Plataformas de Ensino Digital

e-Learning Platforms

Comunicar em Segurança

fundação MEO

O que são? Plataformas de Ensino Digital

A tecnologia está a transformar a educação. As **plataformas de ensino digital** são espaços que permitem aos alunos aprender e interagir através da Internet. Estas ferramentas oferecem acesso a conteúdos pedagógicos como vídeos, exercícios interativos e até aulas ao vivo.

As **plataformas de ensino digital** permitem desenvolver competências técnicas e comportamentais (pesquisa, autonomia e pensamento crítico) a partir de qualquer lugar com ligação à Internet. É importante estabelecer limites e acompanhar as atividades online das crianças e dos adolescentes. Os adultos devem estar atentos aos riscos associados, nomeadamente no isolamento social, na segurança e na privacidade online.

O apoio dos adultos é essencial para garantir que as **plataformas de ensino digital** sejam utilizadas de forma segura e educativa, sendo este tema uma excelente oportunidade para conversar sobre os benefícios e riscos da Internet.

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.

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.

2

3

Controlar chats e áudios

A gestão das aulas ou trabalhos de grupo pode ser dificultada quando os microfones dos participantes estão ligados ou quando não existe moderação no chat. As plataformas podem ser configuradas para que esta situação não aconteça. A restrição de partilha de mensagens em grupos maiores pode ser uma mais-valia para impedir a difusão de conteúdos maliciosos. O organizador da sessão virtual é o responsável pela gestão destas opções.

Senhas de acesso às sessões

Existem algumas formas de aumentar a segurança nas plataformas digitais. Pode ser definida uma password de acesso à sessão online e estabelecer que apenas os utilizadores aprovados pelo anfitrião podem ingressar na mesma.

4

5

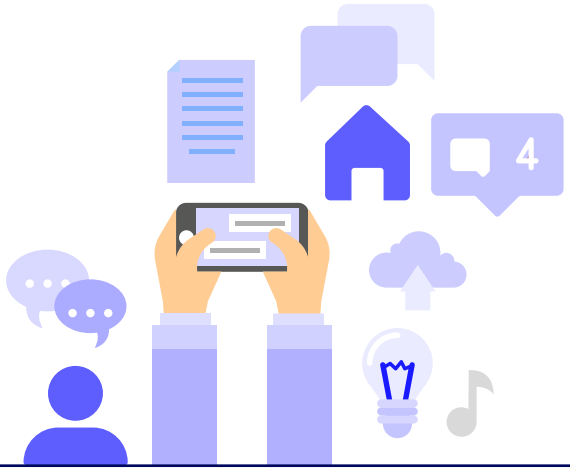
Pedir ajuda, denunciar e bloquear

As plataformas de ensino digital têm formas de denunciar situações abusivas.
Em 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, para que não sejam descarregadas aplicações com malware. Devem ser sempre utilizadas fontes oficiais e seguras, como o Google Play Store (Android) ou a App Store (iOS).

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.

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

Nos últimos anos o uso de **plataformas de ensino digital** tornou-se cada vez mais comum, com impactos positivos para a educação. No entanto, é importante que os adultos estejam atentos a alguns sinais que podem indicar que as crianças e os adolescentes podem estar a ser vítimas de alguma forma de abuso ou exploração nessas plataformas. Os sinais podem passar por:

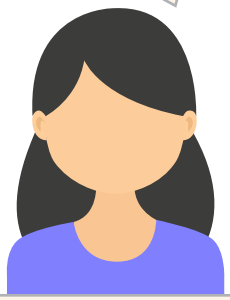
1. **Mudanças repentinas de comportamento (ex.: isolamento social, alterações no padrão de sono, nervosismo, mudanças de humor frequentes, sintomas de depressão e ansiedade);**
2. **Atividade online suspeita (ex.: receber mensagens ou chamadas de números anónimos ou desconhecidos; criar contas em plataformas desconhecidas ou impróprias para a idade; e histórico de navegação com conteúdo inapropriado, suspeito ou sem qualquer informação);**
3. **Comportamentos online preocupantes (ex.: partilha de notícias falsas, linguagem online mais agressiva, discurso de ódio ou criação de perfis falsos);**
4. **Sinais físicos visíveis (ex.: hematomas ou feridas sem explicação, comportamentos autolesivos, choro fácil e descontextualizado);**
5. **Incapacidade de tomar decisões (pode tornar os menores em alvos mais fáceis de manipular e a serem facilmente identificados por ideologias extremistas).**

Como Iniciar o Diálogo

A digitalização do ensino trouxe inúmeras vantagens, mas também novos desafios. A segurança online tornou-se uma prioridade, especialmente quando se trata da proteção de dados pessoais partilhados em **plataformas de ensino digital**. Seguem-se 10 questões que podem ajudar a abordar o tema:

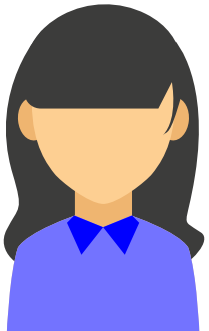
O que é que mais gostas de fazer quando estudas online?

Quais são as plataformas de ensino digital que costumas usar?



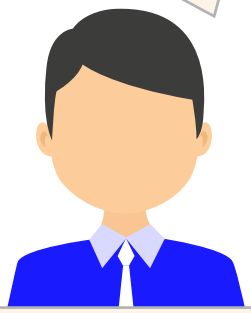
Costumas interagir com os teus colegas através da plataforma de ensino digital? De que forma?

O que farias se recebesses uma mensagem, de alguém que não conheces, a convidar-te para conversar noutra plataforma?



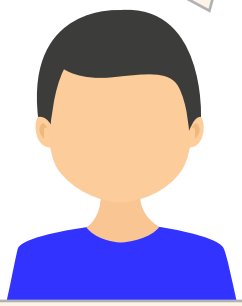
Tens ideia quanto tempo é que passas à frente do computador/tablet?

Sabes o que é assédio digital/cyberbullying e como é que te podes proteger?



Quais são os cuidados que tens para proteger as tuas informações pessoais online?

Sabes o que é uma password forte?



O que farias se percebesses que alguém estava a ter acesso às tuas contas online?

Sabes a quem é que podes pedir ajuda se te sentires inseguro ou com medo?

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