Privacidade e Segurança Digital

Privacy & Online Security

COMUNICAR
EM SEGURANÇA

fundação MEO

O QUE É?
A Privacidade e Segurança Digital...

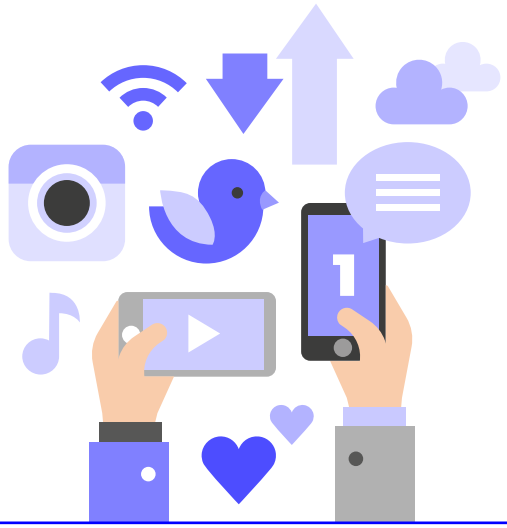
Atualmente, as crianças e os jovens privilegiam a Internet e as redes sociais para interagir. Sendo a adolescência uma fase de afirmação e construção da personalidade, a utilização da Internet permite comunicar de forma mais fácil e desenvolver um maior sentido de pertença ao permitir ter uma maior rede de contactos.

A procura por likes e seguidores pode, no entanto, levar a comportamentos de risco e à exposição excessiva. A imagem que vemos nas redes sociais é muitas vezes manipulada e pode gerar expectativas irreais.

Devem ser definidos e explicados os limites de utilização da Internet, realçando a importância da proteção dos dados pessoais, bem como evitar o contacto com pessoas desconhecidas.

A família e a escola devem promover a educação digital, ensinando as crianças e os adolescentes a usarem a Internet de forma crítica, consciente e segura. Só conhecendo as vantagens e os riscos será possível usufruir de uma experiência online positiva e benéfica para o crescimento.

SUGESTÕES



1

Comunicar... Comunicar e... Comunicar

A utilização da Internet não deve ser um tema que se deva evitar. É fundamental falar abertamente com as crianças e os adolescentes, incentivando-os a contar o que veem, o que gostam e se algum conteúdo os incomoda.

Ativar o controlo parental

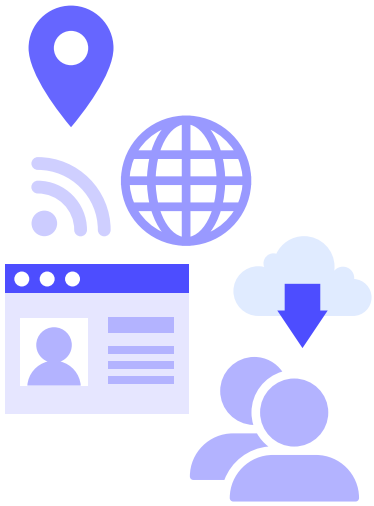
É muito importante fazer a instalação de aplicações de controlo parental, bem como criar perfis específicos para a idade do utilizador. As aplicações, como o Google Family Link, permitem a aprovação ou o bloqueio remoto a aplicações e sites, no dispositivo da criança e do adolescente, e a gestão do tempo de utilização do telemóvel/tablet.

2

3

Regras de utilização

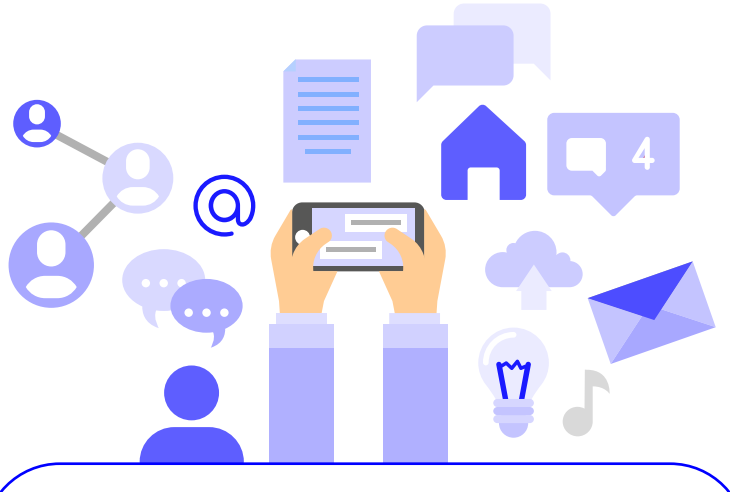
É importante definirem-se regras de utilização da Internet e dos equipamentos (ex.: tempo limite de utilização, sites que podem ser vistos ou instalação de jogos e aplicações) que devem ser partilhadas com as crianças e os adolescentes. Pode fazer-se um "contrato", com as regras de utilização, para ser assinado e que poderá ajudar na gestão de futuros conflitos.



4

Não partilhar dados pessoais

Partilhar informação privada pode parecer inofensivo, mas aumenta os riscos associados à utilização de redes sociais, jogos online e sites. Por informação privada entende-se dados pessoais como nome completo, morada (de residência ou de férias), idade, escola, fotografias e vídeos.
Para além dos dados pessoais, não devem ser partilhadas as rotinas diárias.
Nos computadores partilhados na escola recomenda-se o uso de uma ligação privada, pois não permite guardar usernames, passwords e histórico de navegação. Desta forma, futuros utilizadores do mesmo equipamento não vão ter acesso a informação privada e que não é sua.
Nas redes sociais o perfil deve ser privado porque restringe o acesso ao conteúdo, apenas a pessoas previamente aprovadas pelo utilizador. O WhatsApp tem um modo de visualização única das imagens e opções que impedem fazer o printscreen por parte de quem recebe as imagens.
Alguns jogos, como o Roblox, indicam que o nome real deve ser diferente do nome do jogador. A utilização de uma alcunha/nickname é uma boa prática a implementar.



