crianças e adolescentes, incentivando a prostituição infantil com fotos, DVDs e vídeos, mostrando nus de adolescentes em poses de índole sexual e erótica, ainda neste contexto, a conduta criminosa das pessoas que trabalham as redes internacionais de pornografia infantil consiste, entre outras, em enganar e seduzir famílias que deixam os filhos posarem para fotos pseudoartísticas (Santos e Manteigas, 2010).

Através de sites específicos sobre sexo, é possível encontrar fotos, vídeos, textos de contexto erótico, Serra (2009) refere que a Net segue o dinheiro. Os militares tiveram dinheiro para criá-la e a indústria do sexo tem dinheiro para expandi-la. Para Jorge (2012), cerca de 24% das crianças e jovens afirmam ter visto imagens de cariz sexual, online e offline, tendo uma predominância masculina (81%). A internet é a fonte de imagens de cariz sexual para cerca de metade destes jovens que as viram online e offline. As crianças mais novas veem este tipo de imagens em revistas ou livros, ou através de televisão ou filmes. Pelo contrário, o telemóvel através de SMS ou MMS, ou Bluetooth são os vínculos mais populares entre os mais velhos (24% dos jovens com 13-14 anos), ou seja, apesar da dramatização do contacto das crianças com estes conteúdos pornográficos através da Internet, continua a haver outras fontes destes conteúdos, numa cultura crescentemente sexualizada, que também têm as suas manifestações entre a cultura juvenil.

Em Portugal existe uma lei fundamental que criminaliza a pornografia infantil, através do art.º 172º., n.º3, al. d) 172 do Código Penal. Este artigo estipula que quem exibir ou ceder a qualquer título ou por qualquer meio – que poderá ser veiculado através da Internet por meio de sítios, fóruns, salas de conversação, email, fotografias, filmes ou gravações pornográficas de menores de 14 anos, pratica o crime de abuso sexual, sendo punido com pena de prisão de 3 anos. Quem praticar esses atos com intenção lucrativa é punido com pena de prisão de 6 meses a 5 anos.

(continua)

4. Cyberbullying

Como já vimos anteriormente, as crianças e os adolescentes utilizam cada vez mais as tecnologias para comunicarem e se relacionarem. Nestes relacionamentos podem existir divergências ou conflitos, que se traduzem em determinadas ações levadas a cabo através de diversas formas e meios, incluindo a Internet e/ou qualquer dispositivo eletrónico de comunicação. Estas ações, quando são feitas através da Internet denominam-se por cyberbullying. De acordo com o site da Internet Segura a expressão cyberbullying é uma palavra composta por "cyber" diz respeito ao uso das novas tecnologias de comunicação (correio eletrónico, telemóveis) e o "bullying relativo ao fenómeno dos maus-tratos por parte de "rufião" (bully) ou grupo de rufiões. O cyberbullying para Santos e Manteigas (2010) verifica-se quando uma criança ou adolescente, que se esconde atrás do anonimato da Internet, provoca, intimida, ameaça, atormenta, importuna ou amedronta outra criança ou adolescente.

Para Slonje & Smith (2008), cyberbullying é definido como uma emergência do "Bullying que ocorre através de tecnologias modernas, e especificamente de telefones celulares ou da Internet" (147). Ainda para Silva (2010): " (…) no caso do cyberbullying a natureza vil de seus idealizadores e/ou executores ganha uma "blindagem" poderosa pela garantia de anonimato que eles adquirem (…) os bullies cibernéticos (ou virtuais) se valem de apelidos (nicknames), nomes de outras pessoas conhecidas ou de personagens famosos de filmes, novelas. Os bullies virtuais são a meu ver, verdadeiros covardes mascarados de valentões, que se escondem nas redes de "esgoto" do universo fantástico dos grandes avanços tecnológicos da humanidade" (126). Na opinião de Willard (2003), referido por Andrade (2012), os estudantes que se sentem mais confortáveis a comunicar online em vez de pessoalmente, tendem a encarar o Cyberbullying como um recurso, sendo um meio de vingança para os alunos que são vítimas de bullying na escola, tornando-se os agressores online. Para Pinheiro (2009), o cyberbullying é definido por "persistência", a "pesquisabilidade", a " replicabilidade". A persistência significa que tudo o que é colocado online fica registado para sempre. No que diz respeito à pesquisabilidade refere-se à possibilidade que qualquer pessoa tem de encontrar e aceder à informação colocada online e, por fim, a replicabilidade é a capacidade de reproduzir toda a informação que é colocada online, publicando e deixando de estar no controlo da pessoa.

(continua)

Willard (2013) refere que existem diferentes manifestações desta realidade, sendo elas as lutas online, o assédio, a difamação, a representação/personificação, as partilhas pessoais e embaraçosas, a exclusão e a perseguição online. Os perigos e efeitos nocivos relacionados com o cyberbullying são inúmeros sendo eles de psicológico os mais comuns (Santos e Manteigas, 2010):

- *Aumento do número de casos: o crescimento da acessibilidade às TIC faz com que exista uma cada vez maior quantidade de meios e de vítimas do cyberbullying;*

- *Graves consequências ao nível psicológico: Vários estudos indicam que as consequências psicológicas resultantes do cyberbullying são maiores do que as do bullying praticado sem recurso à tecnologia;*

- *Se as vítimas forem alvo de ações continuadas de cyberbullying, poderão assumir comportamentos depressivos ou suicidas;*

- *Publicação, em sítios na Internet e em blogues, de conteúdo violentos, inapropriados, provocadores, ameaçadores ou de índole sexual tendo como alvo as vítimas do cyberbullying.*

Em Portugal, o cyberbullying não é considerado um crime, mas as atividades que constituem o cyberbullying permitem que sejam tomadas medidas legais (Whitby, 2013). A prática do cyberbullying diminui com o aumento do nível de escolaridade, apurando-se que 74% dos alunos do 10º e 12º anos referiu que nunca enviou mensagens ofensivas enquanto que, no 9º ano, essa percentagem diminui para 44% (Azevedo, 2012). A escola deve estar consciente do problema do cyberbullying, pois esta deve promover a capacidade de se debruçarem sobre questões associadas à literacia digital, à segurança online, e ao uso responsável e positivo das TIC. Como refere Amado et al., (2009), " (…) quanto mais consciente a escola está acerca deste problema, quanto mais transparente é a sua forma de lidar com o mesmo, mais pequena é a dimensão que o problema parece assumir".

5. Pedofilia

Estes predadores sexuais são normalmente do sexo masculino e de meia-idade e pertencem a todas as classes sociais, normalmente sabem manusear bem as tecnologias de informação e comunicação navegando em fóruns, salas de conversação, Instant Messaging, blogues e sítios de relacionamento social. Conhecem bem o calão utilizado na Internet para contactar e desenvolver as suas atividades de predação sexual com menores (Santos e Manteigas, 2010).

(continua)

Para Hamada & Sanchez (2009), a troca de pornografia infantil não é a única atividade empregada, existe um prolongamento à invasão de sites de "bate-papo" em que os menores de idade se encontram. Alguns pedófilos utilizam esses sites para iniciar o processo de aliciamento das crianças. Estes predadores apresentam-se como um tipo especial de criança com relação à idade, género, passatempos e interesses de modo a atrair as crianças. A partir do momento que a criança responde, o processo de aliciamento ocorrerá em cinco estágios:

1) Formação da amizade;

2) Formação do relacionamento;

3) Avaliação do risco (por parte do pedófilo);

4) Exclusividade, em que a criança encontra-se presa à armadilha do pedófilo (ilusão de um relacionamento de amor e confiança mútuos);

5) Estágio sexual, consistente no aumento de introdução de material sexual (por meio de discrições verbais do pedófilo) e assim chegar à gratificação sexual por parte do pedófilo e o sentimento da criança em ser amada.

As crianças que se encontram mais vulneráveis às ações dos predadores sexuais são aquelas que têm problemas, estão desinformadas das ações deste tipo de predadores, estão a explorar a sua sexualidade e que tentam afastar-se do controlo dos pais, procurando novos relacionamentos fora do âmbito familiar (Santos & Manteigas, 2010). Dada a sua "imensidão", a internet permite que os pedófilos atuem livremente sem quaisquer interferências, onde muitos pedófilos desenvolveram habilidade e somaram conhecimentos que os tornam hackers (indivíduos com alto grau de conhecimentos sobre informática). Existem também os chamados cyberpunks (indivíduos com mega capacidade de compreensão de programas, dados e códigos, bem como análise rápida, estes indivíduos dificilmente serão apanhados (Hamada & Sanchez, 2009). A maneira como a informação é utilizada varia bastante, no entanto pode ser dividido em seis categorias o perfil dos utilizadores na Internet. Existem os colecionadores, os produtores, os sexualmente onívoros (praticantes de atividades sexuais bizarras), os curiosos sexuais (sujeitos a evoluir à pedofilia), os literários (que consideram as imagens de pornografia um direito) e os empresários (cuja definição não necessita de explicações). Infelizmente, com a evolução dos meios de acesso de informação, a pornografia infantil pode ser acedida em qualquer lugar (Hamada & Sanchez, 2009).

