Guia para os pais que querem proteger os seus filhos na internet*

Agrupamento de escolas Elias Garcia
Secção de tecnologias de informação e comunicação

*Texto adaptado do artigo “O guia definitivo para proteger seu filho online em 2021”, de Ariel Hochstadt, disponível em https://pt.vpnmentor.com/blog/o-guia-completo-para-os-pais-que-querem-proteger-os-seus-filhos-na-internet/

Índice

Introdução

Atualmente, vemos notícias sobre o impacto da tecnologia nas nossas vidas diárias e muitos de nós começamos a pensar sobre como a tecnologia nos afeta pessoalmente. **Mas quantos de nós já parou para pensar sobre como isso afeta os nossos filhos?** Cada vez mais cedo, as crianças têm acesso a dispositivos eletrónicos e à internet. Em casa, na escola, com os colegas e amigos as crianças utilizam as tecnologias para comunicar, realizar tarefas escolares, jogar, comunicar com outros, visionar diversos tipos de conteúdos, etc.

A tecnologia chegou para ficar, mas muitos não pensam nos riscos em termos de segurança cibernética. Estudos revelam que **muitos pais nunca verificam a atividade online dos seus filhos**. E essa atividade online aumenta a cada ano.

Para muitas crianças, o mundo online é mais real do que o mundo real. **É crucial para o bem-estar dos nossos filhos que entendamos o que eles veem online e como isso pode afetar o seu bem-estar físico e emocional.**

O problema é que muito de nós sentem que não são capazes de entender o mundo online. Instagram, Snapchat, TikTok e Twitter são desconcertantes o suficiente, sem mencionar o 4chan e o TOR. Além disso, pensamos que não temos as competências digitais necessárias para navegar neste ambiente complexo.

A boa notícia **é que não é assim tão difícil usar determinados controlos técnicos para protegermos os nossos filhos online.** Mais importante ainda é que **a melhor coisa que pode fazer para proteger os seus filhos é conversar com eles!**

Defina limites claros para o que e quando eles acedem online, mas esteja também disponível para conversar quando os seus filhos cometerem um erro ou tiverem ido longe demais.
Neste guia, descrevemos oito áreas às quais deve prestar atenção ao navegar no mundo online. Dependendo das idades dos seus filhos, nem tudo se aplicará a si. Pense neste manual não apenas como diretrizes para o que deve fazer agora, mas àquilo a que deve prestar atenção à medida que os seus filhos crescem.

1. Smartphones e aplicações

Dar ao seu filho um smartphone traz inúmeras vantagens, podendo ser uma excelente ferramenta de segurança. O seu filho pode usá-lo caso precise de o contatar e, se utilizar o GPS do smartphone dele, pode rastrear a sua localização.
Os smartphones, no entanto, também podem ser mal utilizados, e em algumas situações podem deixar as crianças vulneráveis. **Como os smartphones são dispositivos pessoais, muitas vezes não sabemos o que nossos filhos fazem com eles ou como os usam.**

Ao dar ao seu filho um smartphone, deve ter diretrizes claramente delineadas e dizê-las ao seu filho. Se o seu filho já tiver um smartphone, nunca é tarde demais rever ou definir algumas regras. Implemente regras de uso do smartphone com o seu filho. Ao garantir que seus filhos o envolvem nas atividades que ele realiza com o telemóvel, estará a ajudar a mantê-lo em segurança.

Há muitas precauções que pode tomar para implementar a segurança do smartphone:

- ✓ Peça ao seu filho para assinar um contrato de smartphone antes de lhe dar um. Imprima uma lista de regras e coloque-a num local público da sua casa.
- ✓ Instale uma aplicação de controlo parental. As aplicações de controlo parental para crianças menores permitem limitar o uso do seu filho, determinar a sua localização e monitorizar as suas chamadas e mensagens. As aplicações de controlo parental também permitem que desligue certas funcionalidades em diferentes horas do dia.
- ✓ Defina limites em relação ao tempo de utilização do smartphone ao longo do dia.
- ✓ Seja um exemplo para o seu filho: não leve o seu telemóvel para a mesa, não envie mensagens enquanto dirige e não utilize o telefone ao mesmo tempo que conversa com o seu filho.
- ✓ Estabeleça uma estação de carregamento numa localização central da sua casa. À noite, o smartphone deve ficar fora do quarto do seu filho de forma a que não o possa utilizar no período de descanso.

