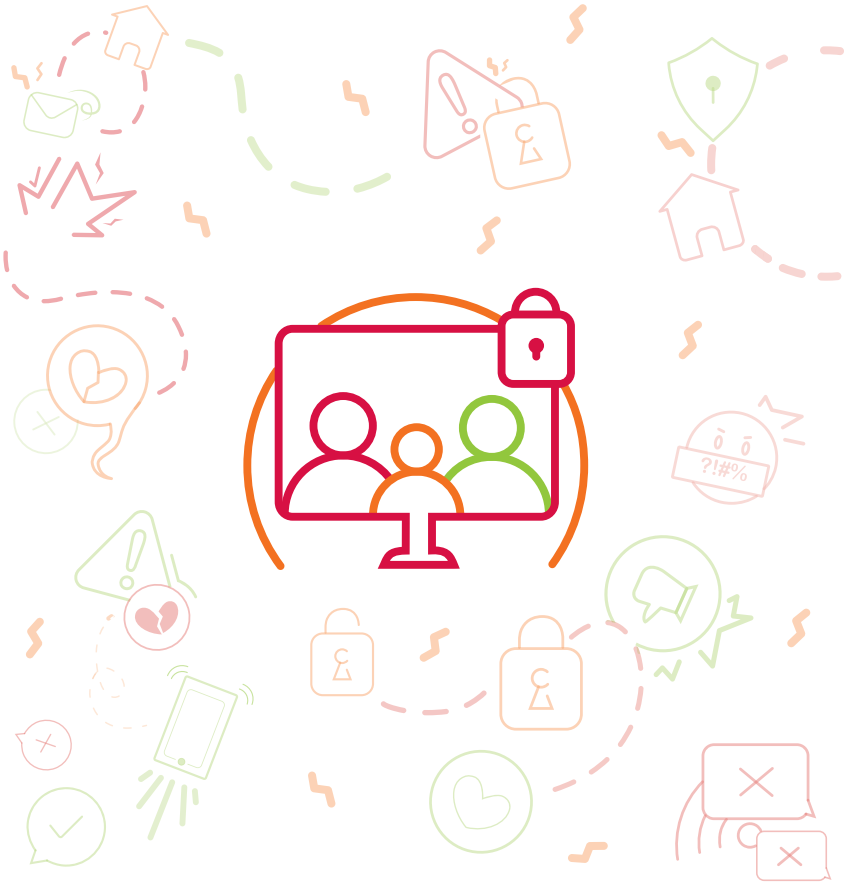
GUIA PARA FAMÍLIAS



SENSIBILIZAR E EDUCAR PARA A CIBERSEGURANÇA

APAV®
associação portuguesa de
Apoio à Vítima

Título: Guia para Famílias – Sensibilizar e Educar para a Cibersegurança
Projeto: Projeto CIBER_FAMÍLIAS: Sensibilizar e Educar para a Cibersegurança
Autor: APAV – Associação Portuguesa de Apoio à Vítima
Baseado em Design Original de: Último Take
Re-Interpretação de Design, Ilustração e Paginação: APAV

Impressão:
Tiragem:
ISBN: 978-989-35232-4-7
Depósito Legal:

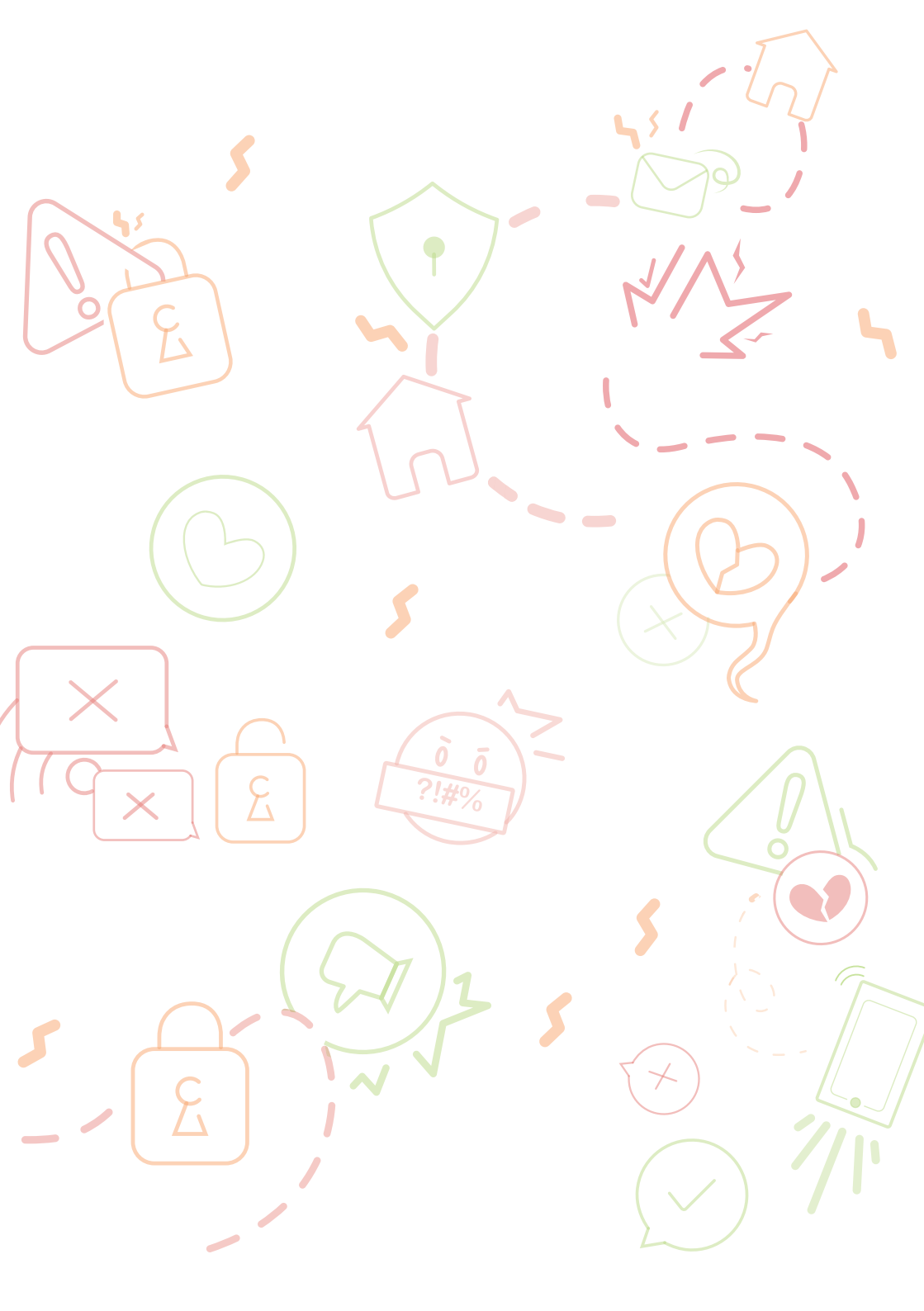
Contactos:
APAV
Rua José Estêvão, 135 – A
1150-201 Lisboa