FÉLIX, 2014: 73-77

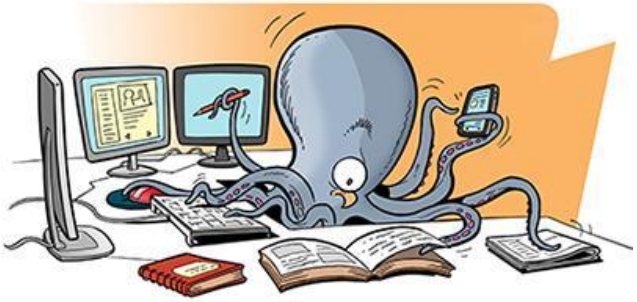
SeguraNet

5 dicas para recolheres informação na net

indica sempre as **fontes consultadas**, na Bibliografia

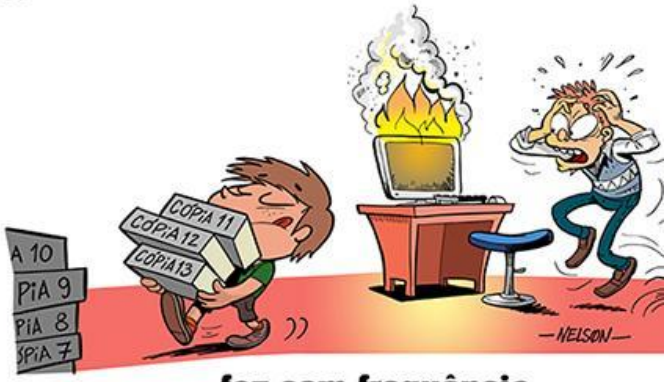
Bibliografia: SOARES, Bernardo - 1986. Livro do Desassossego. Mem Martins: Europa-América. Vol II

usa as tuas próprias palavras e, quando usas palavras de outros autores, coloca essa **informação entre aspas** e **cita os autores**



usa sempre **diversas fontes** de informação

compara as informações que recolhes e seleciona as fontes mais credíveis



faz com frequência **cópias de segurança**

www.seguranet.pt

REPÚBLICA PORTUGUESA | EDUCAÇÃO | direção-geral educação | internet segura.pt | ins@fe | Co-financiado pela União Europeia O Mecanismo Interligar a Europa

Seguranet

Segurança na Internet: uma aprendizagem para o presente (2014)

Dissertação de Mestrado Integrado de Tânia Margarida Ferreira: "A segurança na Internet constitui-se atualmente como um tópico de amplo debate. Por um lado pretende-se que crianças e jovens utilizem os recursos disponibilizados na Internet como oportunidades, por outro lado colocam-se as questões: "A que perigos se expõem? Como navegam? Fazem-no de forma segura e responsável?". Tendo como ponto de partida os objetivos: 1) Compreender a forma como os alunos encaram a segurança na Internet; 2) Incentivar os alunos a debater a problemática da segurança na Internet; e 3) Fomentar o enraizamento de comportamentos responsáveis na utilização da Internet; este relatório apresenta um estudo sobre a referida problemática. O estudo foi implementado numa turma de 22 alunos, do 8º ano do ensino básico, na disciplina de Tecnologias de Informação e Comunicação".

Disponível on-line »

Preventive measures – how youngsters avoid online risks (2014)

Documento da EU Kids Online: "To protect children from online risks, it is important to recognize that children's perceptions of online problematic situations may greatly differ from those of adults. What adults perceive as problematic does not necessarily result in a negative or harmful experience for children.

This report shows that children's perceptions of online risks strongly depend on their awareness of how online activities may turn into problematic or harmful situations. Also important is their knowledge of effective preventive measures, since it appears that when children feel capable of dealing with a risk they are less fearful or worried by it. Children expressed a range of concerns about online problems that sometime bother or upset them. The salient risks in children's eyes are online bullying and harassment, unwelcome contact from strangers, misuse of personal information, issues related to sexual content or communication, and commercial content.

Looking at the media platforms where these incidents occur, about half of unpleasant online experiences happen on social networking sites such as Facebook. While children acknowledge the potential risks of social networking sites, they do not necessarily do something to avoid the risk. However, when they do feel capable of dealing with the risk, they are less fearful or worried about it.

These new findings result from the qualitative analysis of 57 focus groups and 113 personal interviews with children aged 9 to 16. In total, 349 children from nine different European countries (Belgium, Czech Republic, Greece, Italy, Malta, Portugal, Romania, Spain, and UK) were invited to explain what they perceive as problematic or harmful online, and what they do to prevent harm from occurring".

Disponível on-line »

Crianças e meios digitais móveis em Portugal: resultados nacionais do Projeto Net Children Go Mobile (2014)

Publicação da autoria de Cristina Ponte *[et al.]*: "As crianças e jovens estudados na presente investigação, entre os 9 e 16 anos, estão a crescer num mundo onde a distinção entre internet fixa e móvel se esbate tanto pelo acesso ubíquo através de wifi e cobertura 3G/4G, como pela disponibilidade de equipamentos convergentes, como os smartphones, os tablets, os portáteis e as consolas de jogos.

Estas tecnologias e as suas práticas sociais de uso estão também sujeitas a contínua mudança. A internet, cada vez mais pelos meios móveis, proporciona oportunidades significativas para a sociabilidade, expressão pessoal, aprendizagem, criatividade e participação. Contudo, encaradas numa perspetiva do "risco", essas mesmas tecnologias, que igualmente proporcionam conetividade permanente, usos individualizados e características multimédia, parecem apresentar menos vantagens.

Desde 2006, a rede EU Kids Online tem investigado oportunidades e riscos online de crianças e jovens, mostrando a sua interdependência: quanto mais as crianças usam a internet, não só é maior o leque de oportunidades a que têm acesso, como também é maior a sua exposição a riscos online. Um momento importante foi constituído pelo inquérito europeu, que envolveu 25 países entre os quais Portugal, em 2010.

(…)

A participação de Portugal no presente inquérito do projeto Net Children Go Mobile, que envolveu outros seis países europeus (Bélgica, Dinamarca, Irlanda, Itália, Reino Unido e Roménia), foi possível pelo financiamento da Fundação para a Ciência e a Tecnologia. Essa participação constitui um importante contributo para o conhecimento do contexto nacional em que se desenvolve esse novo ambiente digital, numa perspetiva comparada com outros países e com a situação de há quatro anos.

Neste relatório apresentam-se os resultados sobre Portugal, comparando-os com os resultados de outros países do projeto Net Children Go Mobile e, sempre que possível, fazendo referência aos dados de 2010 do inquérito EU Kids Online". pp. 43-44

Disponível on-line »

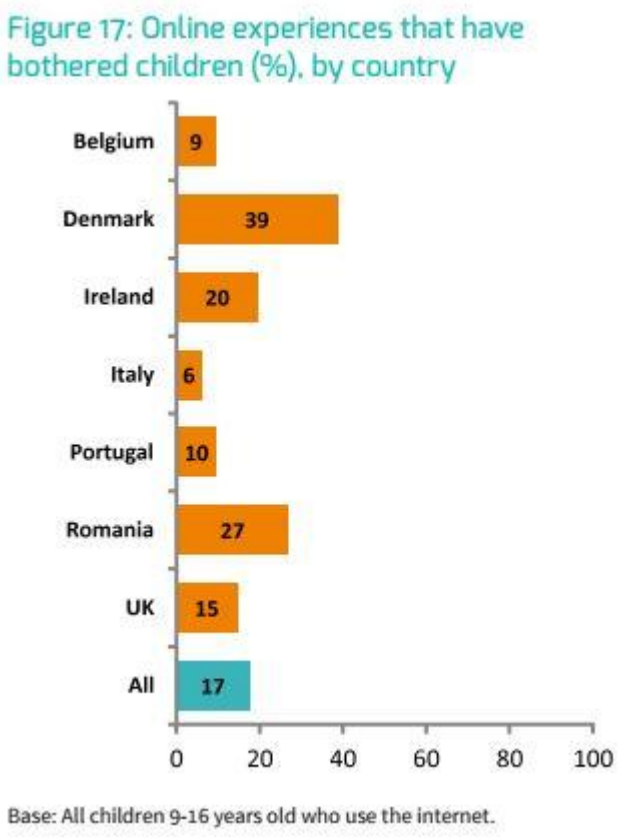
Apresentação sobre as temáticas da segurança digital (2014)

Recurso da Seguranet. Disponível on-line »

International Telecommunication Union

Net Children Go Mobile final report (with country fact sheets) – November (2014)

Relatório de Giovanna Mascheroni & Andrea Cuman. Contém dados sobre Portugal.
Disponível on-line »



NCGM Final Report 2014 - Gráfico pág .24

The Web We Want/ A rede que queremos (2013)

Documento criado pela European Schoolnet em colaboração com a rede Insafe, com o apoio da Liberty Global e da Google: "A Internet que queremos é uma brochura educativa, destinada a jovens entre os 13 e os 16 anos, que apresenta um conjunto de ferramentas que educa os adolescentes a saberem proteger-se quando estão online.

Este recurso, tão necessário a professores, jovens e pais, foi criado com a participação ativa de adolescentes de toda a Europa, aprovado pela Comissão Europeia e traduzido para português".

