Cibercrime

Cybercrime

Comunicar
em Segurança

fundação MEO

O que é?
Cibercrime

O **cibercrime** é o nome dado a qualquer prática ilícita e ilegal realizada através da Internet, como roubo de dados pessoais, criação de perfis falsos, burlas online, ciberbullying e disseminação de vírus.

Uma das maiores dificuldades no combate ao cibercrime é a sua natureza transnacional. Para além de ser complicado identificar a origem e os autores do crime, o facto da legislação variar consoante o país cria lacunas na lei que podem ser exploradas por pessoas mal-intencionadas.

O pensamento crítico deve ser desenvolvido precocemente, ensinando às crianças e aos adolescentes conceitos como segurança, privacidade ou fraude, e incentivando-os a denunciar qualquer situação que os deixe desconfortáveis. Isso inclui criar passwords fortes, evitar clicar em links suspeitos, manter o antivírus atualizado e ser prudente na partilha de informações pessoais.

A melhor forma de prevenir o **cibercrime** é através da educação, num trabalho conjunto entre escola e família.

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

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.

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.

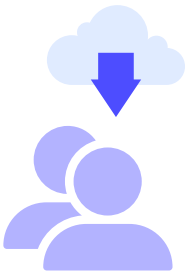
Alguns jogos, como o Roblox, indicam que o nome real deve ser diferente do nome do jogador.

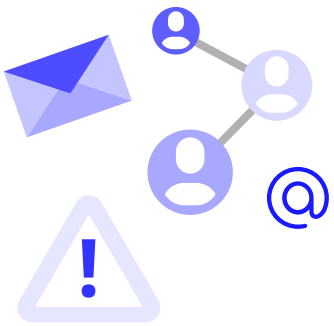
A utilização de uma alcunha/nickname é uma boa prática a implementar.

Não aceitar pessoas desconhecidas como amigos ou seguidores

Aceitar pessoas desconhecidas como amigos ou seguidores nas redes sociais pode parecer inofensivo, mas diminui a privacidade e aumenta o risco de cibercrime.

4





5

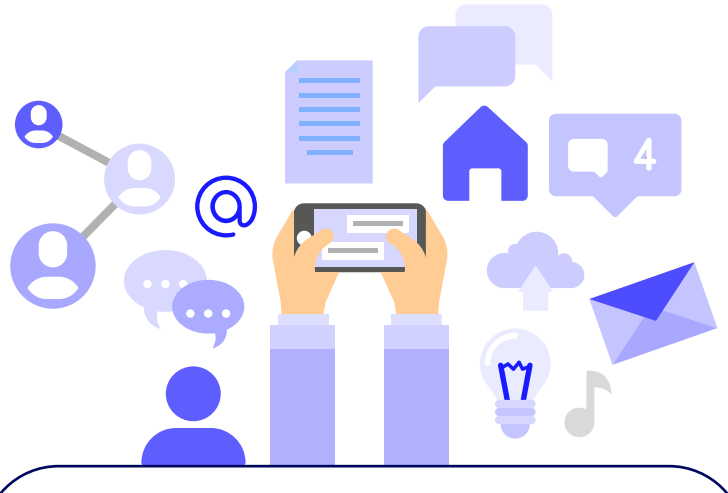
Pedir ajuda, denunciar e bloquear

As redes sociais e os jogos têm formas de denunciar situações abusivas.
Nos casos mais complicados é fundamental denunciar e apresentar provas como mensagens, imagens ou vídeos. Os pedidos de ajuda e denuncia podem ser feitos através da Linha Internet Segura 800 21 90 90 (chamada gratuita).

Instalação de antivírus

Para garantir a segurança das crianças e dos jovens é muito importante ter um antivírus instalado e atualizado nos equipamentos eletrónicos, para que não sejam descarregados jogos com malware.
Devem ser sempre utilizadas fontes oficiais e seguras, como o Google Play Store (Android) ou a App Store (iOS).