Tel. +351 21 358 79 00
Fax +351 21 887 63 51

apav.sede@apav.pt
www.apav.pt

GUIA PARA FAMÍLIAS

SENSIBILIZAR E EDUCAR PARA A CIBERSEGURANÇA



INTRODUÇÃO

A prevenção da violência e a promoção do respeito pelas/os outras/os deve ser uma prioridade no cuidado das crianças, uma vez que é fundamental para o seu desenvolvimento. Todavia, devido à sua particular complexidade, esta deve ser uma tarefa de todas/os: famílias, escola e comunidade.

Este Guia faz parte da coleção de *Guias para Famílias*, desenvolvida pela APAV com o objetivo de envolver as famílias na prevenção da violência, e fornecendo estratégias que podem ser integradas nas dinâmicas familiares. A aplicação destas estratégias na educação das crianças possibilitará às famílias assumir um papel mais ativo na prevenção da violência e na promoção de relacionamentos mais positivos, bem como melhorar a interação entre a criança e a respetiva família.

Esta coleção pretende ajudar as famílias a perceber como pequenos ajustes nos comportamentos poderão ter uma influência positiva no desenvolvimento da criança e na qualidade das relações que esta mantém.

O *Guia para Famílias - Sensibilizar e Educar para a Cibersegurança* apresenta-se como essencial e necessário para que todas as famílias consigam transmitir facilmente às suas crianças estratégias para estas se protegerem dos riscos que correm no mundo digital.

A internet veio alterar profundamente a forma como as pessoas vivem, aprendem, trabalham, interagem e ocupam os seus tempos livres. Hoje em dia, a internet é um pilar essencial nas nossas vidas. E se, para as pessoas adultas já é difícil imaginarem o dia-a-dia sem ela, muito mais difícil seria para as crianças e jovens que já nasceram na "era do digital". As crianças e jovens do século XXI usam o computador, o smartphone e tablet para fazer os trabalhos de casa, falar com amigas/os, jogar online e usar as redes sociais. No entanto, para além de todas as potencialidades, o mundo digital traz consigo inúmeros riscos e desvantagens que colocam as crianças e jovens em situações de vulnerabilidade. Por isso, é fundamental que tenham alguém que as ajude a utilizarem a internet de forma segura, responsável e, acima de tudo, positiva.

GLOSSÁRIO

Há conceitos importantes relacionados com os riscos das crianças e jovens quando estão no mundo online, e que devem ser do conhecimento das famílias. Deixamos aqui alguns:

BOLHA DOS MEDIA

Quando alguém limita as suas relações sociais ao contexto online, isolando-se do "mundo real", diz-se que vive na "bolha dos media". Há cada vez mais crianças e jovens a viver neste contexto, fruto da facilidade da socialização virtual, que lhes permite conhecer pessoas de todo o mundo e selecioná-las consoante interesses em comum.

CATFISHING

Roubo de identidade e criação de um ou mais perfis falsos na internet para enganar emocional e/ou financeiramente.

CHAT

Sistema de comunicação escrita em tempo real, realizada através da internet, pelo qual as pessoas participantes trocam mensagens de texto de forma instantânea.

CLICKBAIT

Pode ser comparado a uma espécie de isco, ou seja, é algo que tem como objetivo fazer-nos aceder a determinados conteúdos. O uso frequente econstante de pontos de exclamação, expressões como "tu não vais acreditar", títulos e imagens atrativas e com um sentido ou sensação de urgência são algumas das características que podem ser úteis na identificação desta tática online. É criado um título e imagem de vídeo apelativo para que as pessoas fiquem curiosas o suficiente para consumir o conteúdo.

CONTEÚDOS IMPRÓPRIOS

São textos, imagens, vídeos ou áudios que são vistos como prejudiciais ao desenvolvimento das crianças. Aqui, estamos a falar não só de conteúdos ilegais (por exemplo, a conteúdo de abuso sexual de menores, incitação ao ódio e à violência), mas também de conteúdos perfeitamente legais (como os que apelam à anorexia, bulimia, automutilação).

GLOSSÁRIO

DATA BREACH

A violação de dados, ou data breach, é um incidente de cibersegurança que compromete os dados que estão na posse de um sistema informático de uma organização. Ocorre sempre que pessoas não autorizadas acedem a dados aos quais não deveriam aceder, levando, por exemplo, à violação da confidencialidade e à exposição de dados pessoais.