Disponível on-line »

Lembra-te:

- Verifica regularmente as tuas definições de privacidade nos *sites* das redes sociais e atualiza-as sempre que necessário
- Utiliza *sites* seguros sempre que possível, por exemplo, https, porque as informações enviadas para estes *sites* são encriptadas.
- Se não tiveres tempo de ler todos os termos e condições quando te registas num *site* novo, pensa se uma ferramenta nova como o **EULAlyzer** pode ajudar.
- Todos somos responsáveis por denunciar conteúdos irregulares que encontramos *online*. Quanto mais o fizermos, maior será o nosso contributo para tornar a Internet um lugar melhor para todos.
- De vez em quando, convém procurar o teu nome (ou programar um alerta do Google para isso) para perceberes melhor o que os outros vão encontrar se te procurarem *online*.
- Embora nem sempre seja fácil, convém ***pensar antes de publicar um post!***

European Schoolnet, 2013

Safebook (2013)

Cartaz traduzido pelo Projecto MiudosSegurosNa.Net. Disponível on-line »

Estás à procura de informações ou conselhos?
Contacta a Rede Insafe do teu país.

Alemanha	www.klicksafe.de	Islândia	www.saft.is
Áustria	www.saferinternet.at	Itália	www.generazioniconnesse.it
Bélgica	www.clicksafe.be	Letónia	www.drossinternets.lv
Bulgária	www.safenet.bg	Lituânia	www.draugiskasinternetas.lt
Chipre	www.cyberethics.info	Luxemburgo	www.bee-secure.lu
Dinamarca	www.medieraadet.dk	Malta	www.besmartonline.org.mt
Eslováquia	www.zodpovedne.sk	Noruega	www.medietilsynet.no
Eslovénia	www.safe.si	Países Baixos	www.digibewust.nl
Espanha	www.protegeles.com	Polónia	www.saferinternet.pl
Estónia	www.targaltinternetis.ee	Portugal	www.internetsegura.pt
Finlândia	www.meku.fi/fisic/	Reino Unido	www.saferinternet.org.uk
França	www.internetsanscrainte.fr	República Checa	www.saferinternet.cz
Grécia	www.saferinternet.gr	Roménia	www.sigur.info
Hungria	www.saferinternet.hu	Rússia	www.nedopusti.ru
Irlanda	www.webwise.ie	Suécia	www.medieradet.se

European Schoolnet, 2013

Programar para prevenir: o uso do Scratch aplicado à segurança na Internet (2013)

Dissertação de Mestrado Integrado de Ana João Lopes: "O ambiente de programação Scratch, criado pelo MIT em 2007, permite criar facilmente histórias interativas, animações, jogos, música e arte e partilhar essas criações na web. Este relatório apresenta o projeto de intervenção pedagógica supervisionada, com uma componente investigativa, que envolveu a utilização do Scratch, como estratégia para promover o desenvolvimento de competências e estruturar conhecimentos relativos à Segurança na Internet. O uso das tecnologias de informação e comunicação, nomeadamente a Web, está generalizado e massificado, na chamada Sociedade de Informação, tornando-se, por isso, cada vez mais importante dotar os alunos de competências para usufruírem desses ambientes de uma forma mais consciente dos riscos, ou seja, mais responsável e segura. O estudo foi implementado numa turma do nono ano do ensino básico, na disciplina de Introdução às Tecnologias de Informação e Comunicação e decorreu ao longo de sete sessões de noventa minutos. Os vinte e sete alunos da turma desenvolveram no Scratch, em grupos de três ou quatro elementos, uma aplicação que consistia num teste de escolha múltipla interativo (quiz) sobre um dos seguintes subtemas do tópico programático Segurança na Internet: segurança nos telemóveis; cyberbullying; phishing; proteção dos dados pessoais; segurança nas redes sociais; segurança no email; segurança nos chats".

Disponível on-line »

Potenciar o uso da Internet no ensino aprendizagem das TIC promovendo comportamentos seguros (2013)

Dissertação de Mestrado Integrado de Fátima Esteves: "As crianças e os adolescentes, em particular, estão cada vez mais expostos aos riscos online, que resultam, regra geral, do seu desconhecimento e da sua ingenuidade. Neste contexto, é imprescindível que estes adquiram uma literacia digital que ultrapasse as competências de uso técnico e inclua dimensões associadas à adoção de comportamentos adequados no ciberespaço, nomeadamente no sentido de evitarem práticas potencialmente perigosas, de diversa natureza. É nesta sequência que foi desenvolvido o projeto, que deu origem ao presente relatório.

Disponível on-line »

What Children Do Online (2013)

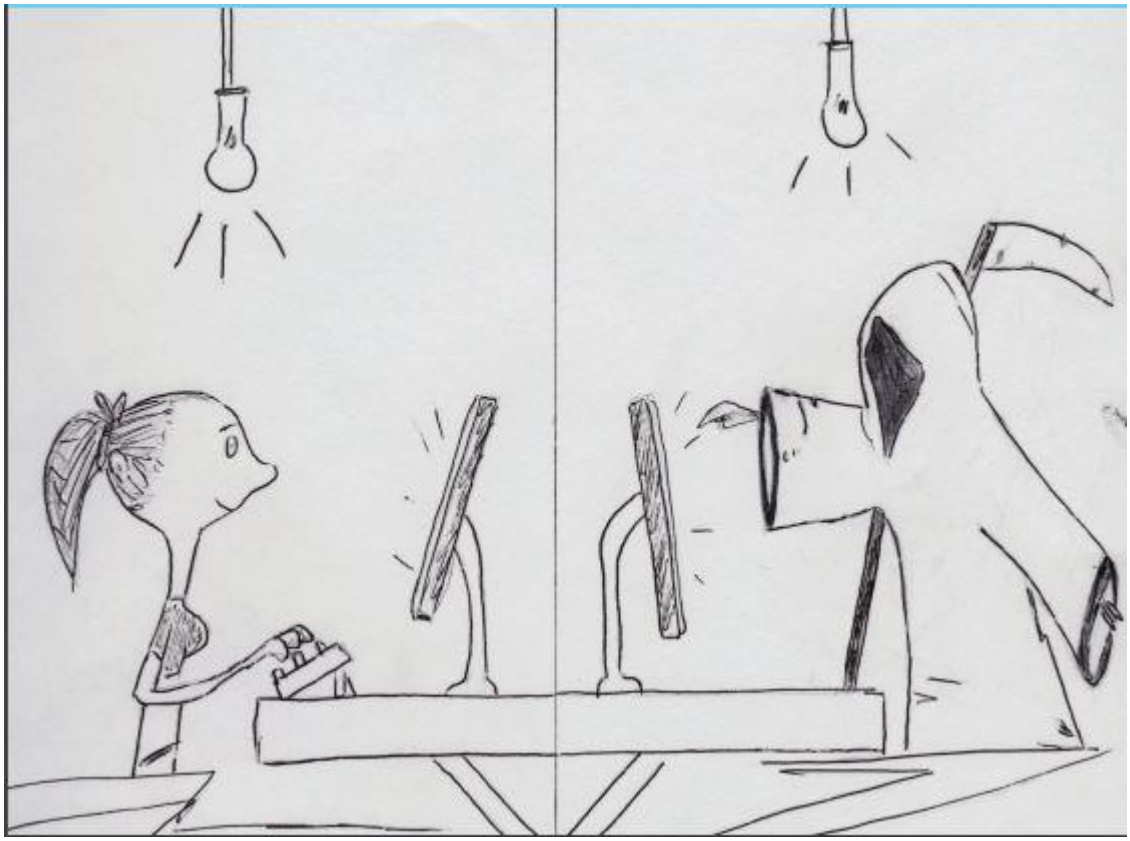
Infografia da Eu Kids Online. Disponível on-line »

Eu Kids Online, 2013

Tu e Internet: (ab)uso, crime e denúncia (2013)

Brochura da responsabilidade do Gabinete Cibercrime da Procuradoria-Geral da República.

Disponível on-line »



Seguranet, 2013

Carta dos Direitos das Crianças na Internet (2012)

Recurso da Campanha Back2school da Insafe. Disponível on-line »

Carta dos Direitos das Crianças na Internet

Todos os direitos mencionados abaixo são baseados num artigo da CDC (Convenção das Nações Unidas sobre os Direitos da Criança – consultar www.unicef.org/crc/).

Depois de as crianças terem formulado e desenvolvido a sua própria carta de direitos na Internet, estes direitos podem ser comparados com os da Carta dos Direitos das Crianças na Internet das Crianças, como forma de lançar a reflexão e o debate.

1. Tens o direito de proteger a tua identidade quando estiveres ligado.

2. Tens o direito de não revelar pormenores pessoais se não souberes ou não tiveres a certeza de quem está do outro lado.

3. Tens o direito de participar, de te divertires e de procurar toda a informação disponível que seja adequada à tua idade e personalidade.

