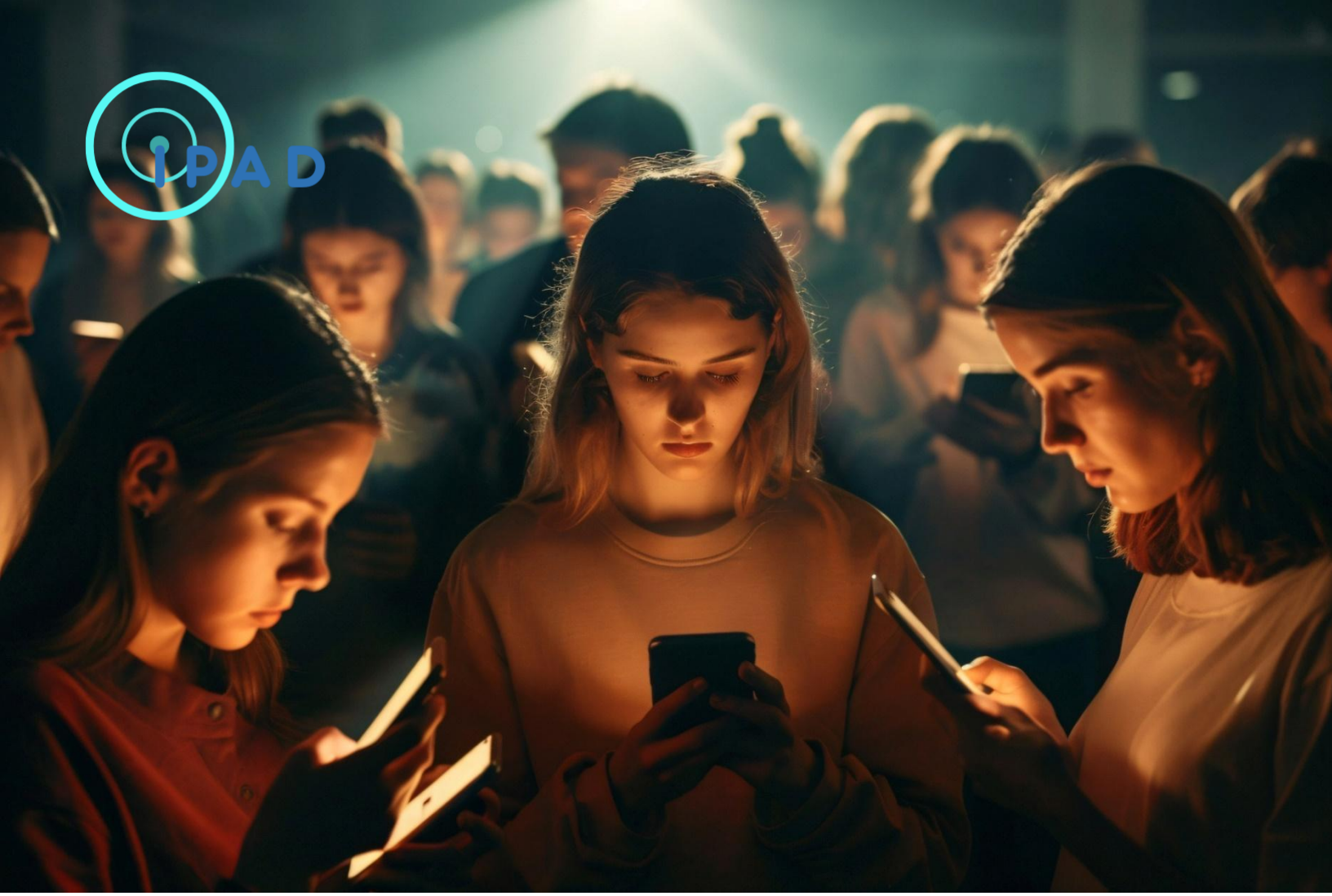

Atividades práticas

Financiado pela União Europeia. Os pontos de vista e as opiniões expressas são as do(s) autor(es) e não refletem necessariamente a posição da União Europeia ou da Agência de Execução Europeia da Educação e da Cultura (EACEA). Nem a União Europeia nem a EACEA podem ser tidos como responsáveis por essas opiniões.
Projeto número 2023-1-ES01-KA220-ADU-000152665

Cofinanciado pela União Europeia

ÍNDICE

INTRODUÇÃO

A **Plataforma de aprendizagem e recursos formativos** foi desenvolvida como um recurso abrangente para **formadores de adultos que trabalham com famílias** no domínio da **educação digital, da literacia das redes sociais e da segurança na Internet**. Este documento integra um conjunto de **atividades de formação inovadoras,** concebidas para melhorar as competências digitais dos adultos, dotando-os dos conhecimentos necessários para navegarem no mundo online de forma segura e responsável.

Este guia sistematiza **atividades práticas e ferramentas de avaliação** desenvolvidas em colaboração pelos parceiros do projeto no âmbito do **IPAD Currículo de formação**. As atividades estão estruturadas em seis unidades-chave, abordando cada uma um aspeto fundamental da li**teracia nas redes sociais e da segurança na Internet para as famílias e os seus filhos**. Disponibilizam aos formadores exercícios prontos a utilizar, metodologias envolventes e estratégias de avaliação para **avaliar o progresso da aprendizagem** e **adaptar as abordagens de ensino com base nas necessidades dos participantes**.

Estrutura do documento

Cada unidade deste guia está estruturada da seguinte forma:

1. **Objetivos de aprendizagem**: descrição dos objetivos relacionados com a unidade e respetivos resultados de aprendizagem
2. **Descrição**: instruções passo a passo sobre como realizar a atividade, incluindo a respetiva duração, preparação prévia, descrição do processo (diferentes etapas) e recomendações metodológicas, se aplicável
3. **Recursos úteis**: ligações para informações adicionais, orientações pedagógicas, estudos de investigação, regulamentos e ferramentas que apoiem a implementação da atividade
4. **Material necessário**: lista dos recursos necessários, tais como computadores, acesso à Internet, aplicações ou outros materiais. Quando necessário, são incluídas fichas de atividade, modelos e imagens
5. **Ferramentas de avaliação**: estratégias para avaliar o impacte da atividade no progresso da aprendizagem dos participantes. Estas ferramentas incluem uma avaliação qualitativa: (observação dos participantes, debates, relatórios, demonstrações e avaliações baseadas em tarefas) e uma avaliação quantitativa (perguntas de escolha múltipla, exercícios de correspondência, afirmações de verdadeiro/falso, atividades de preenchimento de espaços em branco e listas de verificação)

Público-alvo

Este guia destina-se principalmente a **formadores de adultos e facilitadores** que trabalham com famílias para **promover um envolvimento digital seguro e responsável**. Serve como um conjunto de ferramentas práticas para orientar debates sobre **pensamento crítico, cibersegurança, privacidade online, netiqueta e mediação parental**. Ao utilizar estes materiais, os formadores podem capacitar os adultos para **compreenderem os riscos digitais, apoiarem as experiências online dos seus filhos e desenvolverem uma cultura de cidadania digital responsável**.

Como utilizar este documento

Ao integrar a **Base de Dados Digital Online, as Bases Teóricas e Pedagógicas e o Curso *b-Learning***, a **Plataforma de aprendizagem e recursos formativos** disponibiliza um **ecossistema abrangente de recursos educativos**. Os educadores podem utilizar estas ferramentas **individualmente ou em combinação** para criar **experiências de aprendizagem envolventes e eficazes** para adultos e famílias.

Os formadores podem desenvolver atividades práticas, como exercícios autónomos, ou integrá-las em **sessões de formação estruturadas**. As ferramentas de avaliação fornecidas podem ser utilizadas para **acompanhar os progressos dos formandos** e **adaptar as atividades** com base nos seus níveis de literacia digital. Quer seja utilizado em **contextos formativos formais ou informais**, este documento disponibiliza uma **abordagem** flexível e **com impacte para reforçar as competências digitais** das famílias.