5

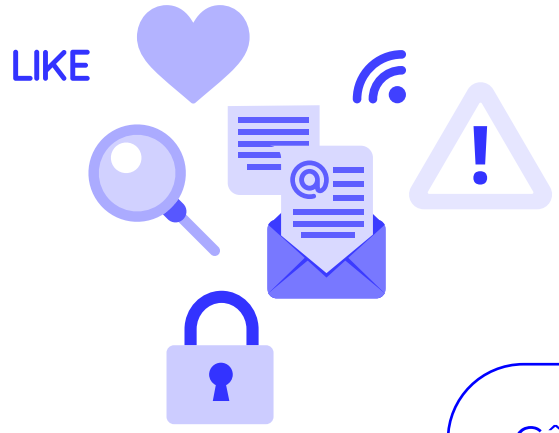
Não falar com pessoas estranhas ou desconhecidas

Conversar com estranhos online (em jogos online, redes sociais ou por emails) pode aumentar o risco de aliciamento online/grooming.

Passwords fortes

As passwords são senhas de acesso a conteúdos privados, devem ser fortes e não podem ser partilhadas. Uma password forte é aquela que é difícil de adivinhar ou decifrar por outras pessoas. Recomenda-se que sejam longas (com letras, números e caracteres especiais) e não devem conter informações pessoais.
Pode ainda ser definida, verbalmente, uma password – entre os adultos, as crianças e os adolescentes – para ser usada para confirmar a identidade de alguém, aumentando, desta forma, a segurança dos contactos efetuados.

6



7

Câmara desligada e tapada

A câmara deve estar sempre desligada e tapada. Apenas deve ser ligada se for mesmo necessária para estudar ou jogar online. Qualquer equipamento com câmara e áudio pode ser controlado por hackers e as imagens podem ser indevidamente partilhadas noutros sites. A câmara e o microfone devem ser usados apenas quando é necessário.

Verificar a idade

É importante estar atento à classificação etária definida nos jogos e nas redes sociais. Segundo a União Europeia, a idade mínima para aceder a redes sociais e serviços de mensagens é de 16 anos. Abaixo desta idade deve explicar-se as razões pelas quais não será possível ter acesso a determinado conteúdo. Podem ser recomendados sites adequados à idade (ex.: Khan Academy, Estudo em Casa, Dá a Mão à Floresta, Canal Panda, Youtube Kids ou Google Kids Space).

8

SINAIS DE ALERTA

É fundamental que os adultos estejam atentos a determinados sinais que podem indicar problemas relacionados com a **privacidade e a segurança digital** das crianças e dos adolescentes. Ao identificar esses sinais, precocemente, é possível tomar as medidas necessárias para os proteger de possíveis riscos online. Os sinais podem passar por:

1. **Mudanças repentinas de comportamento (ex.: isolamento social, alterações no padrão de sono, nervosismo, mudanças de humor frequentes e sintomas de depressão);**
2. **Relutância ou medo em mostrar o que está a fazer no telemóvel, tablet ou computador;**
3. **Partilhar online todos os momentos diários, inclusivamente com detalhe de informações pessoais ou conteúdos privados;**
4. **Atividade online suspeita (ex.: receber mensagens ou chamadas de números anónimos ou desconhecidos; criar contas em plataformas impróprias para a idade; e histórico de navegação com conteúdo inapropriado, suspeito ou sem qualquer informação);**
5. **Ansiedade, nervosismo ou angústia por não ter o telemóvel/não estar 100% do tempo conectado (nomofobia).**

COMO INICIAR O DIÁLOGO

Conversar abertamente com as crianças e os adolescentes sobre a **privacidade e segurança digital** é crucial para garantir que utilizam a Internet de forma segura e responsável.
Seguem-se algumas perguntas que poderão ajudar a iniciar o diálogo:

Que contas segues no Instagram, no TikTok e no Snapchat?

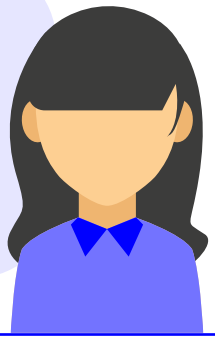
Já recebeste alguma mensagem estranha ou pedido de amizade de alguém que não conheces? O que fizeste?

Como é que defines as tuas passwords? São sempre as mesmas?

O que farias se alguém, que conheceste online, te pedisse para se encontrar contigo? E se te pedisse alguma informação pessoal?

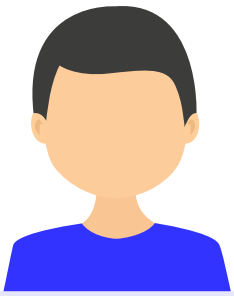
Sabes o que é um perfil falso?

Conheces alguém que já tenha partilhado fotografias ou vídeos online e que depois se tenha arrependido?



Sabes que já é possível clonar a voz e a imagem de uma pessoa?

O que farias se perdesses o teu telemóvel?



Quais são as informações que achas que é seguro partilhar online e quais é que preferes manter em privado?

Sabes identificar um site seguro? Porque é que a segurança dos sites é importante?

design gráfico: We&C

janeiro 2025

Centro Internet Segura
Esclarecimentos e Denúncias

Contacto telefónico gratuito:
800 21 90 90

Correio eletrónico:
linhainternetsegura@apav.pt

COMUNICAR
EM SEGURANÇA

fundação MEO