2. Streaming de conteúdos e Smart TV

Antigamente era comum a família reunir-se em torno da televisão para assistir a um programa e disfrutar da companhia. Atualmente, passou a ser comum ter televisão no quarto e o seu filho acaba por passar horas a assistir a programas sem ter qualquer orientação sobre os conteúdos que deve ou não visionar.

Assistimos a um aumento provedores de streaming em que **os programas disponibilizados nem sempre são adequados às crianças**.
Logicamente há também vantagens, existe uma grande variedade de programas educacionais e documentários dirigidos a crianças e jovens. Alguns deles nem possuem anúncios impedindo assim que o seu filho seja bombardeado com mensagens de publicidade. É possível abrir um mundo inteiro para o seu filho com conteúdo em streaming contínuo – o segredo está em saber usá-lo.

A maioria dos provedores de conteúdo de streaming tem controlos parentais. A Netflix, por exemplo, permite configurar perfis separados para si e para o seu filho. Desta forma, pode **garantir que o seu filho só tem acesso a conteúdos adequados à idade dele**. No entanto, isso não impede que as crianças mudem para o seu perfil, por isso, tem de estar vigilante.

Convém relembrar que a utilização de ferramentas como o controlo parental não substitui as conversas frequentes com o seu filho sobre aquilo a que ele assiste.

Monitorize o tempo passado em frente à TV e limite o número de horas diárias.
Sempre que possível, passe um momento agradável em família junto à TV e aproveite para conhecer os gostos do seu filho e os conteúdos que ele costuma visionar.

3. Consolas de jogos e jogos online

As **consolas de jogos têm sido um motivo de medo e preocupação para muitos pais**. Com tantos jogos com conteúdo violento ou de teor sexual, **é importante ter cuidado com o tipo de jogos que o seu filho escolhe.**

Além disso, os jogos de consola que possuem um componente multiplayer, ou jogos totalmente online, estão **abertos ao abuso de outros jogadores**. Muitos jogos permitem que jogadores de todo o mundo conversem uns com os outros, **expondo potencialmente as crianças ao assédio e ao ciberbullying**. As crianças também podem relacionar-se com outros jogadores e acabar por fornecer informações pessoais.

Os jogos também são uma ótima possibilidade para as crianças desenvolverem uma série de competências tais como a resolução de problemas, comprometer-se com metas a longo prazo ou trabalhar como parte de uma equipa.

Felizmente, a maioria das consolas de jogos fornecem controlos parentais robustos, para que os **pais possam monitorizar os jogos dos seus filhos**.

Algumas medidas que pode tomar:

- ✓ Fale com o seu filho sobre os jogos que ele utiliza.
- ✓ Verifique se o seu perfil está definido como privado.
- ✓ Considere manter a consola de jogos num espaço social compartilhado como a sala de estar.
- ✓ Verifique a classificação de idade dos jogos.
- ✓ Jogue com os seus filhos.
- ✓ Utilize o controlo parentar para configurar o perfil.
- ✓ Limite o tipo de pessoas com quem o seu filho pode falar online.

5. Redes sociais

As redes sociais são também uma preocupação. As nossas crianças utilizam-nas cada vez mais cedo e gastam uma parte considerável do seu tempo a ver publicações, comunicar e criar conteúdos.

Uma pesquisa do grupo sem fins lucrativos Common Sense Media mostrou que há **crianças de 8 a 12 anos de idade que estão online seis horas por dia**, em grande parte em plataformas sociais, **e crianças de 13 a 18 anos de idade, nove horas**!