UNIDADE 1.

MELHORAR A LITERACIA NAS REDES SOCIAIS E O PENSAMENTO CRÍTICO

1.1. Desafio de verificação de factos - detetar a desinformação

1. Objetivos de aprendizagem

1. Aplicar estratégias de pensamento crítico para avaliar a credibilidade e fiabilidade das fontes online
2. Identificar preconceitos, desinformação e notícias falsas, utilizando estratégias de verificação
3. Desenvolver a autonomia na promoção de uma atitude crítica em relação à informação online

2. Descrição

DURAÇÃO: 60 minutos

PREPARAÇÃO:

Reunir uma seleção de artigos de notícias online, publicações nas redes sociais e anúncios reais e falsos.

Preparar uma ficha de trabalho de verificação de factos que inclua perguntas-chave sobre credibilidade, fontes e parcialidade.

Assegurar o acesso a ferramentas de verificação de factos (por exemplo, Snopes, FactCheck.org, Google Reverse Image Search).

DESCRIÇÃO DO PROCESSO:

Etapa 1: Introdução (10 minutos):

Explique sucintamente a importância do pensamento crítico na literacia digital. Introduza táticas de desinformação comuns (clickbait, deepfakes, estatísticas enganosas).

Etapa 2: Atividade de grupo (30 minutos):

Divida os participantes em pequenos grupos. Entregue a cada grupo uma mistura de notícias verdadeiras e falsas

www.docs.google.com/document/d/1Xz2wC5Re3D5S3nT-rjxxn-IwKBaqWe0B/edit

Peça que analisem os artigos utilizando a ficha de trabalho de verificação de factos, verificando as fontes, os URL e utilizando ferramentas de verificação de factos.

www.docs.google.com/document/d/1LBF2j8UZZk1ANKBlUgOi-s4-syqgdb5N/edit

Os grupos apresentam as suas conclusões e justificam as suas decisões.

Etapa 3: Debate e reflexão (20 minutos):

Promova um debate sobre os desafios encontrados. Saliente a importância da verificação dos factos antes de partilhar conteúdos.

RECOMENDAÇÕES METODOLÓGICAS:

- Incentivar os participantes a **justificarem o seu raciocínio,** em vez de se limitarem a adivinhar
- Utilizar **exemplos reais** para tornar a atividade cativante
- Promover a **colaboração e o debate em equipa**

3. Recursos úteis

Snopes - Site de verificação de factos

FactCheck.org - Verificação de notícias políticas

Pesquisa inversa de imagens do Google - Identificar imagens manipuladas

4. Material necessário

- Amostras de notícias impressas ou digitais
  www.docs.google.com/document/d/1Xz2wC5Re3D5S3nT-rjxxn-IwKBaqWeoB/edit
- Ficha de trabalho de verificação de factos
  www.docs.google.com/document/d/1LBF2j8UZZk1ANKBlUgOi-s4-syqgdb5N/edit
- Dispositivos ligados à Internet para verificação

5. Ferramentas de avaliação

Ferramenta de avaliação 1: Lista de controlo de autoavaliação

Os participantes avaliam a sua capacidade de identificar notícias falsas.

Ferramenta de avaliação 2: *Feedback* do debate em grupo

Avaliação do raciocínio e da argumentação.

Ferramenta de avaliação 3: Teste de escolha múltipla sobre indicadores de desinformação

Pode encontrar as Ferramentas de Avaliação no IPAD Currículo de formação

ANEXO I: Exemplos de notícias reais e falsas

NOTÍCIAS REAIS

1. A NASA Confirma a Existência de Água na Lua (2020)

📌 **Título:** NASA Confirma a Existência de Água na Superfície Visível da Lua

🔗 **Fonte:** NASA, Revistas Científicas

📰 **Resumo:** Em 2020, a NASA confirmou a presença de moléculas de água na superfície visível da Lua, utilizando o telescópio SOFIA. Esta descoberta tem implicações para futuras explorações lunares.

✅ **Por que é real?** Publicada por uma organização científica credível (NASA), verificada por múltiplas fontes reputadas e apoiada por investigação científica.

2. A OMS Declara a COVID-19 uma Pandemia Global (2020)

📌 **Título:** Organização Mundial da Saúde Declara a COVID-19 uma Pandemia Global

🔗 **Fonte:** Organização Mundial da Saúde (OMS), CDC, Websites Governamentais

📰 **Resumo:** A 11 de março de 2020, a OMS declarou oficialmente a COVID-19 como pandemia devido à sua rápida propagação global, instando os países a adotarem medidas de saúde pública.

✅ **Por que é real?** Relatada por grandes organizações de saúde e agências de notícias, amplamente documentada com dados oficiais.

3. O Telescópio James Webb Capta as Primeiras Imagens de Galáxias Distantes (2022)

📌 **Título:** Telescópio Espacial James Webb Envia as Primeiras Imagens Deslumbrantes do Universo

🔗 **Fonte:** NASA, BBC, National Geographic

📰 **Resumo:** Em julho de 2022, a NASA divulgou as primeiras imagens a cores captadas pelo Telescópio Espacial James Webb, revelando as vistas mais profundas e detalhadas do universo até à data.

✅ **Por que é real?** Verificada pela NASA e por pesquisas científicas revistas por pares, amplamente divulgada por organizações noticiosas de confiança.

NOTÍCIAS FALSAS

1. Bill Gates Planeia Implantar Microchips nas Vacinas da COVID-19

📌 **Título:** Bill Gates admite que as vacinas da COVID-19 implantarão microchips de rastreio nas Pessoas
🔗 **Fonte:** Publicações Virais nas Redes Sociais, Blogues de Conspiração
📰 **Resumo:** Uma alegação amplamente difundida afirmava que Bill Gates e a OMS planeavam utilizar as vacinas da COVID-19 para implantar microchips de rastreio nos seres humanos.
❌ **Por que é falsa?**

- ✓ Não há qualquer evidência científica que apoie esta alegação
- ✓ Mal-entendido sobre o financiamento de Gates para a investigação em vacinas
- ✓ Rejeitada por organizações de saúde (OMS, CDC)
- ✓ Desmentida por Snopes e Reuters

2. 5G Causa Sintomas da COVID-19

📌 **Título:** Novo estudo prova que as redes 5G são a verdadeira causa da COVID-19
🔗 **Fonte:** Websites Marginais, Publicações Virais nas Redes Sociais
📰 **Resumo:** Alguns teóricos da conspiração alegaram que a tecnologia 5G, e não um vírus, era a verdadeira causa dos sintomas da COVID-19.
❌ **Por que é falsa?**

- ✓ A COVID-19 é causada pelo vírus SARS-CoV-2, confirmado por organizações de saúde globais
- ✓ O 5G é uma tecnologia de comunicação sem fios sem impacte biológico no sistema imunitário
- ✓ Desmentida pela OMS, CDC e cientistas independentes

3. O Governo Vai Proibir o Dinheiro Físico e Obrigará Todos a Usar Moeda Digital

📌 **Título:** Governo dos EUA anuncia que o dinheiro físico será banido até 2025 e que todos terão de usar moeda digital
🔗 **Fonte:** Websites Sensacionalistas, Blogues de Desinformação
📰 **Resumo:** Publicações virais nas redes sociais alegavam, sem fundamento, que os governos planeavam eliminar completamente o dinheiro físico e forçar os cidadãos a utilizar apenas transações digitais.
❌ **Por que é falsa?**

- ✓ Nenhuma declaração oficial do governo ou de instituições financeiras confirma esta alegação
- ✓ As economias continuam a depender de moeda física
- ✓ Desmentida por reguladores financeiros

ANEXO II: Exemplo de ficha de verificação de factos

1. Informações Básicas

- ✓ Título da notícia: _____
- ✓ Fonte/Website: _____
- ✓ Data de publicação: _____
- ✓ Autor (se disponível): _____