DATING APP/APLICAÇÃO DE ENCONTROS

Plataforma digital que permite que as pessoas se conheçam e interajam, com o objetivo de encontrar potenciais relacionamentos.

DEEP WEB

A internet divide-se em dois segmentos: a Surface Web, que corresponde à parte da internet que está registada e que é facilmente acedida através dos motores de busca (e.g. Google) e a Deep Web, que se baseia no conteúdo da internet que não está registado e que não pode ser consultado da maneira convencional. Importa ressalvar que a Dark Web, erradamente confundida com a Deep Web, aloca-se dentro desta, sendo que websites relacionados com a compra e venda de drogas ou conteúdo de abuso e exploração sexual de menores tendem a ser os mais visitados.

DESINFORMAÇÃO E FAKE NEWS

Informação falsa e notícias “fabricadas” divulgadas online com o objetivo de, direta ou indiretamente, favorecer interesses ou grupos políticos. Isto pode traduzir-se num alheamento da realidade e na criação de falsas perceções.

DISCURSO DE ÓDIO ONLINE

É cada vez mais notória a polarização de opiniões nos debates nas redes sociais, blogs e chats de jogos, mais profundos. Muitas pessoas e organizações aproveitam-se do anonimato concedido pela internet, a rapidez com que as mensagens circulam e o alcance das mesmas, para a disseminação massiva de discurso de ódio – baseado num ódio a todas as pessoas ou grupos percebidos como "diferentes" (seja a nível religioso, de cor de pele, país de origem, orientação sexual, identidade de género, contexto socioeconómico, etc.).

GLOSSÁRIO

DOXING
Divulgar informações pessoais e privadas de uma pessoa na internet sem o seu consentimento, muitas vezes com a intenção de prejudicar ou ameaçar essa pessoa.

FILTER BUBBLE
São os conteúdos aos quais os websites nos expõem com base nas pesquisas na internet/websites e naquilo que clicamos com maior frequência. Apesar de parecerem inofensivas, estas “filter bubbles” podem ser prejudiciais: como são criadas pela nossa atividade na internet, vai limitar-nos àquilo que já consumimos e aos nossos interesses, funcionando como uma espécie de barreira entre aquilo que já veem na internet e o resto, deixando de aceder a conteúdos com pontos de vista diferentes.

GASLIGHTING
Abuso psicológico que passa pela distorção da realidade, de modo a favorecer a pessoa agressora, fazendo a vítima duvidar da própria memória, perceção e sanidade.

GHOSTING
Acabar uma relação amorosa de maneira abrupta e inesperada, desaparecendo sem explicar o fim da relação.

INTELIGÊNCIA ARTIFICIAL
Corresponde à capacidade que alguns programas informáticos possuem de simular a inteligência humana, para nos auxiliarem na realização de tarefas. Exemplos destes programas são a Siri, o Google Assistente, a Alexa e o ChatGPT.

LOVE BOMBING
Quando alguém é excessivamente afetuoso e, de repente, muda de comportamento, acusando a outra pessoa, deixando-a vulnerável e a sentir-se culpada de maneira a poder manipulá-la.

GLOSSÁRIO

MALWARE
Este conceito é utilizado para designar códigos informáticos maliciosos que contêm vírus. A criação destes códigos maliciosos visa a infiltração em dispositivos de forma ilícita para a produção de danos, alterações e/ou furto de informações.

REDES SOCIAIS
São plataformas usadas para criar ligações sociais entre pessoas que partilham interesses ou atividades similares.

SEXTING
Consiste na partilha de mensagens íntimas e outros conteúdos sexuais, tais como fotos, vídeos ou áudios. Esta prática é muito comum entre casais jovens e, sendo consensual, é perfeitamente saudável.

SHARETING
Consiste na partilha online de informações de uma criança ou jovem por parte dos seus familiares, através da publicação de fotos, imagens, vídeos ou outros conteúdos que envolvam a criança ou jovem. Esta exposição excessiva da criança ou jovem pode gerar consequências negativas para a/o mesma/o, nomeadamente a perda da sua privacidade e o aumento da sua vulnerabilidade face aos riscos online.

SOBREXPOSIÇÃO
Acontece quando as crianças se expõem demasiado online, partilhando informação pessoal, imagens, vídeos etc., perdendo a sua privacidade e colocando em risco a sua segurança, aumentando a probabilidade de serem vítimas de cibercrime.

SPAM
Refere-se ao envio massivo e indesejado de e-mails ou mensagens. Por vezes, pode estar associado a tentativas de phishing, de furto de informação ou a conteúdos com malware.

QUAIS SÃO OS PRINCIPAIS RISCOS E FORMAS DE VIOLÊNCIA ONLINE?

1 Ciberbullying

O ciberbullying é uma forma de bullying praticada no meio digital (seja através das redes sociais, email, chats de jogos, etc.).

Mas, antes de mais, **o que é o bullying?** Há três características que têm sempre de estar presentes:

I **Intencionalidade –** vontade consciente de magoar e humilhar a vítima;

II **Repetição –** comportamentos agressivos que acontecem mais do que uma vez;

III **Desequilíbrio de poder –** normalmente a pessoa agressora (*bully*) tem algum tipo de superioridade face à vítima (seja por ser mais alta, mais forte, mais popular ou por ter apoio de mais *bullies)*.

Agora que já sabe o conceito de bullying, consegue adivinhar **quais as características adicionais presentes no ciberbullying?**

- É praticado com recurso à internet e às tecnologias de informação e comunicação;
- A pessoa agressora pode ofender, ameaçar ou insultar a vítima, ou até mesmo difundir imagens ou vídeos embaraçosos, com o objetivo de a humilhar e rebaixar.

Sabia também que...