6



7

Ter atenção às compras online

Muitos jogos têm conteúdos gratuitos e outros pagos (ex.: acessórios, emogis ou opções para passar de nível de dificuldade).
Os cartões de crédito devem ser sempre controlados por um adulto, que pode criar cartões virtuais, de utilização única, para serem utilizados nestes casos. Antes de se efetuar um pagamento deve sempre ser feita a validação se o site é credível e seguro (ex.: https, cadeado).

Prevenir situações de phising

Deve-se verificar a origem/remetente do email, se existem erros ortográficos e ter atenção a links ou anexos suspeitos.

8

Sinais de Alerta

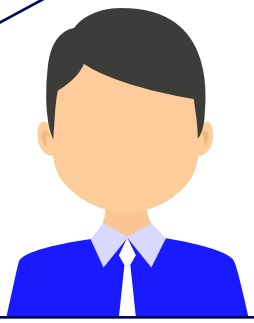
A era digital trouxe consigo inúmeros benefícios, mas também expôs as crianças e os adolescentes a novos riscos como o **cibercrime**. É fundamental que os adultos estejam atentos a alguns sinais que podem indicar que os menores estão a ser alvo de atividades online maliciosas. Os sinais podem passar 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. **Atividade online suspeita (ex.: receber mensagens ou chamadas de números anónimos ou desconhecidos; criar contas em plataformas impróprias para a idade; ou histórico de navegação com conteúdo inapropriado, suspeito ou sem qualquer informação);**
4. **Dificuldade em explicar despesas ou utilização de cartões bancários sem autorização;**
5. **Ansiedade, nervosismo ou angústia por não ter o telemóvel/não estar 100% do tempo conectado (nomofobia).**

Como Iniciar o Diálogo

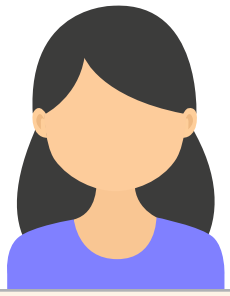
O mundo digital oferece inúmeras vantagens, mas também expõe as crianças e os adolescentes a riscos. Conversar abertamente sobre **cibercrime** é fundamental para que tenham as ferramentas necessárias para navegar na Internet de forma segura. Segue-se um conjunto de perguntas que podem ajudar a iniciar a conversa:

Já ouviste falar em cibercrime? O que é que achas que isso significa?



Na tua opinião, quais são os maiores perigos associados à Internet?

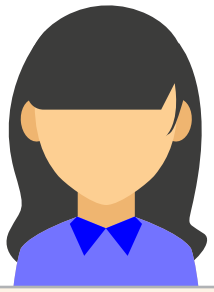
O que vais fazer se alguém que conheceste na Internet te pedir informações pessoais, como a tua morada ou o teu número de telefone?



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

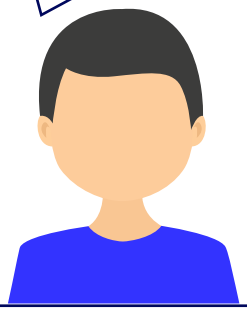
Sabes o que significa phishing?
E smishing, vishing ou quishing?

Como é que podes proteger
o teu telemóvel, tablet
ou computador de um vírus?



Já partilhaste alguma password
com alguém? Porquê?
E o que é que fizeste de seguida?

Se perderes ou se te roubarem
o telemóvel, o que é que podes fazer
para proteger os teus dados?



Se perceberes que estão a utilizar
indevidamente informação pessoal
tua, sabes o que é que deves fazer?

Conheces algum youtuber
ou influencer que fala sobre
segurança na Internet?

abril 2025

Centro Internet Segura
Esclarecimentos e Denúncias

Contacto telefónico gratuito:
800 21 90 90

Correio eletrónico:
linhainternetsegura@apav.pt

Comunicar em Segurança

fundação MEO