2. Avaliação da Fonte

✅ **Verifique a credibilidade da fonte**

Pergunta	Sim	Não	Notas/Justificação
A fonte é uma organização conhecida e reputada (por exemplo, BBC, Reuters, OMS, NASA)?	☐	☐	
O URL do website parece legítimo (por exemplo, .gov, .edu, .org, grandes meios de comunicação)?	☐	☐	
É possível encontrar a mesma história relatada por várias fontes fiáveis?	☐	☐	
O website tem uma página clara de "Sobre Nós" ou uma página de contacto?	☐	☐	

🔍 **Verifique através da utilização de websites de verificação de factos:**

- ➢ Snopes
- ➢ FactCheck.org
- ➢ Reuters Fact Check
- ➢ Pesquisa inversa de imagens do Google

3. Análise do Conteúdo e da Linguagem

✅ **Analise a forma como o artigo está escrito**

Pergunta	Sim	Não	Notas/Justificação
O título utiliza linguagem sensacionalista ou emocionalmente carregada?	☐	☐	
Existem afirmações chocantes sem provas que as sustentem?	☐	☐	
O artigo baseia-se em fontes anónimas ou carece de credenciais do autor?	☐	☐	
São apresentados dados/estatísticas? Se sim, são citados a partir de fontes fiáveis?	☐	☐	
O artigo inclui imagens manipuladas, gráficos enganosos ou *deepfakes*?	☐	☐	

4. Processo de Verificação de Factos

✅ **Utilize estratégias de verificação para confirmar ou desmentir a alegação**

Pergunta	Sim	Não	Notas/Justificação
Realizou uma pesquisa no Google para verificar se há artigos semelhantes em fontes fiáveis?	☐	☐	
Utilizou a Pesquisa Inversa de Imagens do Google para verificar as imagens?	☐	☐	
O artigo fornece *links* para fontes credíveis (estudos científicos, relatórios oficiais)?	☐	☐	

5. Veredicto Final

Com base na verificação de factos, considera que esta notícia é:

☐ Real (credível e verificada)
☐ Falsa (enganadora, carece de credibilidade)
☐ Inconclusiva (necessita de mais verificação)

📢 **Explique o seu raciocínio:**

_____

_____

_____

_____

6. Perguntas para Reflexão

1. Quais foram os principais sinais de alerta que indicaram que a notícia era falsa ou credível?

   _____

2. De que forma as ferramentas de verificação de factos ajudaram na validação da notícia?

   _____

3. Porque é importante verificar os factos antes de partilhar conteúdos online?

   _____

1.2. Análise do conteúdo das redes sociais - conteúdo digital seguro *versus* prejudicial

1. Objetivos de aprendizagem

1. Distinguir entre conteúdos digitais educativos e nocivos para menores
2. Identificar as táticas publicitárias e os seus efeitos nas crianças e nos adolescentes
3. Promover um comportamento responsável na partilha de conteúdos em espaços online

2. Descrição

DURAÇÃO: 60 minutos

PREPARAÇÃO:

Recolha capturas de ecrã de **conteúdos das redes sociais** (publicações educativas, anúncios dirigidos a crianças, conteúdos nocivos ou enganadores). Prepare uma folha de **critérios de avaliação** abrangendo:

- **Adequação à idade**
- **Fiabilidade das fontes**
- **Impacte emocional e intenção**

Assegure o acesso a **plataformas de redes sociais** para análise em direto.

DESCRIÇÃO DO PROCESSO:

Etapa 1: Introdução (10 minutos):

Explique **de que forma as redes sociais influenciam as perceções e os comportamentos.** Debata técnicas publicitárias comuns e o seu impacte nos jovens.

Etapa 2: Análise de grupo (30 minutos):

Divida os participantes em pequenos grupos. Apresente diferentes exemplos de **conteúdos nas redes sociais** (educativos, enganosos, publicidade direcionada, conteúdos violentos ou inapropriados).

Os grupos utilizam a **Ficha de Critérios de Avaliação** para avaliar a segurança dos conteúdos. Cada grupo apresenta os resultados e justifica as suas classificações.

Etapa 3: Debate e reflexão (20 minutos):

Compare perspetivas e debater **as razões pelas quais um conteúdo pode ser enganador ou prejudicial.** Desenvolva **orientações para formadores e famílias** sobre a identificação de conteúdos digitais seguros.

RECOMENDAÇÕES METODOLÓGICAS:

- Incentive os participantes a **refletir sobre a manipulação emocional** nos anúncios publicitários
- Utilize exemplos reais para melhorar o envolvimento
- Promova um **debate** aberto **sobre questões éticas** na criação de conteúdos digitais

3. Recursos úteis

Common Sense Media - Avaliar os conteúdos digitais para crianças

MediaSmarts - Recursos de literacia digital

Descodificador de anúncios - Compreender as técnicas de publicidade

4. Material necessário

- Capturas de ecrã de **conteúdos variados das redes sociais**
- **Ficha de Critérios de Avaliação**
- Dispositivos ligados à Internet para revisão de conteúdos em direto

5. Ferramentas de avaliação

Ferramenta de avaliação 1: Avaliação por lista de controlo

Os participantes avaliam a adequação do conteúdo utilizando critérios definidos.

Ferramenta de avaliação 2: Debate baseado em cenários

Os grupos discutem casos reais de conteúdos enganosos.

Ferramenta de avaliação 3: Breve reflexão escrita

Os participantes resumem **as principais conclusões** sobre a literacia nas redes sociais.

Pode encontrar as Ferramentas de Avaliação no IPAD Currículo de formação

UNIDADE 2.

FUNDAMENTOS DA CIBERSEGURANÇA E MEDIDAS DE SEGURANÇA NA INTERNET

2.1. *Workshop* sobre os princípios básicos da cibersegurança para educadores de adultos

1. Objetivos de aprendizagem

1. Compreender os conceitos fundamentais de cibersegurança e por que razão são essenciais para a segurança pessoal e familiar online
2. Reconhecer e identificar ameaças cibernéticas comuns, como *phishing*, *malware* e *ransomware* e o seu potencial impacte
3. Aprender as melhores práticas para um comportamento seguro online, incluindo a criação de palavras-passe fortes e a deteção de tentativas de *phishing*
4. Capacitar os formadores para orientarem os formandos na adoção de práticas seguras online e na proteção de dados sensíveis

2. Descrição

DURAÇÃO: 60 minutos

PREPARAÇÃO:

Preparar um conjunto de exemplos de emails de *phishing*, ligações e anexos suspeitos para demonstração.

Configurar dispositivos com acesso à Internet e exemplos de definições de segurança em plataformas como o email e as redes sociais.

Fornecer aos participantes guias sobre gestão de palavras-passe, deteção de *phishing* e definições de segurança.

DESCRIÇÃO DO PROCESSO:

Etapa 1: Introdução às ciberameaças (15 minutos):

Comece com uma visão geral das ameaças cibernéticas comuns (por exemplo, *phishing, malware, ransomware*, engenharia social) e como estas afetam os indivíduos e as famílias. Discuta a importância das noções básicas de cibersegurança, incluindo os conceitos de pegadas digitais e comportamento seguro online.

Etapa 2: Reconhecer o *phishing* e outras ameaças (20 minutos):

Mostre exemplos de emails e mensagens de *phishing*. Oriente os participantes na deteção de sinais de alerta comuns (por exemplo, URL suspeitos, linguagem urgente, pedidos de informações pessoais). Use um teste de *phishing* simulado para permitir que os participantes pratiquem a identificação de ameaças potenciais num ambiente controlado.

Etapa 3: Configuração das definições de segurança (25 minutos):

Oriente os participantes na configuração de medidas básicas de segurança nos seus dispositivos. Inclui:

- Ajustar as definições de privacidade e segurança nas contas das redes sociais
- Demonstrar a configuração da autenticação de dois fatores
- Rever as definições do software antivírus e da proteção por *firewall*. Incentive os participantes a aplicarem estas definições nos seus próprios dispositivos e a fazerem perguntas sobre funcionalidades de segurança específicas.