As consequências do bullying e ciberbullying podem ser graves – sobretudo, quando praticados em contexto de sala de aula, porque a vítima vai ter de passar muito tempo com as pessoas agressoras.

Muitas vezes, há uma continuidade das situações de bullying para ciberbullying e vice-versa, produzindo nas vítimas uma sensação de constante insegurança.

Que comportamentos são considerados ciberbullying?

- Partilha de mensagens, imagens, vídeos ou comentários, com objetivo de ameaçar, insultar ou atacar verbalmente a vítima;
- Partilha de boatos ou mentiras;
- Uso de linguagem ofensiva e discriminatória;
- Furto de identidade (por exemplo, entrar no computador ou telemóvel da vítima para prejudicar a sua reputação, através da partilha de imagens, vídeos ou mensagens ofensivas, sexuais ou discriminatórias em nome da vítima);
- Outing, isto é, revelação pública de segredos da vítima (como a sua orientação sexual, identidade de género, informação embaraçosa e imagens);
- Uso de números falsos ou perfis falsos de redes sociais para ameaçar, insultar ou atacar verbalmente a vítima;
- Apagar a conta ou contas das redes sociais da vítima ou alterar a palavra-passe;
- Incentivar os ataques à vítima nas redes sociais ou chats online, através da partilha de mensagens, imagens, vídeos ou comentários em publicações, maldosos e humilhantes;
- Excluir a vítima de um grupo online (por exemplo, no WhatsApp), com a intenção de a isolar socialmente;

Caso a/o sua/seu educanda/o apresente algum destes sinais, é possível que esteja a ser vítima de ciberbullying:

- Alterações repentinas de comportamento;
- Medo e ansiedade ao utilizar a internet;
- Baixa autoestima;
- Perda de interesse em coisas e atividades de que antigamente gostava;
- Depressão;
- Quebras no desempenho escolar;
- Pesadelos e insónias;
- Alterações de apetite;
- Conflitos com colegas de turma ou com outras pessoas próximas;
- Comportamentos autolesivos (ex. automutilações e tentativas de suicídio).

DICAS PARA AS FAMÍLIAS

- **Ajude a criança ou jovem a desenvolver estratégias para a resolução positiva de conflitos.**

- Se a criança ou jovem se sentir magoada, atacada ou ofendida, deve dizer que não gosta do que aconteceu, centrando-se no que pensa sobre o assunto e como o comportamento da outra pessoa a fez sentir.

- Se, ainda assim, ela não for capaz de resolver o conflito sozinha, deve pedir ajuda a uma pessoa adulta de confiança.

O que não me posso mesmo esquecer...

A pessoa adulta de confiança é a pessoa que escuta com atenção, valoriza o pedido de ajuda, valida os sentimentos da criança ou jovem e que ajuda a encontrar respostas adequadas às suas necessidades.

Se pretender saber mais sobre a pessoa adulta de confiança, pode consultar o nosso Guia para Famílias - Sensibilizar e Educar para a Segurança que se encontra disponível online gratuitamente.

2 Ciberstalking

O ciberstalking é um comportamento de perseguição (stalking) que acontece no mundo digital (seja através das redes sociais, email, chats de jogos, etc.).

Mas, antes de mais, o que é que caracteriza o stalking?

- Assédio persistente e contactos indesejados;
- Objetivo de conhecer, seduzir, controlar a vida da vítima, começar (ou reatar) uma relação mais próxima com essa pessoa (seja amizade ou namoro);
- Colocar a vítima numa situação de desconforto, medo e intimidação.

Como no stalking, no ciberstalking, a pessoa agressora pode ser conhecida da vítima ou um total desconhecido.

Que comportamentos são considerados ciberstalking?

- Ligar constantemente à vítima;
- Enviar várias mensagens, emails ou comentários nas redes sociais até a vítima responder;
- Roubar a identidade da vítima;
- Fazer ameaças;
- Aceder, sem autorização da vítima, ao seu email ou conta das redes sociais, a fim de monitorizar informação privada e o quotidiano da vida da vítima, ou para agir em seu nome;
- Estabelecer contactos de natureza sexual indesejados (por exemplo, enviando fotografias íntimas não solicitadas).

Saiba também que...

Estes comportamentos, para além de persistentes, tendem a tornar-se mais graves com o tempo, podendo ter início com chamadas constantes e culminando no furto de identidade ou em ameaças.

O que diz a lei?

O ciberstaking está enquadrado no tipo de crime de "perseguição", previsto no artigo 154.º-A do Código Penal.

Significa isto que, se a pessoa agressora tiver mais de 12 anos pode ser legalmente responsabilizada pela prática destes comportamentos, com medidas que podem chegar ao internamento em centro educativo, dependendo da gravidade dos factos praticados.

Se a criança ou jovem apresentar algum destes sinais, é possível que esteja a ser vítima de ciberstalking:

- Começar a isolar-se socialmente;
- Apresentar quebras no rendimento escolar;
- Alterar repentina e radicalmente a sua aparência física;
- Estar constantemente em estado de alerta;
- Apresentar distúrbios alimentares (como a bulimia, a anorexia ou a compulsão alimentar);
- Dormir mal, ter pesadelos e insónias;
- Sentir medo e ansiedade;
- Apresentar sintomas de depressão e pensamentos suicidas;
- Tentar magoar-se, ou mesmo tentativas de suicídio.

DICAS PARA AS FAMÍLIAS

- Explique à criança ou jovem o que é o ciberstalking e quais as suas consequências;
- Mostre-se sempre disponível para ouvir a criança ou jovem sobre a sua atividade online;
- Explique que não é saudável nem normal ser-se constantemente perseguida/o ou contactada/o por outras pessoas;
- Incentive-a/o a bloquear a pessoa agressora, a guardar todos os registos de contacto (ou tentativas), e a pedir ajuda a uma pessoa adulta de confiança.