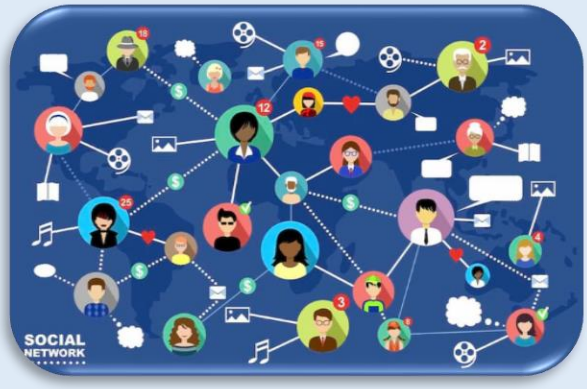
Convém ressalvar que a maioria das redes sociais não permite utilizadores com menos de trezes anos. No entanto, as nossas crianças contornam esse obstáculo mentindo na idade na altura de criar um perfil e muitos pais ajudam-nos a criar uma conta.

As redes sociais podem ser particularmente viciantes para pré-adolescentes e adolescentes. Elas também abrem a porta para uma variedade de perigos, como o ciberbullying, a partilha de conteúdos inadequados e a possibilidade de estabelecer conversas com estranhos.

Por outro lado, o acesso às redes sociais também é fundamental para o desenvolvimento da identidade social dos adolescentes. É a forma como eles se conectam com os amigos, e pode ser uma maneira saudável de conviver com outras pessoas. A chave é estabelecer alguns limites para que seja uma experiência positiva.

O que pode fazer:

- ✓ Imponha um ambiente seguro.
- ✓ Não deixe o seu filho utilizar as redes sociais antes de ter idade legal para o fazer.
- ✓ Mantenha o computador num local público, de forma a que possa monitorizar a atividade do seu filho.
- ✓ Limite a quantidade de tempo gasto nas redes sociais.
- ✓ Ajude-o a definir configurações de privacidade.
- ✓ Verifique os contatos do seu filho.



5. Bullying cibernético

Infelizmente, o bullying cibernético é uma realidade e está frequentemente nas notícias, com relatos de situações em que adolescentes são vítimas deste tipo de ataque. O bullying cibernético ocorre nas várias plataformas online e pode assumir diferentes formas: rumores e boatos, envio de mensagens ameaçadoras, publicação de imagens/vídeos comprometedores ou humilhantes, mensagens falsas, fazer-se passar pelo próprio, etc.

O bullying cibernético é particularmente prejudicial pela facilidade com que o ataque passa a ser do conhecimento da comunidade do atingido. Colegas, amigos, familiares, professores e até simples conhecidos assistem muitas vezes à humilhação de uma criança. Assim, a agressão pode ser espalhada pela Internet e existir de forma permanente, a menos que seja denunciada e retirada.

O ciberbullying é extremamente persistente. Se uma criança for alvo de bullying tradicional, a sua casa é mais do que nunca um lugar de refúgio. Uma vez que as plataformas digitais estão constantemente disponíveis, as vítimas do bullying cibernético têm dificuldade em encontrar alívio.

O ciberbullying é mais difícil de detetar pois há menos probabilidade de pais e professores se aperceberem de que a criança está a ser atacada online. Para além disso, **menos da metade das crianças que sofrem bullying online dizem aos pais ou a outro adulto.**

Para prevenir uma situação bullying cibernético fale com o seu filho sobre o assunto e encoraje-o a falar consigo sobre a sua atividade online. Para além disso deve estar atento ao comportamento do seu filho.

Uma série de sinais de alerta podem ser apresentados:

- ✓ Uma criança que é intimidada pode desativar a sua conta na rede social e abrir uma nova.
- ✓ Ela pode começar a evitar situações sociais, mesmo que gostasse de ser sociável no passado.
- ✓ As vítimas de bullying cibernético muitas vezes escondem o monitor ou dispositivo eletrónico (smartphone/tablet) quando outras pessoas se aproximam
- ✓ A criança torna-se reservadas sobre o que faze online.
- ✓ A criança mostra sinais de angústia ou tristeza.