Etapa 4: Reflexão e perguntas e respostas (10 minutos):

Dinamize um debate sobre os desafios comuns de cibersegurança enfrentados por famílias e indivíduos. Peça aos participantes que partilhem como planeiam integrar estas práticas de segurança nas rotinas diárias. Responda a quaisquer perguntas restantes e forneça orientações sobre outros recursos de cibersegurança.

RECOMENDAÇÕES METODOLÓGICAS:

- **Utilizar simulações interativas**: crie um ambiente seguro para simular a deteção de *phishing* e a configuração da segurança
- **Simplificar as explicações técnicas**: evite os jargões, utilizando exemplos do quotidiano para explicar os conceitos de cibersegurança
- **Incentivar a aplicação prática**: assegure-se de que os participantes podem acompanhar o processo nos seus dispositivos para ganhar confiança

3. Recursos úteis

Guia de deteção de phishing - Um guia ilustrado sobre como identificar tentativas de *phishing*.

www.consumer.ftc.gov/articles/how-recognize-and-avoid-phishing-scams

Tutorial em vídeo sobre a autenticação de dois fatores - Um pequeno vídeo sobre a configuração da autenticação de dois fatores nas redes sociais.

www.youtube.com/watch?v=9T66xFMsUxo

Recurso familiar de segurança online - Um recurso da ConnectSafely que disponibiliza dicas de segurança digital e privacidade adaptadas à utilização familiar, abrangendo tópicos desde a segurança das palavras-passe a práticas de navegação seguras.

www.connectsafely.org/safety-tips-advice/

4. Material necessário

- Dispositivos com acesso à Internet (computadores portáteis ou *tablets*)
- Exemplos de mensagens e mensagens de *phishing*
- Guias impressos sobre práticas básicas de cibersegurança

5. Ferramentas de avaliação

Ferramenta de avaliação 1: Teste de conhecimentos sobre cibersegurança

Os participantes responderam a um pequeno questionário para testar a sua compreensão dos principais conceitos de cibersegurança, incluindo a identificação de tentativas de *phishing* e a configuração de definições de segurança.

Ferramenta de avaliação 2: Ficha de reflexão sobre cibersegurança

Os participantes refletem sobre a sua aprendizagem identificando duas ciberameaças, descrevendo uma configuração de segurança que aplicaram e enumerando um novo hábito de cibersegurança que planeiam adotar.

Ferramenta de avaliação 3: Inquérito sobre o *feedback* e a confiança do *workshop*

Os participantes fornecem *feedback* sobre o *workshop* e classificam a sua confiança na gestão de ameaças à cibersegurança e na orientação de outros.

Pode encontrar as Ferramentas de Avaliação no IPAD Currículo de formação

2.2. *Workshop* sobre cibersegurança

1. Objetivos de aprendizagem

1. Identificar e analisar as principais caraterísticas das tentativas de *phishing*, *malware* e outras ameaças online
2. Demonstrar medidas práticas para atenuar os riscos de cibersegurança, como ativar a autenticação de dois fatores e atualizar as definições de privacidade
3. Aplicar o pensamento crítico para resolver desafios de cibersegurança reais mediante cenários
4. Dotar os formadores das competências necessárias para ensinar as famílias e as comunidades a reconhecer e a reagir às ameaças online

2. Descrição

DURAÇÃO: 90 minutos

PREPARAÇÃO:

Prepare estudos de casos ou cenários que realcem desafios comuns de cibersegurança, como emails de *phishing*, palavras-passe fracas ou software desatualizado e imprima materiais que descrevam as melhores práticas para as definições de segurança e a criação de palavras-passe; além disso, assegure-se de que estão disponíveis dispositivos com acesso à Internet para atividades práticas.

DESCRIÇÃO DO PROCESSO:

Etapa 1: Introdução (15 minutos):

Apresente os fundamentos da cibersegurança, as ciberameaças comuns como o *phishing*, o *ransomware* e a engenharia social, bem como as melhores práticas para criar palavras-passe fortes e proteger as contas online.

Etapa 2: Dramatização de cenários (40 minutos):

Divida os participantes em pequenos grupos e atribua a cada um cenário, como um e-mail suspeito de um remetente desconhecido, um aviso de *pop-up* sobre *malware* ou uma violação de dados numa escola ou local de trabalho. Os grupos irão desempenhar o papel de formadores de cibersegurança, decidindo como identificar, mitigar e explicar os riscos envolvidos a um público não especializado. Incentive os participantes a aplicar as ferramentas e práticas que aprenderam, incluindo a identificação de elementos de *phishing* numa mensagem de email, a demonstração de como atualizar as definições de segurança ou instalar software antivírus e a explicação da gestão de palavras-passe utilizando aplicações ou técnicas como a autenticação de dois fatores.

Etapa 3: Partilha e *feedback* (20 minutos):

Cada grupo apresenta o seu cenário e a sua solução aos restantes participantes, enquanto o facilitador dá *feedback* construtivo e esclarece quaisquer dúvidas.

Etapa 4: Reflexão e conclusão (15 minutos):

Conduza um debate sobre como os participantes podem implementar estas soluções na realidade, centrando-se na sensibilização da comunidade e na orientação das famílias.

RECOMENDAÇÕES METODOLÓGICAS:

- Focar nas **aplicações práticas** dos conhecimentos e competências em matéria de cibersegurança para garantir a sua relevância para a vida quotidiana dos participantes
- Utilizar métodos **de aprendizagem ativa** (por exemplo, dramatização) para tornar o conteúdo cativante e memorável
- Incluir **cenários relacionados com as famílias**, refletindo como os formadores de formandos ensinarão os outros

3. Recursos úteis

Guias online:

Mantenha-se seguro online - Conselhos de segurança na Internet

www.staysafeonline.org/

Cyber Aware - Noções básicas de cibersegurança

www.ncsc.gov.uk/cyberaware

FTC - Evitar burlas e fraudes

www.consumer.ftc.gov/

4. Material necessário

- Dispositivos com acesso à Internet (computadores portáteis ou *tablets*).
- Guias impressos ou digitais sobre práticas de cibersegurança, incluindo gestão de palavras-passe e definições de privacidade.
- Quadro branco ou *flipchart* para discussões em grupo e apresentações.

5. Ferramentas de avaliação

Ferramenta de avaliação 1: Teste de conhecimentos sobre cibersegurança

Um questionário que teste a capacidade dos participantes para reconhecer emails de *phishing*, compreender a autenticação de dois fatores e identificar as melhores práticas de cibersegurança.

Instrumento de avaliação 2: Teste de aplicação da cibersegurança

Os participantes respondem a perguntas para demonstrar os seus conhecimentos sobre a aplicação de medidas práticas de cibersegurança, como a ativação da autenticação de dois fatores e a gestão das definições de privacidade.

Ferramenta de avaliação 3: Ficha de reflexão sobre cibersegurança

Os participantes documentam as suas ideias, enumerando as práticas de cibersegurança que aprenderam, descrevendo os desafios enfrentados e descrevendo em pormenor como planeiam formar os outros.

Pode encontrar as Ferramentas de Avaliação no IPAD Currículo de formação

2.3. *Workshop* de identificação e prevenção de ciberameaças

1. Objetivos de aprendizagem

1. Compreender as caraterísticas e o impacto das ciberameaças comuns, como o *phishing*, o *malware* e o *ransomware*
2. Desenvolver competências práticas na identificação e resposta a ciberameaças em cenários reais
3. Capacitar os formadores para orientar os formandos na aplicação de medidas preventivas, como hábitos de navegação seguros e monitorização proativa de ameaças
4. Criar confiança na utilização de ferramentas como o software antivírus e as *firewalls* para aumentar a segurança

2. Descrição

DURAÇÃO: 60 minutos

PREPARAÇÃO:

Para se preparar para esta atividade, o facilitador deve recolher e preparar exemplos de ciberameaças comuns, como emails de *phishing*, páginas de *login* falsas e *pop-ups* de *malware*. Estes exemplos podem ser impressos ou apresentados em formato digital para análise. Além disso, crie um guia sobre como configurar *firewalls* e utilizar software antivírus de forma eficaz. Certifique-se de que os dispositivos com acesso à Internet são configurados com ambientes de demonstração simulados ou seguros para permitir que os participantes pratiquem a configuração das definições de segurança. Por fim, forneça folhetos que resumam as melhores práticas para identificar e prevenir ameaças cibernéticas.