3 Grooming, partilha não consensual de imagens e vídeos e extorsão sexual

O que é que estes termos significam?

- O **grooming** (aliciamento de menores online), abrange um conjunto de técnicas utilizadas por uma pessoa adulta com vista a obter a confiança de uma criança e manipulá-la.

  Em regra, os primeiros contactos que a pessoa agressora estabelece com a criança não têm teor sexual. Procuram estabelecer uma relação de confiança, fazendo elogios, partilhando gostos em comum e, em alguns casos, oferecendo presentes.

  O grooming costuma ter como objetivo fazer com que a criança partilhe vídeos ou imagens suas de cariz sexual, ou pratique atos sexuais ao vivo.

- A **partilha não consensual de imagens e vídeos** pode ocorrer em diferentes circunstâncias, incluindo no âmbito de relacionamentos íntimos, de amizade ou em relações ocasionais. Ocorre quando alguém partilha com outra pessoa um conteúdo íntimo seu e o mesmo é publicado e partilhado por essa pessoa, sem o seu consentimento. Esses conteúdos podem ser partilhados através de vários canais e meios de comunicação, sendo difícil a sua posterior remoção, uma vez que, após a sua publicação online, os mesmos podem ser visualizados e guardados em qualquer dispositivo. Note-se que esta partilha não consensual ou a sua ameaça podem ocorrer também por vários motivos, incluindo por diversão, por excitação, para ostentação, para provocar sofrimento na vítima ou para a sua extorsão, procurando especificamente obter mais conteúdos, dinheiro e/ou a marcação de encontros presenciais.

- Por sua vez, a **extorsão sexual** aparece muitas vezes na sequência de situações de grooming ou partilha não consensual de imagens e vídeos entre pares, e traduzindo-se na tentativa de obter dinheiro, a troco de não divulgar conteúdos íntimos da vítima. Esta prática também constitui **crime** e é cada vez mais praticada entre as crianças e jovens.

O que diz a lei?

O grooming enquadra-se no crime de **aliciamento de menores para fins sexuais**, previsto no artigo 176.º-A do Código Penal português.

Quando alguém **ameaça** partilhar imagens íntimas, sem o consentimento da outra pessoa, está a praticar um crime de ameaça, nos termos do artigo 153.º do Código Penal.

Já quando a pessoa agressora "passa das palavras aos atos" e efetivamente **partilha** essas mesmas imagens íntimas na internet, incorre no crime de devassa da vida privada, previsto no artigo 192.º do Código Penal.

Estes sinais podem significar que uma criança ou jovem está a ser vítima de grooming, partilha não consensual de imagens e extorsão sexual:

- Ter sentimentos de culpa ou vergonha;
- Ser vítima de bullying ou ciberbullying;
- Começar a isolar-se socialmente;
- Sentir medo ou ansiedade;
- Apresentar sintomas de depressão, incluindo pensamentos suicidas;
- Tentar magoar-se, ou até mesmo tentativas de suicídio;
- Ter dificuldades na expressão e exploração da sua sexualidade;
- Ter uma imagem sexualizada (por exemplo, começar a vestir-se com roupa reveladora ou fazer muitas alusões ao sexo e a fantasias sexuais);
- Estar constantemente alerta e sentir-se constantemente vigiada;
- Apresentar distúrbios alimentares (como anorexia, bulimia e compulsões alimentares);
- Começar a dormir mal, ter pesadelos e insónias.

DICAS PARA AS FAMÍLIAS

- Explique à criança ou jovem que existem riscos quando falamos online com pessoas estranhas;
- Tenha proteções (por exemplo, autocolantes) que cubram as câmaras dos seus computadores e tablets;
- Aconselhe-a a nunca partilhar informações pessoais (nome completo, morada, rotina, escola que frequenta, nome de familiares, etc.), nem fotografias ou vídeos íntimos;
- Ensine-a a detetar perfis falsos (por exemplo, pesquisando as fotos de perfil, ao carregar no botão do lado direito do rato e escolhendo a opção "pesquisar imagem no Google");
- Ensine a criança ou jovem a nunca ceder a chantagens online, e que, caso alguém tente chantageá-la, deve bloquear imediatamente a pessoa e contar a uma pessoa adulta de confiança.

LEMBRE-SE:

A sua intervenção pode prevenir uma situação de risco ou pode pará-la antes que se torne mais grave.

4 Phishing

Phishing vem de pesca?

Por acaso vem mesmo! É este o nome que se dá ao envio de mensagens que contêm um link aparentemente legítimo e seguro, mas que é, na verdade, malicioso.

A vítima pode ser direcionada para um website falso da sua entidade bancária, de uma plataforma de videojogos ou de outra entidade, visando a obtenção de dados bancários e de informações confidenciais da vítima.

Estes sinais podem indicar que a criança ou jovem foi vítima de phishing:

- Perdas financeiras inesperadas;
- Medo e ansiedade;
- Sentimentos de raiva e desconfiança constantes e prolongados;
- Culpa;
- Reações injustificadas de julgamento e culpabilização pelas outras pessoas.

O que diz a lei?

A prática de phishing está relacionada com a prática dos seguintes crimes:

- Falsificação ou contrafação de documentos (artigo 256.º do Código Penal);
- Falsidade informática (artigo 3.º da Lei do Cibercrime);
- Acesso ilegítimo (artigo 6.º da Lei do Cibercrime);
- Burla (artigo 217.º do Código Penal).