4. Tens o direito de te expressares livremente quando estás ligado, desde que respeites sempre os outros.

5. Tens o direito de ser ouvido e de ser tratado com respeito.

6. Tens o direito de proteger qualquer coisa que tenhas criado, não importa onde, até mesmo na internet.

7. Tens o direito de ser crítico e debater tudo o que leste ou encontraste na Internet.

8. Tens o direito de utilizar as novas tecnologias para desenvolver a tua personalidade e melhorar as tuas capacidades.

9. Tens o direito de te proteger de vírus e de lixo eletrónico (spam).

INSAFE, 2012

CONNECTED DOT COM: Young people's navigation of online risks (2012)

Estudo conjunto do Centre for Justice and Crime Prevention (CJCP) e UNICEF South Africa: "The opportunities presented by widespread access to, and use of, ICTs (Information and Communication Technologies), are balanced by a number of new risks and dangers that present online. The extent of these risks and dangers, and the way in which young people respond to and deal with them, is largely unknown, at least within the South African context. With this in mind, the Centre for Justice and Crime Prevention (CJCP), in partnership with UNICEF South Africa, undertook a study, aimed at exploring young people's online experience, as part of a larger national research study on school violence. This new study was designed to explore young people's use of social media, the dangers faced online, and the ways in which young people negotiate their own safety online".

Disponível on-line »

Criança e (in)segurança na internet: estudo de caso no 3º ciclo do ensino básico (2012)

Tese de Mestrado de Cátia Cepeda: "Na época em que estamos inseridos é inevitável falar em tecnologia e associado a este conceito vem certamente anexada a internet. Vivemos numa sociedade em constante mutação e por isso temos que acompanhar as diversas realidades que estão perante nós. As escolas não podem fugir a esta realidade, embora por vezes seja um pouco complicado acompanharem. No entanto, não podemos esquecer que a escola e a família são os dois alicerces da educação de uma criança, logo estas duas "instituições" deverão estar em sintonia. O presente projeto teve como objetivo estudar e compreender o uso que as crianças fazem da internet. Nesse sentido, foi realizado um estudo de caso que incidiu sobre os alunos do terceiro ciclo da Escola Secundária Emídio Garcia, na cidade de Bragança. Com o estudo em curso, pretende-se verificar, aprofundar e sobretudo estudar e perceber de que modo as crianças utilizam a internet em ambiente familiar. Além disso, pretende-se também verificar se é usada em segurança ou não. Hoje em dia vemos cada vez mais crianças a brincar, comunicar e relacionar-se com outras pessoas através das potencialidades existentes na internet. Será que ao utilizarem a internet, as crianças estão conscientes dos perigos existentes na mesma? Será que utilizam a internet em segurança? Será que são conhecedoras e detentoras de todo o vocabulário inerente a esta tecnologia? Além disso, o nosso estudo pretende também verificar as mesmas situações no ambiente escolar, pois é neste ambiente que elas passam a maior parte do seu dia. Será que esta instituição está atenta a todos os perigos que existem? Será que faz algum tipo de prevenção? Para a recolha de dados utilizou-se como instrumento um questionário. Em jeito de conclusão e cientes das limitações tecnológicas decorrentes de alguns equipamentos que apetrecham as escolas, da inadequada formação de alguns docentes e até mesmo de alguns pais, acreditamos que a utilização da internet por parte das crianças de modo seguro e controlado seja, ainda hoje, um tema de grande discussão e com bastantes lacunas".

Disponível on-line »

A exploração sexual de crianças no Ciberespaço - aquisição e valoração de prova forense de natureza digital (2012)

Tese de Mestrado de Manuel Magriço: "A exploração sexual de crianças no Ciberespaço constitui presentemente um problema mundial: o desenvolvimento de novas tecnologias que aumentam as formas de acesso ao mundo virtual tem contribuído para a crescente divulgação de material de abuso sexual. Existindo constrangimentos na identificação de vítimas, agressores e locais da prática da violência sexual contra as crianças no Ciberespaço, impõem-se novas metodologias por parte investigação criminal na repressão do fenómeno. O aprofundamento da Cooperação Judiciária Penal Internacional, o reporte de conteúdos por parte de empresas e instituições cuja atividade esteja relacionada com o Ciberespaço às Autoridades de IC, designadamente por parte dos Internet Service Provider, uma análise centralizada da informação, a difusão de boas práticas, a formação especializada dos diversos operadores judiciários sobre os procedimentos relativos à aquisição, valoração e manutenção da cadeia de custódia da prova digital, o apoio pericial técnico e especializado junto do Ministério Público de peritos informáticos forenses, a que se deve aliar o desenvolvimento de ações de prevenção criminal encobertas em linha e a consciencialização pública dos perigos, constituem fatores estruturantes na prevenção e repressão do fenómeno, tendentes a garantir maior segurança às crianças".

Disponível on-line »

Livro da Cartilha de Segurança para Internet (2012)

Da autoria do Centro de Estudos, Resposta e Tratamento de Incidentes de Segurança no Brasil: "A Cartilha de Segurança para Internet e um documento com recomendações e dicas sobre como o usuário de Internet deve se comportar para aumentar a sua segurança e se proteger de possíveis ameaças. O documento apresenta o significado de diversos termos e conceitos utilizados na Internet, aborda os riscos de uso desta tecnologia e fornece uma série de dicas e cuidados a serem tomados pelos usuários para se protegerem destas ameaças".

Disponível on-line »

Joga e aprende: estar online (2011)

Livro de atividades para crianças, da Internet Segura e da rede Insafe: "Hoje em dia, as crianças têm acesso à Internet cada vez mais cedo. Por essa razão, este livro visa introduzir conceitos ligados às novas tecnologias no seu vocabulário e atividades quotidianas.
Ao mesmo tempo que oferece às crianças entre os 4 e os 8 anos de idade 30 páginas de jogos e diversão, este livro de atividades ajuda-as também a enriquecer as suas competências básicas a nível linguístico, matemático, social e cultural. Permite-lhes ter uma visão do impacto que as novas tecnologias podem ter na sua vida quotidiana. Acima de tudo, proporciona a pais e professores uma oportunidade de se sentarem à mesma mesa com as crianças e discutirem estes assuntos importantes.
Embora o livro de atividades tenha sido criado de forma que as crianças mais pequenas possam divertir-se e jogar sozinhas, muitos dos exercícios têm subjacente um nível mais profundo. O folheto visa incentivar pais e professores a falarem de temas como a privacidade e as novas tecnologias com os seus fi lhos e alunos, logo a partir de tenra idade, uma vez que estas questões já desempenham um papel indubitavelmente importante nas suas vidas". (p. 2)

Disponível on-line »

A integração das TIC no Ensino Básico: a segurança online (2011)

Dissertação de Mestrado de Maria Elisabete Pires: "Constata-se que as escolas do Ensino Básico recorrem frequentemente ao uso das Tecnologias de Informação e Comunicação. Constata-se, também, que as crianças e jovens têm vindo a aumentar a utilização destas tecnologias, incluindo o acesso à Internet, em ambiente escolar e extraescolar, sem que exista um efetivo controlo nestes acessos. No presente trabalho procurou-se analisar as diversas vertentes envolvidas na questão da segurança online: as tecnologias, os recursos humanos e os processos envolvidos, junto das escolas do Ensino Básico".

Disponível on-line »

Geração digital: ouvindo as crianças falar de oportunidades e riscos online (2011)

Artigo de Ana Francisca Monteiro e António Osório: "A investigação sobre a utilização de tecnologias por crianças em Portugal aponta para uma crescente autonomização e individualização do uso da internet. A pesquisa nota ainda existir um desfasamento entre o discurso dos pais e dos filhos quanto às experiências online dos mais novos, designadamente no que diz respeito às experiências de risco. Evidências desta natureza realçam a importância de apostar em estratégias de intervenção e investigação centradas na perspetiva das próprias crianças. No âmbito da promoção de uma vivência online saudável, importa integrar a agenda de oportunidades, riscos e segurança que, na ótica das próprias crianças, orienta a sua relação com os media, designadamente a Internet. Neste texto apresentam-se resultados de uma investigação qualitativa em curso, na qual participaram 16 crianças entre 10 e 12 anos".

Disponível on-line »

SimSafety - Simulador de navegação para a segurança na Internet: analisando a implementação de um projeto europeu em quatro escolas do norte de Portugal (2011)

Artigo de Teresa Castro *[et al.]*: ""SimSafety: simulador de navegação para a segurança na Internet" é um projeto cofinanciado pela União Europeia, direcionado para pais, professores e alunos que, através de uma abordagem de colaboração entre adultos e crianças, promove a literacia para uma utilização saudável e responsável da Internet. O Instituto de Educação da Universidade do Minho liderou o projeto em Portugal, implementando-o em quatro escolas do norte do país. Este texto tem como objetivo descrever, de modo sucinto, o estudo da implementação do projeto em Portugal: iniciativas, estratégias, metodologias e resultados aferidos ao longo de um ano de sessões experimentais de aprendizagem, em ambiente simulado, que envolveram adultos e crianças, numa relação dinâmica do conhecimento, pelo objetivo comum de aproximar imigrantes e nativos digitais".