DESCRIÇÃO DO PROCESSO:

Etapa 1: Introdução às ciberameaças (15 minutos):

O facilitador inicia a sessão com uma breve palestra que apresenta as ameaças cibernéticas mais prevalecentes, incluindo *phishing, malware, ransomware* e ataques de engenharia social. Cada tipo de ameaça é explicado com exemplos reais para ilustrar o seu potencial impacte nos indivíduos e nas famílias. O facilitador salienta a importância de reconhecer estas ameaças precocemente e de adotar medidas preventivas para se manter seguro online.

Etapa 2: Atividade de identificação de ameaças (20 minutos):

Os participantes são divididos em pares e recebem exemplos simulados de ameaças cibernéticas, tais como um e-mail suspeito, uma página de início de sessão falsa ou um anúncio *pop-up* que afirma que o sistema está infetado. Cada par analisa o exemplo que lhe foi atribuído, identifica o tipo de ameaça que representa e regista os principais indicadores que o assinalam como uma ameaça. A seguir, os participantes discutem as medidas que tomariam para evitar serem vítimas da ameaça e documentam as suas conclusões.

Etapa 3: Exploração das ferramentas preventivas (15 minutos):

O facilitador demonstra como configurar *firewalls* e utilizar software antivírus para detetar e bloquear ameaças. São fornecidas instruções passo a passo para ativar estas ferramentas em dispositivos e plataformas comuns. Em seguida, os participantes praticam a aplicação destas medidas em dispositivos ou contas de demonstração, com a orientação do facilitador para garantir a exatidão.

Etapa 4: Reflexão e conclusão (10 minutos):

A sessão termina com um debate em grupo para abordar equívocos comuns sobre as ferramentas de cibersegurança e a sua eficácia. Os participantes partilham as suas ideias e refletem sobre como podem utilizar estas competências para educar formandos e famílias nas suas comunidades. O facilitador incentiva os participantes a continuarem a praticar e a partilhar medidas preventivas para promover uma cultura de segurança online.

RECOMENDAÇÕES METODOLÓGICAS:

- Utilizar exemplos quotidianos de ciberameaças para ajudar os participantes a compreender as suas implicações práticas
- Incorporar atividades de colaboração, como o trabalho de grupo, para promover o envolvimento e a aprendizagem entre pares, reforçando simultaneamente a confiança através da prática com ferramentas de segurança
- Fornecer materiais de acompanhamento para garantir que os participantes possam continuar a aprender e ensinar eficazmente estas competências a outros

3. Recursos úteis

Dominar a análise de emails de phishing: Resposta a incidentes

www.youtube.com/watch?v=EjY26pqgyME

Segurança cibernética 101: Proteger-se online

www.youtube.com/watch?v=MuVswL8UN_I

Centro de Segurança Google - Como se proteger on-line

www.safety.google/

4. Material necessário

- Exemplos de ciberameaças, tais como emails de *phishing* ou websites falsos (impressos ou digitais).
- Dispositivos com acesso à Internet para praticar a configuração do antivírus e da firewall.
- Folhetos ou guias sobre a utilização de ferramentas de cibersegurança e a identificação de ameaças.

5. Ferramentas de avaliação

Ferramenta de avaliação 1: Questionário sobre ciberameaças

Um pequeno questionário para testar a compreensão dos participantes sobre as ciberameaças, como o *phishing*, e a sua capacidade de reconhecer os principais sinais de alerta.

Ferramenta de avaliação 2: Ficha de trabalho de resposta a ameaças

Os participantes analisam uma ameaça cibernética simulada, descrevem os principais indicadores e as medidas que tomariam para evitar serem vítimas.

Ferramenta de avaliação 3: Inquérito de *feedback* do *workshop*

Um inquérito para recolher *feedback* sobre a relevância da sessão e medir a confiança dos participantes na identificação e resposta a ciberameaças.

Pode encontrar as Ferramentas de Avaliação no IPAD Currículo de formação

UNIDADE 3.

COMPREENDER OS AMBIENTES ONLINE DE MENORES

3.1. Navegar no mundo digital - como as redes sociais moldam as nossas vidas

1. Objetivos de aprendizagem

1. Adquirir conhecimentos práticos sobre as plataformas de redes sociais mais populares entre os menores (por exemplo, TikTok, YouTube, Instagram, Snapchat) e compreender as suas caraterísticas, vantagens e riscos
2. Desenvolver competências para analisar criticamente os hábitos digitais dos jovens e identificar estratégias para apoiar os menores na navegação segura nessas plataformas

2. Descrição

DURAÇÃO: 90 minutos

OBJETIVO:

Esta atividade visa ajudar os participantes a compreender as principais caraterísticas, o apelo e os riscos potenciais das "Quatro Grandes" plataformas de redes sociais (YouTube, TikTok, Instagram e Snapchat) entre os menores. Ao explorar estas plataformas, os participantes obterão informações sobre como apoiar os menores na sua utilização de forma responsável e segura.

PREPARAÇÃO:

Preparar uma apresentação ou um folheto que resuma as principais estatísticas e caraterísticas das "Quatro Grandes" plataformas (YouTube, TikTok, Instagram e Snapchat).

Assegurar o acesso a computadores ou smartphones com ligação à Internet.

Criar uma ficha de trabalho para os participantes preencherem durante a atividade. Eis algumas rubricas que podem ser consideradas:

- Principais caraterísticas da plataforma atribuída
- Riscos e benefícios potenciais
- Estratégias para uma utilização responsável
- Questões para reflexão

DESCRIÇÃO DO PROCESSO:

Etapa 1: Introdução (10 minutos):

Apresente brevemente a atividade e os seus objetivos. Explique que o objetivo é explorar as "Quatro Grandes" plataformas para compreender melhor o seu apelo entre os menores e os riscos associados.

Partilhe as principais estatísticas do relatório do Pew Research Center (por exemplo, tendências de utilização de plataformas entre menores):

- Percentagem de menores que utilizam cada plataforma
- Tendências no consumo de conteúdos (por exemplo, vídeos de curta duração, transmissões em direto)
- Preocupações comuns (por exemplo, *cyberbullying*, tempo de ecrã, privacidade dos dados)

Reforce a importância de abordar a discussão com empatia e evitar, tanto quanto possível, linguagem de julgamento.

Etapa 2: Discussão em grupo (20 minutos):

Divida os participantes em pequenos grupos e atribua a cada grupo uma das "Quatro Grandes" plataformas. Peça aos grupos para debaterem:

- Que caraterísticas tornam esta plataforma apelativa para os menores? Exemplos podem incluir o algoritmo da plataforma, os elementos interativos ou a comunidade.
- Quais são os potenciais riscos que esta plataforma apresenta? Exemplos podem incluir a exposição a conteúdos inadequados, preocupações com a privacidade ou impactes negativos na saúde mental.
- Como é que os adultos podem ajudar os menores a utilizar esta plataforma de forma responsável? Exemplos podem incluir o estabelecimento de limites saudáveis e a educação sobre as definições de privacidade

Etapa 3: Exploração da plataforma (30 minutos):

Cada grupo explorará a plataforma que lhe foi atribuída (através de smartphones ou computadores). Os participantes devem identificar:

- Tipos de conteúdos populares - o que é atualmente tendência (por exemplo, memes, vlogs, desafios).
- Definições de privacidade e funcionalidades de segurança - como é que a plataforma protege os membros? (por exemplo, definições de controlo parental, funcionalidades de denúncia).
- Exemplos de cultura de influência e do seu impacte - como é que os influenciadores moldam os comportamentos e as tendências dos utilizadores?