DICAS PARA AS FAMÍLIAS

- Aconselhe a criança ou jovem a não frequentar websites cujo endereço não seja iniciado por “https” e não tenha o símbolo de um cadeado;
- Oriente-a para nunca clicar em links enviados por pessoas desconhecidas – seja através de email, mensagens, chats, etc;
- Chame a atenção para e-mails, mensagens e comentários mal escritos – já que podem indicar que foram traduzidos automaticamente ou enviados por quem não domina o idioma;
- Aconselhe a criança ou jovem a pesquisar excertos dos emails, mensagens ou comentários no Google (para perceber se aquele conteúdo já foi reportado como fraudulento);
- Verifique sempre, com a presença da criança ou jovem, se os dispositivos que ela usa (computador, tablet ou smartphone) estão devidamente atualizados e protegidos – e ensine-a a atualizá-los;
- Nunca faça download de ficheiros ou aplicações em redes wi-fi públicas e aconselhe a criança ou jovem a agir da mesma forma.

5 Burlas Online

O que são as Burlas online?

A burla caracteriza-se pelo engano ou erro da vítima, que a leva a entregar algo indevidamente à pessoa agressora (normalmente dinheiro), com a convicção de que essa entrega ou pagamento era lícito e devia acontecer.

Pela sua ingenuidade, as crianças e jovens são facilmente enganadas e podem, por isso, ser potenciais vítimas de burlas.

Em Portugal, há três tipos de burlas online que se destacam:

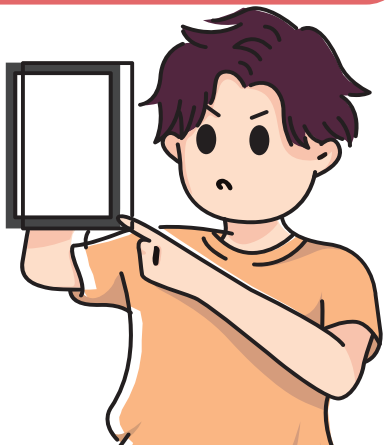
I **Burlas no comércio eletrónico**
Quando uma criança ou jovem compra uma consola online que vem danificada, por exemplo.

II **Burlas bancárias**
Quando se recebe um email, supostamente de uma entidade bancária, e se carrega no link para autorizar um pagamento.

III **Burlas nos relacionamentos amorosos**
Quando, no contexto de um namoro ou amizade online, é sugerido ou pedido à vítima que transfira dinheiro ou envie presentes.

O que diz a lei?

As burlas online são punidas como crime de burla (artigo 217.º do Código Penal), e crime de burla informática (artigo 221.º do Código Penal).



QUAL É O MEU ESTILO PARENTAL?

Todas as famílias são diferentes. No entanto, podemos dizer que há quatro tipos de estilos parentais que as famílias costumam adotar com as suas crianças e jovens relativamente ao uso que estas fazem da internet.

Em qual dos estilos parentais é que a sua família se enquadra melhor? Para descobrir, procure responder às seguintes perguntas:

1. Em minha casa, existem regras claras para as atividades online das crianças ou jovens?

   A. Sim

   B. Não

Se respondeu "não" a esta pergunta, passe para a pergunta 4.

2. Quando a criança não cumpre as regras, o que faço?

   A. Monitorizo e corrijo os comportamentos negativos, reforçando os positivos.

   B. Dou preferência a meios punitivos e violentos.

3. Na definição de regras, costumo ter em consideração a vontade da criança ou jovem?

   A. Não

   B. Sim

4. De que forma costuma comunicar com a criança ou jovem?

   A. Tenho uma comunicação aberta e clara, baseada no respeito mútuo.

   B. Tenho uma comunicação fechada e pouco diálogo com a criança ou jovem.

5 Como definiria a sua família em termos de afeto e carinho?

A. A nossa família é afetuosa, carinhosa e compressiva.

B. Na nossa família, há poucas demonstrações de afeto e carinho.

I Se respondeu “sim” à primeira pergunta e maioritariamente a opção "A" nas perguntas seguintes, é provável que o seu estilo parental seja com autoridade (alto controlo parental e alto afeto parental).

Famílias com autoridade, ao mesmo tempo que estabelecem regras claras para as variadas atividades online levadas a cabo pelas suas crianças e jovens, monitorizam e corrigem os comportamentos negativos, reforçando os positivos. Aqui, a comunicação é aberta, clara e baseada no respeito mútuo. Neste estilo parental, as famílias tendem a ser afetuosas, carinhosas, compreensivas e atendem às necessidades gerais das crianças e jovens.

Se respondeu “sim” à primeira pergunta e maioritariamente a opção “B” nas perguntas seguintes, é provável que o seu estilo parental seja autoritário (alto controlo parental e baixo afeto parental).

II As famílias que adotam um estilo autoritário estabelecem, ao darem preferência a meios punitivos e violentos, regras restritivas relativas ao uso da internet, não tendo em consideração a palavra ou vontade da criança ou jovem. Por norma, existe pouca abertura e pouco diálogo no seio familiar.

III Se respondeu “não” à primeira pergunta e maioritariamente a opção “A” nas perguntas seguintes, é provável que o seu estilo parental seja permissivo (baixo controlo parental e alto afeto parental).

Este estilo parental é pautado por um baixo controlo, mas alto afeto parental. Ou seja, enquadram-se neste estilo famílias que, apesar de serem bastante afetivas e comunicativas, não estabelecem de forma clara as regras e os limites para para o uso da internet. Neste caso, aliada à recetividade da utilização da internet, as famílias dão liberdade às crianças e jovens para que estes definam e regulem seu próprio comportamento online.

IV Se respondeu “não” à primeira pergunta e maioritariamente a opção “B” nas perguntas seguintes, é provável que o seu estilo parental seja “laissez-faire” (baixo controlo parental e baixo afeto parental).