6. Privacidade e segurança da informação

Como pais, estamos muito preocupados com o efeito do mundo online sobre o bem-estar emocional e físico de nossos filhos. As crianças são suscetíveis a ameaças à segurança da informação que podem causar danos financeiros. Essas são exatamente as mesmas ameaças que os adultos enfrentam: **malware e vírus, golpes de phishing e roubo de identidade**.
A questão é que as crianças são muito menos experientes e geralmente são muito mais confiantes do que os adultos. Para as crianças, compartilhar as suas informações pessoais, como seu nome completo ou onde elas vivem, pode não parecer algo importante. **Elas podem até ser enganadas por um terceiro malicioso para compartilhar as informações do seu cartão de crédito.**
Há várias formas pelas quais os hackers e ladrões podem obter informações de crianças. Jogos grátis, filmes ou até mesmo toques de telemóvel podem infetar o seu computador e roubar as suas informações.

O que deve dizer ao seu filho?

- ✓ Tenha uma conversa com o seu filho sobre as ameaças online. Certifique-se de que eles sabem identificar um ataque de phishing ou um site de jogos desonestos.
- ✓ Certifique-se de que eles mantêm todas as suas informações privadas e de que nunca publicam o seu nome completo, número de telefone, endereço ou escola que frequentam em um lugar público.
- ✓ Fale com o seu filho sobre as senhas a utilizar. Ter uma senha forte, em que se combinam letras, números e carateres especiais, é a primeira medida para evitar invasões e roubos de identidade.
- ✓ Diga a seus filhos para evitar o uso de Wi-Fi pública – esta é uma forma fácil para os hackers entrarem nos seus dispositivos.

O que pode fazer para criar um ambiente seguro:

- ✓ Instale um programa antivírus no seu computador e nos dispositivos móveis de todos os membros da família.
- ✓ Pense em instalar uma VPN ou rede privada virtual no seu computador. Uma VPN, ou rede privada virtual, criptografa a sua conexão e oculta seu endereço de IP, tornando anónima a sua navegação na Web. Assim os hackers têm mais dificuldade em aceder e roubarem as suas informações privadas.
- ✓ Instale um bloqueador de anúncios para que os seus filhos não vejam publicidade enganosa que os encoraje a instalar programas maliciosos no seu computador.

7. Visionar conteúdos inapropriados online

Como a Internet é tão aberta e pública, também é um lugar onde as crianças podem aceder a conteúdos destinados a adultos, conteúdos que elas podem achar perturbadores, confusos ou angustiantes. “Conteúdo inapropriado” pode significar muitas coisas para muitas pessoas diferentes, desde palavrões a violência, até conteúdo de teor sexual.

Não é fácil, mas, deve conversar com os seus filhos sobre o que eles podem ver online. **Muitas crianças não recorrem aos pais quando veem algo que talvez elas não devessem ter visto** por medo de que os seus pais fiquem zangados com eles e lhes tirem os seus dispositivos ou o acesso à Internet.
Se o seu filho chegar a casa com esse tipo de problema, **a melhor coisa a fazer é responder com calma e estar aberto à discussão**. Se o conteúdo em discussão for de teor sexual, o seu filho provavelmente ficará envergonhado, principalmente quando conversa com os pais sobre esse tipo de questões. Deixe-o saber que está lá para ele e disponível para responder às suas perguntas.
É aconselhável conversar com os seus filhos com honestidade e franqueza.
Muitas pesquisas mostraram que a pornografia pode ter um efeito prejudicial sobre os jovens, dando-lhes noções distorcidas e pouco saudáveis sobre o sexo. Ao mesmo tempo, é totalmente normal o seu filho revelar curiosidade sobre sexo e relacionamentos. Assim, se acontecer uma **conversa sobre o tome aproveite a oportunidade para direcionar o seu filho para uma ideia positivo sobre a sexualidade.**

Há também uma série de etapas que pode seguir para tentar evitar que os seus filhos sejam expostos a conteúdo para os quais não estejam preparados, como configurar controlos parentais. Lembre-se, porém, de que o controlo parental não substitui a comunicação aberta com o seu filho.