Etapa 4: Apresentações em grupo (20 minutos):

Cada grupo apresenta as suas conclusões ao grupo maior. Destaque as principais conclusões, tais como riscos, benefícios e estratégias para uma utilização segura.

Etapa 5: Conclusão e reflexão (10 minutos):

Promova um debate de grupo sobre a forma como os conhecimentos adquiridos podem ser aplicados em cenários reais (por exemplo, conversas com menores, definição de limites). Exemplos de perguntas para estimular a discussão incluem:

- Como é que os adultos podem iniciar conversas com os menores sobre a utilização das redes sociais?

- Que limites ou orientações podem ser úteis?
- Como é que os adultos podem manter-se informados sobre a evolução das caraterísticas e dos riscos das plataformas?

Distribua uma folha de reflexão para os participantes anotarem as suas principais aprendizagens.

RECOMENDAÇÕES METODOLÓGICAS:

- Encorajar os participantes a abordar a atividade com mente aberta e a evitar linguagem crítica
- Salientar a importância da empatia e da compreensão ao discutir os hábitos digitais dos menores.

3. Recursos úteis

Relatório do Pew Research Center (2023): Adolescentes, redes sociais e tecnologia 2023

Educação de senso comum: Currículo de Cidadania Digital

Be Internet Awesome da Google: Plataforma de aprendizagem interactiva

4. Material necessário

- Computadores ou telemóveis com acesso à Internet
- Projetor ou ecrã para apresentações
- Folhetos com um resumo das caraterísticas e estatísticas da plataforma
- Fichas de trabalho para debates e reflexões em grupo

5. Ferramentas de avaliação

Ferramenta de avaliação 1: Questionário pós-atividade (Ferramentas de avaliação)

Disponibilize o questionário com os seus formandos, analisando em conjunto as respostas corretas (disponíveis no final do documento). Aproveite esta oportunidade para reforçar os princípios e teorias fundamentais discutidos ao longo da atividade prática, pedindo aos participantes que expliquem porque é que uma determinada resposta é a correta, demonstrando as lições que aprenderam.

Pode encontrar as Ferramentas de Avaliação no IPAD Currículo de formação

3.2. Manter-se resiliente online - lidar com o *cyberbullying* e o assédio

1. Objetivos de aprendizagem

1. Identificar os sinais de *cyberbullying* e assédio online e a compreender o seu impacte psicológico nos menores
2. Desenvolver estratégias práticas para responder e prevenir o cyberbullying, incluindo técnicas de comunicação e intervenção empáticas

2. Descrição

DURAÇÃO: 120 minutos

OBJETIVO:

Esta atividade visa dotar os participantes de conhecimentos e competências para identificar, abordar e prevenir o *cyberbullying*. Através da análise de estudos de caso, da representação de papéis e de debates em grupo, os participantes aprenderão a apoiar os menores que são vítimas de assédio online e a desenvolver a sua resiliência nos espaços digitais.

PREPARAÇÃO:

Prepare estudos de caso ou cenários que descrevam casos de *cyberbullying*. Os exemplos podem incluir:

- Um menor a ser assediado em conversas de grupo
- Uma adolescente que sofre comentários que envergonham o seu corpo nas redes sociais
- Uma criança é excluída ou gozada em comunidades de jogos online

Nota: Dado que se trata de um tema potencialmente muito sensível, é necessário assegurar um equilíbrio entre cenários realistas e evitáveis, sem entrar em exemplos demasiado gráficos. Eis um exemplo de um estudo de caso adequado para esta atividade:

Cenário: Um jovem de 14 anos chamado Alex tem recebido comentários maldosos nas suas publicações no Instagram. Alguns colegas de turma criaram uma conta falsa para gozar com a aparência de Alex e os comentários estão a tornar-se cada vez mais ofensivos. Alex começou a evitar as redes sociais e parece retraído na escola.

Questões para debate:

- Que sinais indicam que o Alex está a ser vítima de *cyberbullying*?
- Como é que o Alex se pode estar a sentir e como é que um adulto pode validar essas emoções?
- Que ações imediatas podem ser tomadas para resolver a situação?

- Que estratégias a longo prazo podem ajudar Alex a desenvolver a sua capacidade de resistência e a sentir-se mais seguro online?

Crie uma lista de recursos para denunciar o *cyberbullying*. Os exemplos podem incluir ferramentas de denúncia específicas da plataforma (por exemplo, o recurso de denúncia de *bullying* do Instagram), linhas de ajuda nacionais (por exemplo, Childline, Cyberbullying Research Center) ou serviços de apoio baseados na escola ou na comunidade.

Desenvolva um guião de dramatização para os participantes praticarem estratégias de intervenção. Incluir sugestões para uma escuta empática, validação de emoções e resolução colaborativa de problemas.

Além disso, recursos como folhetos informativos podem ser especialmente valiosos para esta atividade. Considere um breve texto introdutório sobre o desenvolvimento da resiliência, que aborde temas como o incentivo à comunicação aberta, o ensino da literacia digital e do pensamento crítico e a promoção de métodos de autocuidado e de regulação emocional.

DESCRIÇÃO DO PROCESSO:

Etapa 1: Introdução (15 minutos):

Defina *cyberbullying* e assédio online, utilizando exemplos do mundo real (artigos noticiosos).

Debata o impacte psicológico nos menores (os exemplos podem incluir ansiedade, depressão e problemas de autoestima, retraimento social, declínio académico ou efeitos a longo prazo na confiança), bem como a importância da empatia na abordagem destas questões.

Etapa 2: Análise do estudo de caso (30 minutos):

Divida os participantes em pequenos grupos e forneça a cada um estudo de caso. Incentive os participantes a registar quaisquer pontos interessantes que surjam durante os debates.

Peça aos grupos para analisarem o cenário e identificarem:

- Sinais de *cyberbullying*. Como é que os adultos podem reconhecer quando um menor está a ser vítima de *cyberbullying*? (por exemplo, mudanças de comportamento, relutância em usar dispositivos).
- Potenciais impactes emocionais na vítima. O que é que a vítima pode estar a sentir e como é que os adultos podem validar essas emoções?
- Estratégias de resposta imediata e a longo prazo. Que ações imediatas podem ser tomadas (por exemplo, documentar o abuso, bloquear o agressor)? Que estratégias a longo prazo podem ajudar (por exemplo, criar resiliência, procurar apoio profissional)?

Etapa 3: Atividade de dramatização (40 minutos):

Os grupos encenam uma conversa entre um adulto e um menor que foi vítima de *cyberbullying*. Concentrar-se na escuta empática (reconhecer os sentimentos do menor sem interromper ou minimizar a sua experiência), validar as emoções (utilizando frases como "Lamento imenso que isto lhe tenha acontecido" ou "A culpa não é sua") e desenvolver em colaboração um plano de ação (por exemplo, denunciar o abuso, procurar o apoio de um adulto de confiança).

Etapa 4: Debate em grupo (20 minutos):

Os grupos partilham as suas experiências de dramatização e discutem o que funcionou bem e o que poderia ser melhorado. As perguntas para estimular o debate podem incluir:

- Que estratégias funcionaram bem durante o jogo de papéis?
- Que desafios enfrentaram os participantes e como podem ser resolvidos?
- Quais as principais conclusões que podem ser aplicadas em situações do mundo real?

Destaque as principais estratégias para responder ao *cyberbullying*, tais como documentar o abuso e denunciá-lo às plataformas e procurar apoio de adultos ou profissionais de confiança.