Disponível on-line »

Seguranet


SeguraNet
5 dicas
para estares bem na net
respeita os outros
pensa antes de publicares
TELEFONES MORADAS ETC...
TUDO SOBRE
não partilhes tudo
FACEBOOK
BLOGS
EMAIL
atenção à tua pegada digital
—NELSON—
denuncia situações de ciberbullying
www.seguranet.pt
REPÚBLICA PORTUGUESA
EDUCAÇÃO
direção-geral educação
internet segura.pt
ins@fe
Co-financiado pela União Europeia
O Mecanismo Interligar a Europa

Seguranet

Riscos de utilização das TIC (2011)

Artigo de Paula Maria Ferreira: "Na atualidade, as Tecnologias de Informação e Comunicação (TIC) fazem parte da vida das crianças e dos jovens. No entanto, estes utilizam-nas frequentemente sem consciência dos seus riscos e oportunidades. O uso descuidado e exagerado de tecnologias, como o telemóvel ou a Internet, podem pôr em causa a sua segurança e prejudicar a sua integridade física e psicológica. Cabe à escola, aos pais e à sociedade em geral sensibilizar os mais novos para os perigos e conduzi-los numa utilização mais segura das TIC. Neste sentido, é nosso objetivo refletir sobre alguns destes riscos tentando conjugar opiniões de especialistas com notícias do dia-a-dia".

Disponível on-line »

A participação das escolas portuguesas no Projeto Seguranet. Estudo múltiplo de casos (2011)

Publicação de J.L.P. Ramos: "Este resumo corresponde ao estudo de avaliação no que diz respeito à participação das escolas portuguesas no projeto SeguraNet. Este projeto é dinamizado por várias entidades em Portugal, entre estas o Ministério da Educação e Ciência. O estudo envolveu 10 escolas em todo o território continental de Portugal. Envolveu em média 6 professores de cada escola e uma amostra representativa dos alunos. Os alunos, que no total das escolas são 1155, têm na sua maioria entre 11 e 14 anos. O estudo referido é constituído por duas partes distintas mas complementares: uma primeira parte que corresponde ao estudo sobre o conjunto das escolas, professores e alunos participantes nesta avaliação e uma segunda que diz respeito aos estudos de caso realizados. Este estudo revela o papel vital da escola no contexto do problema da utilização segura da Internet por crianças e jovens. Nas escolas que estiveram em observação os professores revelaram sobretudo preocupação com estes assuntos e muitos passaram aos atos, promovendo a utilização segura das tecnologias, com o conhecimento e os meios de que dispõem, tendo aqui o projeto Seguranet desempenhado uma importante função de informação e suporte às escolas e aos professores. O reforço do papel da escola nas estratégias de apoio a crianças e jovens no domínio da segurança na Internet, através de ações diretas e ou mediadas pelos professores e pelas famílias, parece ser a linha de trabalho que emerge deste estudo e que deve, considerando os resultados obtidos, ser aprofundada no futuro".

Disponível on-line »

International Telecommunication Union

Risks and safety on the internet: the perspective of European children. Full findings and policy implications from the *EU Kids Online* survey of 9-16 year olds and their parents in 25 countries (2011)

Publicação da autoria de Sonia Livingstone *[et al.]*: "This report presents the full findings from a new and unique survey designed and conducted according to rigorous standards by the EU Kids Online network. It was funded by the European Commissions' Safer Internet Programme in order to strengthen the evidence base for policies regarding online safety.

- A random stratified sample of 25,142 children aged 9-16 who use the internet, plus one of their parents, was interviewed during Spring/Summer 2010 in 25 European countries.
- The survey investigated key online risks: pornography, bullying, receiving sexual messages, contact with people not known face-to-face, offline meetings with online contacts, potentially harmful user-generated content and personal data misuse.
- In this report, 'children' refers to internet using children aged 9-16 across Europe. 'Using the internet' includes any devices by which children go online and any places in which they go online". (p. 5)

Disponível on-line »

Navegação segura na Internet – riscos e desafios (2010)

Artigo de Carina Pires, Cristina Novo e Joana Gomes: "O avanço tecnológico e a utilização massiva das Tecnologias de Informação e Comunicação (TIC) têm transformado a forma de viver de cada indivíduo nas sociedades atuais, a uma velocidade incomparável no passado. Deste modo não é difícil reconhecer que, o uso das TIC fizeram emergir benefícios a nível da distribuição da Informação, da velocidade de comunicação interpessoal, da aquisição de conhecimentos, do desenvolvimento de relações pessoais, entre outros aspetos das vidas de crianças, jovens e adultos do século XXI.

No âmbito da disciplina Comunicação Educacional e Meios e Materiais de Ensino (CEMME), lecionada no curso de licenciatura em Educação de Infância, da Escola Superior de Educação de Santarém (ESES), surgiu a oportunidade de realização de um projeto que teve como principal objetivo a sensibilização de pais, educadores de infância e alunos do ensino superior, sobre os perigos a que estamos sujeitos na utilização das TIC em geral e da Internet em particular, promovendo momentos de reflexão conjunta relativamente a boas práticas a adotar.

Deste trabalho, fica a convicção de que muito caminho ainda há para percorrer na formação de professores e educadores, no que toca à forma como usam a rede Internet e como cuidam dos computadores de que são utilizadores, já que os jovens que frequentam a formação de nível 1 (1º ciclo de Bolonha) são assíduos utilizadores das TIC, mas revelam lacunas no que toca à exposição a que se sujeitam na rede. De igual forma, têm alguma dificuldade em respeitar e cuidar da segurança pessoal e dos seus computadores, muito embora a amostra com que trabalhámos tenha tentado passar uma imagem diferente, mais informada e esclarecida do que aquilo que verificámos na realidade dos workshops e nas reflexões que deles resultaram".

Disponível on-line »

SeguraNet

5 dicas para continuares seguro na net

cuidado com o que **instalas**

usa **pseudónimos** ***(nicknames)***

tem cuidado com as tuas ***passwords***

atenção às **fotos e vídeos que publicas**

torna as tuas **contas seguras e encerra sempre as sessões**

www.seguranet.pt

REPÚBLICA PORTUGUESA | EDUCAÇÃO | direção-geral educação | internet segura.pt | ins@fe | Co-financiado pela União Europeia O Mecanismo Interligar a Europa

Seguranet

Proteção da privacidade de menores na internet: responsabilidade parental (2008)

Dissertação de Mestrado de Jorge Manuel Costa: "A privacidade é algo de que toda a gente fala, e quer proteger. Há um sentimento generalizado de que essa privacidade é algo de valioso, pessoal, que merece atenção e proteção na medida em que as ameaças à privacidade pessoal podem ser consideradas ameaças à segurança individual. Essas ameaças são particularmente graves quando se manifestam sobre as crianças. Com a Internet a permitir a comunicação com virtualmente qualquer outra pessoa no planeta que tenha acesso ao mesmo recurso, a sua utilização por parte de menores possibilita depararem-se com pessoas que coloquem a sua segurança em risco. Qual a melhor forma de proteger um menor das ameaças à segurança por parte de um estranho na Internet? A quem cabe educar, ou formar, no sentido de evitar esses encontros na Internet ou, no caso de isso acontecer, de evitar que o menor seja identificável – isto é, mantendo a informação relativa a si e à sua família no desconhecimento de terceiros – evitando assim que o encontro "virtual" possa vir a permitir um encontro "real"? A quem cabe a responsabilidade pelo comportamento do menor na Internet?"

Disponível on-line »

Declaration of the Committee of Ministers on protecting the dignity, security and privacy of children on the Internet (2008)

Documento do Conselho da Europa. Disponível on-line »

Tiras BD SeguraNet (s.d.)

Tiras de banda desenhada da responsabilidade da SeguraNet. Disponível on-line »

Tiras BD SeguraNet

Cyberbullying

Mais recursos da SeguraNet (cartazes, vídeos, brochuras, etc.) (s.d.)

Disponível on-line »

Internet Addiction Test (IAT) (s.d.)

Ferramenta em site para medir o grau de dependência em relação à Internet, da responsabilidade da autoria de Dr. Kimberly Young do Center for Internet Addiction: "The Internet Addiction Test (IAT) is the first Validated measure of Internet Addiction described in the **IAT Manual** to measure Internet use in terms of mild, moderate, to several levels of addiction".

Disponível on-line »

Indicações para a utilização segura dos dispositivos móveis (s.d.)

Folheto da SeguraNet sobre segurança nos dispositivos móveis. Disponível on-line »

Seguranet

Checklist sobre Segurança no Computador (s.d.)

Documento da SeguraNet. Disponível on-line »

Guia de Facebook para os Jovens (s.d.)

Folheto que ajuda a utilizar corretamente o Facebook, da SeguraNet. Disponível on-line »

Seguranet

Pensa em como te podes proteger online (s.d.)

Folheto da responsabilidade da Insafe e da INHOPE, com o apoio da Comissão Europeia.

Disponível on-line »

Pensa nos conteúdos que publicas! (s.d.)

Folheto da responsabilidade da Insafe e da INHOPE, com o apoio da Comissão Europeia.

Disponível on-line »

Educar a los menores en el uso sin riesgos de Internet: guía para madres y padres (s.d)

Documento editado pelo Ayuntamiento de Vitoria-Gasteiz.

Disponível on-line »

Pensa na tua lista de contactos online! (s.d.)

Folheto da responsabilidade da Insafe e da INHOPE, com o apoio da Comissão Europeia.

Disponível on-line »

Sextortion: Be careful when flirting in front of a webcam! (s.d.)