O estilo parental “laissez-faire”, também designado de negligente, traduz-se em baixos níveis de controlo e de afeto. As famílias que adotam este estilo são, tendencialmente, insensíveis, incompreensíveis e pouco exigentes relativamente ao uso da internet pelas suas crianças e jovens. No fundo, não há um envolvimento ativo, o suporte emocional é fraco, assim como a comunicação.

Todos os estilos parentais são válidos. No entanto, é importante lembrar que...

- O envolvimento positivo das famílias nas atividades online das crianças e jovens tende a diminuir os problemas relacionados com o uso da internet e a promover o bem-estar online.
- Uma postura demasiado controladora pode ter um efeito contraproducente, e levar a que a criança ou jovem procure aceder à internet quando a família não está a ver – estando, assim, mais exposta a situações de risco.

COMO PRATICAR UMA PARENTALIDADE DIGITAL MAIS POSITIVA?

I **Descubram a internet em conjunto.**

Pode ser uma atividade divertida! Ficará surpreendida/o com aquilo que a criança ou jovem lhe pode ensinar.

II **Faça uso dos controlos parentais e configure os dispositivos.**

Uma grande parte das aplicações com acesso à internet têm, integrados em si, controlos e filtros que permitem limitar o tempo de utilização ou restringir o acesso a conteúdo inapropriado.

MAS ATENÇÃO!

Controlar os aspetos mais técnicos não substitui a importância do diálogo com a criança ou jovem.

III **Tente chegar a um consenso quanto às regras do uso da internet e das tecnologias em casa.**

LEMBRE-SE

As regras devem ser realistas e adaptadas à sua família, podendo ser revistas conforme as necessidades e interesses que vão surgindo. Limites realistas e consistentes ajudam as crianças e jovens a estabelecerem e desenvolverem hábitos digitais saudáveis e positivos.

IV **Mostre interesse na vida online da criança ou jovem.**
Desta forma, é mais provável que esta lhe conte se estiver perante alguma das situações de risco descritas acima.

V **Promova uma cultura de privacidade.**
Através de um diálogo aberto e sincero, lembrando a criança ou jovem para não partilhar informações pessoais, como nome completo, morada, escola que frequenta, nome de familiares, etc.

LEMBRE-SE

As contas nas redes sociais têm "modo privado". É importante incentivar a criança ou jovem a usar esta opção, uma vez que os conteúdos partilhados publicamente podem ser vistos por qualquer pessoa.

Se necessário, faça uma demonstração de como configurar as definições de privacidade, insistindo na ideia de que quanto mais os outros sabem sobre nós, mais vulneráveis estaremos.

VI **Ensine-a a questionar: "esta informação é real?", detetando fake news.** No mundo digital, há todo o tipo de informações. Tendo isto em conta, é importante dar ferramentas às crianças e jovens que as ajudem a desenvolver espírito crítico e a pensar por elas próprias.

VII **Faça o que sugere!**
Conhece o ditado: "faz o que eu digo, não faças o que eu faço?"

As crianças e os jovens aprendem muito através da imitação. Estão atentas ao que se diz em família, ao que se faz e quanto tempo é dedicado ao uso da internet e dos dispositivos digitais. Por isso, é importante adotar um comportamento exemplar e não transmitir mensagens contraditórias.

A NÃO ESQUECER

- Uma parentalidade digital positiva dá às crianças e jovens as ferramentas que elas precisam para aproveitarem, de forma segura, as vantagens do mundo digital.
- Ao termos um diálogo aberto, transparente, sincero, empático e de confiança, incentivamos as crianças e jovens a exporem as suas dúvidas e a partilharem as situações que as tenham deixado desconfortáveis.

Se a criança ou jovem partilhou consigo alguma coisa menos positiva (ou preocupante):

I. Agradeça e valide a partilha.

II. Tente encontrar uma solução para o problema.

III. Ensine à criança ou jovem o que esta deve fazer se voltar a acontecer algo semelhante.

QUE RESPOSTAS DE APOIO EXISTEM?

Em seguida, apresentamos uma lista de contactos de entidades que lhe poderão ser úteis. Além desses contactos, pode ser importante realizar uma pesquisa adicional para perceber se, na sua área de residência, encontra outros serviços e respostas.

APAV

A Associação Portuguesa de Apoio à Vítima (APAV), é uma organização nacional sem fins lucrativos e de solidariedade social que tem como principal objetivo apoiar as vítimas de qualquer tipo de crime, assim como os seus familiares e pessoas amigas.

Se precisar de ajuda ou informação pode, de forma **gratuita** e **confidencial:**

- Ligar para a **Linha de Apoio à Vítima** (116 006), que se encontra disponível todos os dias úteis, das 8h00 às 23h00;
- Dirigir-se a um dos **Gabinetes de Apoio à Vítima** (GAV), localizados em diferentes pontos do país. Para saber a morada e os contactos do GAV mais próximo de si, carregue aqui: *http://apav.pt*;
- Enviar um **e-mail** para *apav.sede@apav.pt*. Entraremos em contacto consigo o mais rapidamente possível;
- Contactar-nos por outros meios, como pelo **Skype** (apav_lav) ou através de mensagem privada numa das nossas **redes sociais** (Messenger, X, Instagram, YouTube, LinkedIn).

Linha Internet Segura (LIS)

A LIS, plataforma que apoia vítimas de cibercrime e presta esclarecimentos com o objetivo de tornar a navegação na internet mais segura, é gerida pela APAV e está enquadrada nas atividades do Consórcio Centro Internet Segura, coordenado pelo Centro Nacional de Cibersegurança (CNCS).

A LIS integra dois serviços: a Helpline e a Hotline.