Etapa 5: Conclusão e reflexão (15 minutos):

Distribua um folheto com sugestões para desenvolver a resiliência nos menores. Peça aos participantes para refletirem sobre a forma como podem aplicar estas estratégias nos seus próprios contextos. Incentive-os a refletir sobre as seguintes questões:

- O que aprendeu sobre como lidar com o *cyberbullying*?
- Como é que vai abordar as conversas com menores sobre assédio online?
- Que medidas podem ser tomadas para criar um ambiente digital mais seguro para os menores?

RECOMENDAÇÕES METODOLÓGICAS:

- Sublinhar a importância de criar um ambiente seguro e sem juízos de valor para que os menores possam partilhar as suas experiências
- Incentivar os participantes a praticar uma escuta ativa e evitar dar lições durante as dramatizações.

3. Recursos úteis

Guias online:

StopBullying.gov: Recursos sobre Cyberbullying

Educação de senso comum: Kit de ferramentas para o cyberbullying

NSPCC (REINO UNIDO): Recursos de segurança online

4. Material necessário

- Folhetos de estudos de caso
- Guiões de dramatização
- Folhetos com sugestões para desenvolver a resiliência
- Acesso a computadores ou telemóveis para pesquisa de ferramentas de comunicação

5. Ferramentas de avaliação

Ferramenta de avaliação 1: Questionário pós-atividade - documento Ferramentas de avaliação.

Promova a realização de um questionário aos participantes, analisando as respostas corretas (encontradas no final do documento) em conjunto no final. Utilize esta oportunidade para incutir ainda mais os princípios e teorias fundamentais discutidos ao longo da atividade prática, pedindo-lhes que expliquem porque é que uma determinada resposta é a "correta", demonstrando as lições que aprenderam.

Pode encontrar as Ferramentas de Avaliação no IPAD Currículo de formação

3.3. Segurança online para menores - utilização inteligente e segura da internet

1. Objetivos de aprendizagem

1. Aprender a ensinar aos menores os principais conceitos de literacia digital, incluindo a privacidade online, a segurança dos dados e o comportamento ético
2. Desenvolver ferramentas e atividades práticas para melhorar as competências de literacia digital dos menores, como a criação de palavras-passe fortes e o reconhecimento de tentativas de *phishing*

2. Descrição

DURAÇÃO: 90 minutos

OBJETIVO:

Esta atividade visa melhorar a compreensão dos participantes sobre os conceitos de literacia digital e equipá-los com ferramentas práticas para ensinar estas competências a menores. Através de *workshops* interativos e debates em grupo, os participantes ficarão a conhecer os riscos online, as melhores práticas de cibersegurança e as estratégias para desenvolver a literacia digital dos jovens.

PREPARAÇÃO:

Preparar uma apresentação sobre conceitos de literacia digital, incluindo:

- Encriptação: Como protege os dados e garante a privacidade
- *Cookies*: A sua finalidade e como geri-las
- Higiene digital: Melhores práticas para se manter seguro online (por exemplo, atualizar software, evitar ligações suspeitas)

Elabore um folheto com sugestões para melhorar a literacia digital. Alguns tópicos sugeridos incluem a criação de palavras-passe fortes e únicas, o reconhecimento de tentativas de *phishing* e a gestão das definições de privacidade das redes sociais.

DESCRIÇÃO DO PROCESSO:

Etapa 1: Introdução (10 minutos):

Defina literacia digital e a sua importância no ambiente online moderno, bem como alguns dos exemplos mais comuns de riscos online, tais como:

- *Phishing*: tentativas fraudulentas de roubar informações pessoais
- Violações de dados: Acesso não autorizado a dados sensíveis

- *Malware*: Software concebido para perturbar ou danificar dispositivos

Etapa 2: *Workshop* interativo (40 minutos):

Verificador da força da palavra-passe

- Os participantes criarão e testarão palavras-passe utilizando uma ferramenta online
- Introduzir a importância de palavras-passe fortes e únicas e da autenticação de dois fatores (2FA). As sugestões para criar palavras-passe seguras incluem: utilizar uma mistura de letras, números e símbolos; evitar palavras ou frases comuns; utilizar um gestor de palavras-passe para armazenar e gerar palavras-passe.

Detetores de e-mails de *phishing*

- Apresente aos participantes exemplos de mensagens eletrónicas de *phishing* e peça-lhes que identifiquem os sinais de alerta.
- Debata táticas comuns utilizadas pelos burlões, tais como: linguagem urgente ou ameaçadora; endereços ou ligações de remetentes suspeitos; pedidos de informações pessoais ou financeiras.
- Partilhe estratégias para evitar tentativas de *phishing*, tais como verificar os dados do remetente e evitar clicar em ligações desconhecidas.

Etapa 3: Debate em grupo (20 minutos):

Divida os participantes em pequenos grupos e peça-lhes para pensarem em formas de ensinar os menores sobre literacia digital. As perguntas para orientar a discussão podem incluir:

- Como podemos tornar os conceitos de literacia digital interessantes para os menores?
- Que atividades ou ferramentas podem ajudar os menores a compreender os riscos online?
- Como podemos incentivar os menores a praticar uma boa higiene digital?

Os grupos partilham as suas ideias com o grupo maior.

Etapa 4: Conclusão e reflexão (20 minutos):

Distribua um folheto com dicas e recursos de literacia digital. Aqui está um modelo de amostra que pode utilizar como inspiração:

Dicas de literacia digital

1. Criar palavras-passe fortes:

- Utilizar uma mistura de letras maiúsculas e minúsculas, números e símbolos
- Evitar a utilização de informações pessoais (por exemplo, datas de aniversário, nomes)
- Considerar a utilização de uma frase-passe (por exemplo, "O MeuCãoAmora2Jogar!")

2. Reconhecer os sinais comuns de *phishing*:

- Verificar se o endereço de correio eletrónico do remetente apresenta inconsistências
- Procurar erros ortográficos e gramaticais

- Evitar clicar em ligações ou descarregar anexos de fontes desconhecidas

3. Praticar uma boa higiene digital:

- Atualizar regularmente o software e os dispositivos
- Utilizar software antivírus e ativar *firewalls*
- Ser cauteloso ao partilhar informações pessoais online

4. Ensinar os menores sobre literacia digital:

- Utilizar atividades interativas (por exemplo, jogos, questionários) para tornar a aprendizagem divertida
- Incentivar conversas abertas sobre riscos e segurança online
- Dar o exemplo de bons hábitos digitais e debater as suas próprias experiências

Peça aos participantes para refletirem sobre como podem incorporar estes conceitos no seu trabalho com menores, comprometendo-se com uma mudança positiva que possam integrar nos seus contextos profissionais no futuro. Incentive-os a refletir sobre questões como: O que é que aprenderam sobre literacia digital e segurança online? Como é que vão incorporar estes conceitos no vosso trabalho com menores? Que desafios poderão enfrentar e como os podem resolver?

RECOMENDAÇÕES METODOLÓGICAS:

- Utilizar exemplos do mundo real para tornar os conceitos mais próximos e cativantes
- Incentivar os participantes a pensar de forma criativa sobre como ensinar estes conceitos aos menores

3. Recursos úteis

Be Internet Awesome da Google: Plataforma de aprendizagem interativa

Educação de senso comum: Lições de literacia digital

Norton Security: Sugestões para a segurança online

4. Material necessário

- Computadores ou telemóveis com acesso à Internet
- Folhetos sobre conceitos de literacia digital
- Acesso a ferramentas online (por exemplo, verificador da força da palavra-passe, teste de *phishing*)

5. Ferramentas de avaliação

Ferramenta de avaliação 1: Questionário pós-atividade - documento Ferramentas de avaliação.

Promova a realização de um questionário aos participantes, analisando as respostas corretas (encontradas no final do documento) em conjunto no final. Utilize esta oportunidade para incutir ainda mais os princípios e teorias fundamentais discutidos ao longo da atividade prática, pedindo-lhes que expliquem porque é que uma determinada resposta é a "correta", demonstrando as lições que aprenderam.

Pode encontrar as Ferramentas de Avaliação no IPAD Currículo de formação

UNIDADE 4.