Folheto da responsabilidade da Insafe e da INHOPE, com o apoio da Comissão Europeia.

Disponível on-line »

Vídeos no Youtube

Canal do Youtube Internet Segura - Histórias do Lucas

Esta série de animação criada pela produtora GO-TO em parceria com o IAC – Instituto de Apoio à Criança é dirigida a crianças entre os três e os oito anos e aborda temas como a cidadania, as questões sociais e culturais, entre outros – sempre ligados ao universo das crianças – tendo como inspiração a Declaração Universal dos Direitos das Crianças. Em cada episódio as personagens da série dão a conhecer estes temas sempre num tom divertido.

Disponível on-line »

Dados estatísticos

Relatório Anual de Segurança Interna 2016 (2017)

Relatório do Sistema de Segurança Interna (páginas 31 a 33). Disponível on-line »

A influência dos estilos parentais na utilização da Internet por crianças e adolescentes (2016)

Tese de Mestrado de Sandra Mendonça: "O presente estudo tem por objetivo compreender de que forma os estilos parentais influenciam a utilização da Internet por crianças e adolescentes. Por sua vez, pretende-se perceber como as famílias de baixo contexto socioeconómico e condição de imigrante acompanham e medeiam a utilização da Internet pelos filhos. A amostra utilizada envolveu 119 crianças e adolescentes e respetivo pai ou mãe. Os dados foram recolhidos mediante a aplicação de um questionário construído para o efeito. De acordo com os resultados, a utilização da internet é elevada entre as crianças e adolescentes, verificando-se o mesmo nos pais. A casa é o local de maior acesso e o recurso mais utilizado é o telemóvel. Os pais revelam-se mais confiantes na utilização da internet, comparativamente aos filhos. O estilo autoritativo na utilização da internet é o mais evidente entre os pais em estudo. Quanto às estratégias de mediação parental, todas evidenciam uma correlação positiva com os estilos parentais. A mediação ativa da segurança é a mais utilizada entre os pais em estudo, sendo que falar com a criança/adolescente sobre o que faz na internet e nas redes sociais são as práticas mais realizadas. Em relação aos riscos, a sua expressão entre as crianças e adolescentes em estudo é relativamente baixa, não se verificando diferenças a nível de sexo. Face aos estilos parentais, estes não parecem ter influência na redução dos riscos. Contrariamente às pesquisas de Valcke *[et al.]* (2010) os que estilos parentais não parecem influenciar significativamente a utilização da internet pelas crianças e adolescentes".

Estatísticas nas páginas 7 a 14.

Disponível on-line »

International Telecommunication Union

"Nos últimos anos, o uso da Internet por crianças e adolescentes tem-se tornado uma prática bastante comum (Johnson, 2010), pelo que o seu contacto com a internet ocorre cada vez mais cedo, a partir dos 5 anos de idade (…). Pesquisas realizadas em países desenvolvidos indicam um elevado uso da internet em casa pelas crianças, cerca de 92% (…). Estudos desenvolvidos a nível da Europa indicam que 60% das crianças e adolescentes entre os 9 e os 16 utilizam diariamente a internet e cerca de 33% pelo menos semanalmente (…). Este fato explica, de certa forma, a elevada confiança digital evidenciada pelas crianças (92%) em comparação com os seus pais (62%), e a difícil tarefa destes em acompanhá-las, de forma a assegurar uma utilização segura da internet pelos filhos (Livingstone 2007). Segundo o estudo EU Kids (2014), 36% das crianças e adolescentes entre os 9 e 16 anos afirmam ter mais conhecimentos acerca da Internet do que os seus pais. Apesar da baixa competência e confiança digital evidenciadas pelas crianças mais pequenas, a maioria, entre os 11 e os 16 consegue bloquear mensagens de pessoas indesejáveis (64%), encontrar conselhos de segurança online (64%), alterar as configurações de privacidade no seu perfil das redes sociais (56%), comparar sites e avaliar a sua qualidade (56%) e bloquear o spam (51%) (EU Kids Online, 2014).

(…)

Em Portugal o uso da internet pelas crianças ocorre, em média, a partir dos 9 anos de idade. O acesso é feito sobretudo em casa, com os rapazes a evidenciar um maior uso (80%) comparativamente às raparigas (68%). Fora de casa, nomeadamente na escola, os papéis invertem-se, com as raparigas a liderar o uso da internet (25%), face aos rapazes (12%) (Net Children Go Mobile, 2014). O acesso à internet é feito sobretudo através do computador portátil (60%), colocando Portugal na segunda posição entre os países em estudo (Net Children Go Mobile, 2014). O telemóvel surge a seguir (35%), sendo mais utilizado pelas raparigas, de acordo com o mesmo estudo. Relativamente à idade, os adolescentes entre os 13 e 16 anos evidenciam um maior uso da internet, quer em casa ou na escola, em comparação com as crianças entre os 9 e 12 anos (Net Children Go Mobile, 2014). Em relação aos pais, cerca de 68% usa a Internet, situando-se abaixo da média europeia (85%). No que concerne às atividades, as mais realizadas são: ouvir música (52%), ver vídeo clips e estar nas redes sociais (50%) e trocar mensagens instantâneas (47%). À exceção das redes sociais, liderada pelas raparigas entre os 13 e 16 anos (71%), os rapazes evidenciam percentagens superiores nas restantes atividades. A realização de jogos sozinho ou contra o computador surge com a quarta atividade mais mencionada, sendo liderada pelos rapazes entre os 9 e 12 anos (Net Children Go Mobile, 2014)".

MENDONÇA, 2016: 8-9

"As crianças e adolescentes estão cada vez mais presentes no mundo virtual, sobretudo nas redes sociais, na medida em que acedem cada vez mais à internet e em idades mais precoces. O projeto Eu Kids Online afirma que, em 2010, 24% das crianças entre os 9-12 anos tinha um perfil numa rede social e 58% dos adolescentes entre os 13-16 anos. Em 2014 verificou-se um aumento dos valores, passando a 38% para as crianças entre os 9-12, e 81% para os adolescentes entre os 13-16 anos (Net Children Go Mobil, 2014). O Facebook destaca-se com a principal rede social usadas pelas crianças e adolescentes das diferentes idades, com uma percentagem de 61%.

(…)

No que respeita às crianças e adolescentes portuguesas, de acordo com o estudo Net Children Go Mobil (2014), 76% têm um perfil numa rede social, sendo o Facebook a rede mais utilizada pela esmagadora maioria das crianças em estudo (97%). Com o avançar da idade verifica-se um aumento significativo do uso de redes sociais, passando de 27% aos 9-10 anos para 80% aos 11-12 anos (Net Children Go Mobil, 2014). As restrições de idade impostas por algumas redes sociais (entre elas o Facebook) revelam-se ineficazes quando verificamos um crescimento significativo do uso das redes sociais por crianças com idade inferior a 13 anos. Relativamente às definições de privacidade, cerca de 44% das crianças e adolescentes com perfil em redes sociais afirma tê-lo privado, só disponível para os amigos, com maior percentagem por parte das raparigas (52%) e das crianças de 11-12 anos (61%). O perfil parcialmente privado é evidenciado por 27%, destacando-se novamente as raparigas (32%) e os adolescentes entre os 13-16 anos (35%). O perfil público é mencionado por 29%, com maior incidência nos rapazes (33%) e nos mais novos (39%). Quanto à informação disponibilizada no perfil das redes sociais, 83% disponibiliza o seu apelido, principalmente as raparigas entre os 13-16 anos (93%) e os rapazes entre os 9-12 anos (93%). A divulgação da morada apresenta valores pouco significativos (8%) sendo mais expressiva entre as raparigas dos 13-16 anos. O contacto telefónico é apresentado por 11%, sobretudo raparigas entre os 13-16 anos. Relativamente à escola e a uma idade que não é verdadeira, ambos são mencionados por 67% das crianças e adolescentes, sendo que, face à escola, são os adolescentes que mais a mencionam, sem grandes diferenças entre raparigas (67%) e rapazes (62%), enquanto a idade incorreta é evidenciado sobretudo por crianças entre os 9-12 anos, sendo 71% rapazes e 76% raparigas".

MENDONÇA, 2016: 11-12

"Em Portugal, no que concerne à exposição aos riscos, de acordo com as informações do estudo Net Children, Go Mobile (2014), apenas 10% das crianças e adolescentes reportaram sentir-se incomodados, por algo que tenha encontrado na internet, com maior incidência entre as raparigas, sobretudo as mais velhas (13-14 anos), e crianças de famílias de meios socioeconómicos baixos. Em relação aos tipos de risco encontrados, considerando o Bullying, uma em 10 crianças refere ter experienciado esta situação, sobretudo as raparigas (13%) tanto as mais novas (9-10 anos) como as adolescentes de idade intermédia (13-14 anos). Quanto às mensagens sexuais, também designado por Sexting, apenas 5% das crianças e adolescentes portugueses mencionaram ter experienciado esta situação, situando-se abaixo da média europeia (11%). Relativamente aos encontros com alguém que conheceram na internet, 11% das crianças e adolescentes portugueses revelaram ter tido esta experiência, com forte incidência entre os adolescentes acima dos 12 anos. Não se registam diferenças significativas a nível do género e estatuto socioeconómico. Estes valores situam-se abaixo da média europeia (26%). A nível da visualização de imagens sexuais, 27% das crianças e adolescentes portugueses declaram ter visto imagens sexuais nos últimos 12 meses, sobretudo os adolescentes entre 15-16 anos e crianças e adolescentes de baixo estatuto socioeconómico.