Helpline:
Trata-se de um serviço gratuito, confidencial e anónimo, que pretende o esclarecimento e apoio a todas as pessoas que apresentem questões sobre o uso de plataformas ou tecnologias digitais. Este esclarecimento está acessível através de formulário (*http://www.internetsegura.pt/lis/pedir-esclarecimento*), contacto telefónico (800 21 90 90) e e-mail (*linhainternetsegura@ apav.pt*).

Hotline:
Trata-se de um serviço de denúncia de conteúdos ilegais online, nomeadamente de situações relacionadas com abuso sexual de menores, apologia ao racismo e à violência. A denúncia, anónima e confidencial, pode ser realizada através dos contactos indicados anteriormente ou através do formulário disponibilizado "Denunciar Conteúdo Ilegal" *(http://www.internetsegura.pt/lis/denunciar-conteudo-ilegal).*

As denúncias recebidas são triadas e analisadas por profissionais qualificadas/os, sendo devidamente encaminhadas para as autoridades nacionais ou congénere internacional.

Forças de Segurança

A **Polícia Judiciária** (PJ), através da Unidade Nacional de Combate ao Cibercrime e à Criminalidade Tecnológica (UNC3T), investiga crimes cibernéticos e disponibiliza também no seu website um formulário para a apresentação de queixa online (*https://qe.pj.pt/login*) ou de denúncia anónima (*https://www.policiajudiciaria.pt/denuncia-anonima/*).

Além de ser possível dirigir-se presencialmente à PJ, pode ir a uma esquadra da **Polícia de Segurança Pública** (PSP) ou a um posto da **Guarda Nacional Republicana** (GNR) para apresentar queixa ou denunciar um cibercrime de que tenha conhecimento.

Websites Úteis

Associação Portuguesa de Apoio à Vítima (APAV)
Website: www.apav.pt

Associação para o Planeamento da Família (APF)
Website: www.apf.pt

Associação de Mulheres Contra a Violência (AMCV)
Website: www.amcv.org.pt

Associação Portuguesa de Crianças Desaparecidas (APCD)
Website: www.ap-cd.pt

Comissão para a Cidadania e a Igualdade de Género (CIG)
Website: www.cig.gov.pt

Comissão Nacional de Promoção dos Direitos e Proteção das Crianças e Jovens (CNPDPCJ)
Website: www.cnpdpcj.gov.pt

Direção-Geral da Saúde (DGS)
Website: www.dgs.pt

Fundação da Juventude (FJ)
Website: www.fjuventude.pt

Guarda Nacional Republicana (GNR)
Website: www.gnr.pt

Instituto de Apoio à Criança (IAC)
Website: www.iacrianca.pt

Polícia Judiciária (PJ)
Website: www.policiajudiciaria.pt

Polícia de Segurança Pública (PSP)
Website: www.psp.pt

Segurança Social (SS)
Website: www.seg-social.pt

SNS 24 - Centro de Contacto do Serviço Nacional de Saúde
Website: www.sns24.gov.pt

União de Mulheres Alternativa e Resposta (UMAR)
Website: www.facebook.com/UMARfeminismos

Contactos Úteis

Número Nacional de Emergência
112 (gratuito)

Linha Nacional de Emergência Social
114 (gratuito)

Linha SOS Criança
116 111 (gratuito)

Linha de Apoio à Vítima da APAV
116 006 (gratuito)

Linha Internet Segura
800 21 90 90 (gratuito)

Linha Segurança Social
300 502 502

Linha SOS Criança Desaparecida
116 000 (gratuito)

SNS 24
808 24 24 24

Serviço de Informação às Vítimas de Violência Doméstica
800 202 148 (gratuito)

ONDE ENCONTRAR INFORMAÇÃO ADICIONAL?

Se quiser obter informação adicional sobre as temáticas abordadas neste Guia, poderá também consultar as sugestões abaixo apresentadas. Muitas delas possuem conteúdos específicos para as crianças.

Recursos digitais do **Instituto de Apoio à Criança**, disponíveis em www.iacrianca.pt/recursos-digitais;

Folhas informativas da **APAV**, que abordam, de forma sintética, um conjunto variado de temáticas e formas de violência, disponíveis em www.apav.pt/apav_v3/index.php/pt/folhas-informativas;

Guiões de Educação Género e Cidadania, lançados pela Comissão para a Cidadania e a Igualdade de Género, disponíveis em www.cig.gov.pt;

Espaço Crianças e Jovens, da Comissão Nacional de Promoção dos Direitos e Proteção das Crianças e Jovens, disponível em www.cnpdpcj.gov.pt/espaco-criancas-e-jovens;

Segura Net – Navegar em Segurança, com diversos recursos para crianças, famílias e professores/as, disponível em https://www.seguranet.pt/;

Recursos online da Linha Internet Segura, disponíveis em www.internetsegura.pt;

Website www.prevencao.apav.pt desenvolvido pela **APAV** e que contém diversos recursos, para famílias e profissionais, de prevenção e sensibilização;

Website www.apavparajovens.pt desenvolvido pela **APAV** e destinado a crianças e jovens, com informação sobre segurança e proteção face a diferentes formas de violência;

Website www.abcjustica.pt desenvolvido pela **APAV** e destinado a crianças e jovens, com conteúdos informativos, vídeos e jogos sobre o funcionamento da Justiça e os direitos das vítimas.

NOTAS

Esta publicação foi desenvolvida pela Associação Portuguesa de Apoio à Vítima (APAV), com o apoio financeiro dos Prémios Caixa Social, iniciativa da Caixa Geral de Depósitos.

CIBER_FAMÍLIAS

SENSIBILIZAR E EDUCAR PARA A CIBERSEGURANÇA

Financiado por:

Caixa Social
PRÉMIOS'23
PROJETO PREMIADO

APAV®
associação portuguesa de
Apoio à Vítima