Converse com o seu filho:

- ✓ Deixe o seu filho saber que pode falar consigo sempre que algo o incomoda ou quando tem dúvidas sobre qualquer coisa que tenha visto online.
- ✓ Deixe-o saber que é totalmente normal ter curiosidade sobre vários temas.

Passos que você pode dar para bloquear conteúdo inapropriado:

- ✓ Defina filtros para bloquear conteúdos inadequados, como a pornografia.
- ✓ Defina o Google para o modo “Seguro” para que os seus filhos não vejam inadvertidamente conteúdo inapropriado nos resultados da pesquisa.
- ✓ Instale um bloqueador de anúncios para evitar publicidade com conteúdo inapropriado.

8. Predadores online

Na nossa última seção, demos uma olhada na ameaça online mais obscura e assustadora de todas: os predadores infantis online.
Os predadores tentam criar um relacionamento com uma criança com a intenção de abusar dela. A Internet tornou a vida muito mais fácil para os predadores infantis e **escolhem as suas vítimas através de qualquer meio online: rede social, jogos, e-mail, mensagens de texto, etc.** No entanto, o método mais comum é utilizando as salas de chat online.

Muitas vezes, o predador cria múltiplas identidades online, fingindo serem crianças para enganar as crianças e assim conseguir conversar com elas. Seguidamente descobrem o máximo possível procurando informações no perfil que a criança tem em redes sociais e no que elas dizem nas salas de chat. Estes predadores frequentemente enganam ou coagem as suas vítimas para uma atividade sexual online, via webcam ou envio de imagens sexuais. Nem sempre é fácil saber se uma criança está a ser assediada, principalmente porque a maioria mantém isso em segredo.

Há, no entanto, uma série de sinais de alerta:
A criança pode tornar-se mais secreta, porque o predador frequentemente a ameaça e lhe diz para não falar os pais ou amigos.
A criança pode tornar-se triste, introvertidas, distraída e ter mudanças de humor repentinas.

Mais uma vez o diálogo constante com o seu filho é decisivo para prevenir uma situação semelhante. É absolutamente importante que o seu filho saiba que pode contar consigo e conversar sobre qualquer assunto.

O que deve dizer ao seu filho?

- ✓ Tenha uma discussão com seu filho sobre a existência de predadores online. Certifique-se de que eles sabem que não devem conversar com estranhos nem partilhar informações.
- ✓ Diga ao seu filho que ele podem falar consigo sobre qualquer problema.

Se, por alguma razão, pensa que seu filho está em risco, procure apoio na polícia e na escola.

Conclusão

Existem muitas ferramentas para ajudá-lo a manter os seus filhos seguros online. Desde VPNs, software antivírus a filtros de Internet e controlos parentais. **Mas nada disso é realmente suficiente para ajudar a proteger o seu filho**.

Como repetimos várias vezes neste guia, a chave não é dominar um conjunto de ferramentas e técnicas complicadas. Na verdade, a maioria é muito fácil de configurar, portanto, não deixe a falta de habilidade técnica detê-lo e se necessário peça ajuda a um profissional.

A tarefa mais importante, mas também muito mais difícil, é ter **conversas frequentes, abertas e honestas com o seu filho sobre a sua vida e a sua atividade online**. Recorde-se que as empresas de Internet, as redes sociais, os provedores de jogos e de streaming podem ajudá-lo a definir limites de conteúdo, mas eles não têm necessariamente preocupações sobre a segurança do seu filho.

A melhor pessoa para manter o seu filho seguro online é você. Falar sobre como ficar seguro na Internet é um excelente canal para construir um relacionamento confiável e positivo com o seu filho.

A segurança na Internet precisa ser uma prioridade para todos os pais e cuidadores.

*Texto adaptado do artigo “O guia definitivo para proteger seu filho online em 2021”, de Ariel Hochstadt, disponível em https://pt.vpnmentor.com/blog/o-guia-completo-para-os-pais-que-querem-proteger-os-seus-filhos-na-internet/