Relativamente à exposição a outros conteúdos inapropriados, nomeadamente distúrbios alimentares, conteúdos de incentivo à automutilação ou ao consumo de drogas, materiais que promovem discriminação e violência contra certos grupos 10% das crianças e adolescentes portugueses viram um ou mais destes tipos de conteúdos.

As percentagens mais elevadas são referentes a publicação de mensagens que atacam certos grupos (8%), conteúdos que falam sobre ou sugerem formas de automutilação (6%) e conteúdos que incentivam distúrbios alimentares (5%). Estes valores encontram-se abaixo da média europeia (20%, 11% e 13% respetivamente).

Foram ainda mencionados outros riscos, sendo os valores mais elevados referentes a vírus no computador (15%), uso indevido da sua password/telemóvel para aceder à informação do próprio ou para se passar por este (4%) e uso da sua informação pessoal de uma forma que não gostou (2%). No que respeita à forma como as crianças e adolescentes lidam com os riscos com os quais se deparam na internet, a procura de apoio junto dos pais é a situação mais mencionada, sendo a mãe mais solicitada (68%), em comparação ao pai (53%). Os irmãos (36%) e amigos (32%) surgem posteriormente".

MENDONÇA, 2016: 13-15

Enquadramento legal

Constituição da República Portuguesa

"Artigo 26.º
(Outros direitos pessoais)

1. A todos são reconhecidos os direitos à identidade pessoal, ao desenvolvimento da personalidade, à capacidade civil, à cidadania, ao bom nome e reputação, à imagem, à palavra, à reserva da intimidade da vida privada e familiar e à proteção legal contra quaisquer formas de discriminação".

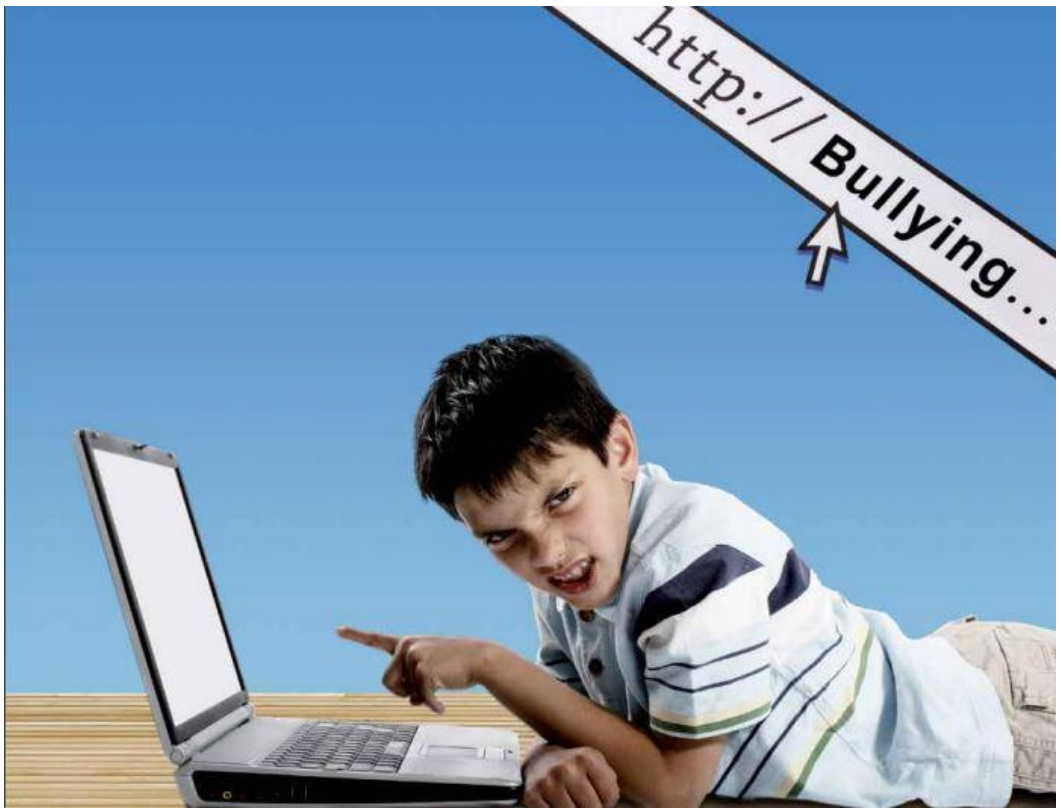
Disponível on-line »

Convenção de Lanzarote de 2007 (Convenção do Conselho da Europa para a Proteção das Crianças contra a Exploração Sexual e os Abusos)

"Artigo 23.º – Abordagem de crianças para fins sexuais

Cada Parte toma as necessárias medidas legislativas ou outras para qualificar como infração penal o facto de um adulto propor de forma dolosa, através de tecnologias de informação e comunicação, um encontro a uma criança que não tenha atingido a idade estabelecida em aplicação do n.º 2 do artigo 18.º, com a finalidade de cometer nesse encontro qualquer uma das infrações estabelecidas em conformidade com a alínea a) do n.º 1 do artigo 18.º ou com a alínea a) do n.º 1 do artigo 20.º, desde que essa proposta seja seguida de atos materiais que visem a tal encontro". (pp. 17-18)

Disponível on-line »



International Telecommunication Union

Código Penal

Artigo 153.º - Ameaça

1 - Quem ameaçar outra pessoa com a prática de crime contra a vida, a integridade física, a liberdade pessoal, a liberdade e autodeterminação sexual ou bens patrimoniais de considerável valor, de forma adequada a provocar-lhe medo ou inquietação ou a prejudicar a sua liberdade de determinação, é punido com pena de prisão até um ano ou com pena de multa até 120 dias.

Artigo 154.º - Coação

1 - Quem, por meio de violência ou de ameaça com mal importante, constranger outra pessoa a uma ação ou omissão, ou a suportar uma atividade, é punido com pena de prisão até três anos ou com pena de multa.

Artigo 171.º - Abuso sexual de crianças

1 - Quem praticar ato sexual de relevo com ou em menor de 14 anos, ou o levar a praticá-lo com outra pessoa, é punido com pena de prisão de um a oito anos. (…)
3 - Quem: (…)
b) Atuar sobre menor de 14 anos, por meio de conversa, escrito, espetáculo ou objeto pornográficos; …

Artigo 176.º Pornografia de menores

"1 - Quem:
a) Utilizar menor em espetáculo pornográfico ou o aliciar para esse fim;
b) Utilizar menor em fotografia, filme ou gravação pornográficos, independentemente do seu suporte, ou o aliciar para esse fim;
c) Produzir, distribuir, importar, exportar, divulgar, exibir ou ceder, a qualquer título ou por qualquer meio, os materiais previstos na alínea anterior;
d) Adquirir ou detiver materiais previstos na alínea b) com o propósito de os distribuir, importar, exportar, divulgar, exibir ou ceder;
é punido com pena de prisão de um a cinco anos.
2 - Quem praticar os atos descritos no número anterior profissionalmente ou com intenção lucrativa é punido com pena de prisão de um a oito anos.
3 - Quem praticar os atos descritos nas alíneas a) e b) do n.º 1 recorrendo a violência ou ameaça grave é punido com pena de prisão de 1 a 8 anos.
4 - Quem praticar os atos descritos nas alíneas c) e d) do n.º 1 utilizando material pornográfico com representação realista de menor é punido com pena de prisão até dois anos.
5 - Quem, intencionalmente, adquirir, detiver, aceder, obtiver ou facilitar o acesso, através de sistema informático ou qualquer outro meio aos materiais referidos na alínea b) do n.º 1 é punido com pena de prisão até 2 anos.
6 - Quem, presencialmente ou através de sistema informático ou qualquer outro meio, sendo maior, assistir ou facilitar acesso a espetáculo pornográfico envolvendo a participação de menores de 16 anos de idade é punido com pena de prisão até 3 anos.
7 - Quem praticar os atos descritos nos n.º 5 e 6 com intenção lucrativa é punido com pena de prisão até 5 anos.
8 - A tentativa é punível".

(Continua)

Código Penal (Continuação)

Artigo 180.º - Difamação

1 - Quem, dirigindo-se a terceiro, imputar a outra pessoa, mesmo sob a forma de suspeita, um facto, ou formular sobre ela um juízo, ofensivos da sua honra ou consideração, ou reproduzir uma tal imputação ou juízo, é punido com pena de prisão até 6 meses ou com pena de multa até 240 dias.

Artigo 181.º - Injúria

1 - Quem injuriar outra pessoa, imputando-lhe factos, mesmo sob a forma de suspeita, ou dirigindo-lhe palavras, ofensivos da sua honra ou consideração, é punido com pena de prisão até 3 meses ou com pena de multa até 120 dias.

Artigo 192.º - Devassa da vida privada

1 - Quem, sem consentimento e com intenção de devassar a vida privada das pessoas, designadamente a intimidade da vida familiar ou sexual:

a) Intercetar, gravar, registar, utilizar, transmitir ou divulgar conversa, comunicação telefónica, mensagens de correio eletrónico ou faturação detalhada;

b) Captar, fotografar, filmar, registar ou divulgar imagem das pessoas ou de objetos ou espaços íntimos;

c) Observar ou escutar às ocultas pessoas que se encontrem em lugar privado; ou

d) Divulgar factos relativos à vida privada ou a doença grave de outra pessoa;

é punido com pena de prisão até um ano ou com pena de multa até 240 dias.

Artigo 199.º - Gravações e fotografias ilícitas

1 - Quem sem consentimento:

a) Gravar palavras proferidas por outra pessoa e não destinadas ao público, mesmo que lhe sejam dirigidas; ou

b) Utilizar ou permitir que se utilizem as gravações referidas na alínea anterior, mesmo que licitamente produzidas;

é punido com pena de prisão até 1 ano ou com pena de multa até 240 dias.

2 - Na mesma pena incorre quem, contra vontade:

a) Fotografar ou filmar outra pessoa, mesmo em eventos em que tenha legitimamente participado; ou

b) Utilizar ou permitir que se utilizem fotografias ou filmes referidos na alínea anterior, mesmo que licitamente obtidos.

Artigo 217.º - burla

1 - Quem, com intenção de obter para si ou para terceiro enriquecimento ilegítimo, por meio de erro ou engano sobre factos que astuciosamente provocou, determinar outrem à prática de atos que lhe causem, ou causem a outra pessoa, prejuízo patrimonial é punido com pena de prisão até três anos ou com pena de multa.

(Continua)

Código Penal (Continuação)

Artigo 221.º - Burla informática

1 - Quem, com intenção de obter para si ou para terceiro enriquecimento ilegítimo, causar a outra pessoa prejuízo patrimonial, interferindo no resultado de tratamento de dados ou mediante estruturação incorreta de programa informático, utilização incorreta ou incompleta de dados, utilização de dados sem autorização ou intervenção por qualquer outro modo não autorizada no processamento, é punido com pena de prisão até 3 anos ou com pena de multa.

2 - A mesma pena é aplicável a quem, com intenção de obter para si ou para terceiro um benefício ilegítimo, causar a outrem prejuízo patrimonial, usando programas, dispositivos eletrónicos ou outros meios que, separadamente ou em conjunto, se destinem a diminuir, alterar ou impedir, total ou parcialmente, o normal funcionamento ou exploração de serviços de telecomunicações.

Disponível on-line »

International Telecommunication Union

Lei do Cibercrime

Artigo 4.º
Dano relativo a programas ou outros dados informáticos

1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, apagar, alterar, destruir, no todo ou em parte, danificar, suprimir ou tornar não utilizáveis ou não acessíveis programas ou outros dados informáticos alheios ou por qualquer forma lhes afetar a capacidade de uso, é punido com pena de prisão até 3 anos ou pena de multa.
2 - A tentativa é punível.
3 - Incorre na mesma pena do n.º 1 quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas ou outros dados informáticos destinados a produzir as ações não autorizadas descritas nesse número.
4 - Se o dano causado for de valor elevado, a pena é de prisão até 5 anos ou de multa até 600 dias.
5 - Se o dano causado for de valor consideravelmente elevado, a pena é de prisão de 1 a 10 anos.
6 - Nos casos previstos nos n.os 1, 2 e 4 o procedimento penal depende de queixa".

Artigo 6.º
Acesso ilegítimo

1 - Quem, sem permissão legal ou sem para tanto estar autorizado pelo proprietário, por outro titular do direito do sistema ou de parte dele, de qualquer modo aceder a um sistema informático, é punido com pena de prisão até 1 ano ou com pena de multa até 120 dias.
2 - Na mesma pena incorre quem ilegitimamente produzir, vender, distribuir ou por qualquer outra forma disseminar ou introduzir num ou mais sistemas informáticos dispositivos, programas, um conjunto executável de instruções, um código ou outros dados informáticos destinados a produzir as ações não autorizadas descritas no número anterior.
3 - A pena é de prisão até 3 anos ou multa se o acesso for conseguido através de violação de regras de segurança.

4 - A pena é de prisão de 1 a 5 anos quando:
a) Através do acesso, o agente tiver tomado conhecimento de segredo comercial ou industrial ou de dados confidenciais, protegidos por lei; ou
b) O benefício ou vantagem patrimonial obtidos forem de valor consideravelmente elevado.

5 - A tentativa é punível, salvo nos casos previstos no n.º 2.

6 - Nos casos previstos nos n.os 1, 3 e 5 o procedimento penal depende de queixa.

Disponível on-line »

Código do Direito de Autor e Direitos Conexos

Artigo 195.º
Usurpação

1 - Comete o crime de usurpação quem, sem autorização do autor ou do artista, do produtor de fonograma e videograma ou do organismo de radiodifusão, utilizar uma obra ou prestação por qualquer das formas previstas neste Código.
2 - Comete também o crime de usurpação:
a) Quem divulgar ou publicar abusivamente uma obra ainda não divulgada nem publicada pelo seu autor ou não destinada a divulgação ou publicação, mesmo que a apresente como sendo do respetivo autor, quer se proponha ou não obter qualquer vantagem económica;
b) Quem coligir ou compilar obras publicadas ou inéditas sem autorização do autor;
c) Quem, estando autorizado a utilizar uma obra, prestação de artista, fonograma, videograma ou emissão radiodifundida, exceder os limites da autorização concedida, salvo nos casos expressamente previstos neste Código.
3 - Será punido com as penas previstas no artigo 197.º o autor que, tendo transmitido, total ou parcialmente, os respetivos direitos ou tendo autorizado a utilização da sua obra por qualquer dos modos previstos neste Código, a utilizar direta ou indiretamente com ofensa dos direitos atribuídos a outrem.

Artigo 196.º
Contrafação

1 - Comete o crime de contrafação quem utilizar, como sendo criação ou prestação sua, obra, prestação de artista, fonograma, videograma ou emissão de radiodifusão que seja mera reprodução total ou parcial de obra ou prestação alheia, divulgada ou não divulgada, ou por tal modo semelhante que não tenha individualidade própria.
2 - Se a reprodução referida no número anterior representar apenas parte ou fração da obra ou prestação, só essa parte ou fração se considera como contrafação.
3 - Para que haja contrafação não é essencial que a reprodução seja feita pelo mesmo processo que o original, com as mesmas dimensões ou com o mesmo formato.
4 - Não importam contrafação:
a) A semelhança entre traduções, devidamente autorizadas, da mesma obra ou entre fotografias, desenhos, gravuras ou outra forma de representação do mesmo objeto, se, apesar das semelhanças decorrentes da identidade do objeto, cada uma das obras tiver individualidade própria;
b) A reprodução pela fotografia ou pela gravura efetuada só para o efeito de documentação da crítica artística.

(continua)

Código do Direito de Autor e Direitos Conexos (continuação)

Artigo 197.º
Penalidades

1 - Os crimes previstos nos artigos anteriores são punidos com pena de prisão até três anos e multa de 150 a 250 dias, de acordo com a gravidade da infração, agravadas uma e outra para o dobro em caso de reincidência, se o facto constitutivo da infração não tipificar crime punível com pena mais grave.
2 - Nos crimes previstos neste título a negligência é punível com multa de 50 a 150 dias.
3 - Em caso de reincidência não há suspensão da pena.

Artigo 199.º
Aproveitamento de obra contrafeita ou usurpada

1 - Quem vender, puser à venda, importar, exportar ou por qualquer modo distribuir ao público obra usurpada ou contrafeita ou cópia não autorizada de fonograma ou videograma, quer os respetivos exemplares tenham sido produzidos no País quer no estrangeiro, será punido com as penas previstas no artigo 197.º
2 - A negligência é punível com multa até 50 dias.

Disponível on-line »

International Telecommunication Union

Sites recomendados

SeguraNet

Internet Segura

Miúdos Seguros na Net

Centro de Segurança para as famílias da Google

EU Kids Online

Guia para os pais Vodafone

Comunicar em Segurança

Childnet International

Net Children Go Mobile

Instituto Nacional de Tecnologías de la Comunicación

Ciberfamilias (Lugar de reunión para padres y educadores)

Pantallas amigas

Chavales. Esta es nuestra web

Asociación de usuarios de Internet

Better Internet for Kids (BIK)

Family Online Safety Institute

Stopcyberbullying.org

Cyberbully411.org

Common Sense Media

KidsHealth

WiredSafety.org

OnGuardOnline

WiredSafety

StaySafeOnline.org

Family Online Safety Institute

A Platform for Good

Microsoft Safety & Security Center

Common Sense Media

It Gets Better Project

Instituto de la Juventud

Be Smart online

Oficina de seguridad del internauta

Agencia Española de Protección de Datos

Asociación de internautas

POSCON

No More Ransom (site sobre "ransomware")

Websites for kids and teens

YouAreHere

OnGuardOnline.gov

NetSmartz.org

NetSmartzKids

NSTeens

Kid-friendly search engines

KidsClick!

KidRex

Kidtopia

Thinga

Kiddle