NAVEGAR NAS DEFINIÇÕES DE PRIVACIDADE E SEGURANÇA

4.1. *Workshop* de sensibilização para a privacidade destinado às famílias

1. Objetivos de aprendizagem

1. Entender o conceito de pegadas digitais e como impactam a reputação e a privacidade online
2. Aprender passos práticos para configurar as definições de privacidade em redes sociais e plataformas digitais, protegendo informações pessoais e familiares
3. Identificar os riscos à privacidade associados à partilha excessiva, especialmente em relação a menores, e descobrir estratégias para evitá-los
4. Desenvolver competências para ajudar famílias a monitorizar e gerir as suas pegadas digitais, garantindo uma presença online mais segura

2. Descrição

DURAÇÃO: 60 minutos

PREPARAÇÃO:

Os formadores preparam materiais, incluindo exemplos de perfis para várias plataformas de redes sociais (como Facebook e Instagram) e orientações sobre configurações de privacidade em diferentes dispositivos (*smartphones*, computadores e *tablets*). Configuram computadores ou *tablets* com acesso à Internet e testam contas de demonstração para permitir a prática do ajuste das definições de privacidade.

DESCRIÇÃO DO PROCESSO:

Etapa 1: Introdução (10 minutos):

Comece por debater o conceito de pegadas digitais e a sua importância. Explique como as atividades online ajudam a construir e influenciar a identidade digital de cada pessoa.

Etapa 2: Demonstração interativa (20 minutos):

Guie os participantes na configuração das definições de privacidade em uma ou duas plataformas populares (como Facebook e Instagram). Demonstre como ajustar as configurações para controlar quem pode ver publicações, informações pessoais e a localização.

Etapa 3: Exercício de cenário (20 minutos):

Apresente cenários reais em que as definições de privacidade ajudam a evitar problemas, como roubo de identidade ou partilha excessiva de informações sobre menores. Incentive os participantes a debater os cenários e ajustar as definições de privacidade conforme a situação apresentada.

Etapa 4: Reflexão e perguntas e respostas (10 minutos):

Promova um debate sobre como as famílias podem trabalhar juntas para manter a privacidade e a segurança digital, compartilhando estratégias e práticas que incentivem uma abordagem coletiva e consciente.

RECOMENDAÇÕES METODOLÓGICAS:

- **Envolver os participantes:** comece com um debate aberto, perguntando aos participantes qual é a sua compreensão e quais são as suas preocupações atuais relativamente às definições de privacidade.
- **Utilizar demonstrações visuais:** certifique-se de que cada passo para configurar as definições de privacidade é apresentado visualmente no ecrã, tornando o processo mais claro e acessível, especialmente para quem tem menos experiência com as plataformas digitais.
- **Estimular a prática imediata:** sempre que possível, incentive os participantes a seguir o processo nos seus próprios dispositivos, aplicando as mesmas definições demonstradas pelo formador. Esta aplicação prática reforça a aprendizagem.
- **Descomplicar conceitos:** torne os termos técnicos e as definições de privacidade mais acessíveis, explicando-os de forma clara e com exemplos do dia-a-dia. Por exemplo, compare restringir quem pode ver um perfil a decidir quem pode entrar na sua casa.
- **Promover o debate e a reflexão**: incentive um debate aberto sobre riscos específicos, como a partilha excessiva de informações sobre menores. Explique os riscos de forma prática, mostrando como até informações aparentemente inofensivas podem ser mal utilizadas.
- **Conhecer a sensibilidade cultural e necessidades pessoais:** reconheça as diferentes necessidades de privacidade dos indivíduos e das famílias, sublinhando que cada agregado familiar pode ajustar as definições de acordo com os seus valores e nível de conforto com as redes sociais.

3. Recursos úteis

Guia sobre como gerir as definições de privacidade das redes sociais

www.socialpilot.co/blog/social-media-privacy-settings-guide

4. Material necessário

- Computadores ou *tablets* com acesso à Internet
- Instruções impressas sobre as definições de privacidade para o Facebook e o Instagram
- *Flipchart* ou quadro branco para apresentar e discutir os pontos-chave

5. Ferramentas de avaliação

Teste de sensibilização para a privacidade

Inquérito de autoavaliação: solicitar aos participantes que avaliem o seu nível de conforto com as definições de privacidade antes e depois do *workshop.*

Ficha de reflexão familiar

Debate de *feedback*: finalizar com um breve debate em grupo sobre o nível de confiança dos participantes na aplicação destas definições no seu dia-a-dia em casa.

Ferramenta de Avaliação 3: Inquérito sobre o *feedback* e a confiança do *workshop*

Inquérito que avalia a confiança dos participantes na aplicação de estratégias de privacidade e a sua satisfação geral com o conteúdo do *workshop*.

Pode encontrar as Ferramentas de Avaliação no IPAD Currículo de formação

4.2. Análise da pegada digital

1. Objetivos de aprendizagem

1. Compreender o conceito de pegadas digitais e como as atividades online influenciam e moldam a identidade digital de cada pessoa
2. Aprender métodos para analisar a própria pegada digital e identificar possíveis riscos para a privacidade
3. Capacitar as famílias a avaliar e gerir de forma crítica as suas pegadas digitais, promovendo interações online mais seguras

2. Descrição

DURAÇÃO: 55 minutos

PREPARAÇÃO:

Os formadores preparam fichas de trabalho impressas com uma lista de atividades típicas online (como publicações nas redes sociais, compras online e partilha de localização) e o respetivo impacte potencial nas pegadas digitais. Garantem acesso à Internet para que os participantes possam pesquisar os seus próprios nomes online como parte da atividade.

DESCRIÇÃO DO PROCESSO:

Etapa 1: Introdução (10 minutos):

Comece por discutir o conceito de pegada digital e como as ações quotidianas online, como publicações, pesquisas e interações, contribuem para essa pegada. Explique o impacte duradouro das pegadas digitais, abordando a influência que podem ter na reputação, na privacidade e até nas oportunidades de emprego.

Etapa 2: Exercício de autoanálise (20 minutos):

Distribua as fichas de trabalho e peça aos participantes que façam uma lista das suas atividades recentes online ou dos seus vestígios digitais (como publicações nas redes sociais, comentários em fóruns ou compras online). Instrua os participantes a pesquisarem os seus nomes em motores de busca e redes sociais para identificar que informações estão publicamente visíveis. Incentive-os a avaliar as suas descobertas, identificando quaisquer informações inesperadas ou potencialmente sensíveis que possam comprometer a sua privacidade ou reputação.

Etapa 3: Reflexão e debate em grupo (15 minutos):

Conduza um debate em grupo para os participantes partilharem o que descobriram sobre a sua pegada digital, como se sentem em relação a isso e que mudanças consideram necessárias no seu comportamento online. Forneça dicas práticas para gerir e reduzir as pegadas digitais, como verificar regularmente as definições de privacidade, apagar conteúdos antigos e ser mais seletivo na partilha de informações online.

Etapa 4: Reflexão e perguntas e respostas (10 minutos):

Promova um debate sobre como as famílias podem colaborar para manter a privacidade e a segurança digitais, partilhando estratégias como definir regras para boas práticas online.

RECOMENDAÇÕES METODOLÓGICAS:

- **Incentivar a abertura e o respeito**: garanta aos participantes que a atividade decorre num ambiente livre de julgamentos e que só devem partilhar ideias ou experiências com as quais se sintam confortáveis
- **Utilizar exemplos da vida real**: apresente casos reais que demonstrem como as pegadas digitais impactaram positivamente ou negativamente as pessoas, ajudando a contextualizar o tema
- **Facilitar a reflexão**: faça perguntas orientadoras como: "De que forma esta informação afeta a sua privacidade?" ou "Que alterações, se for caso disso, faria ao seu comportamento online?" para incentivar uma análise crítica e promover discussões construtivas

3. Recursos úteis

Lista de controlo da pegada digital

Gerir a pegada digital para se manter seguro online

4. Material necessário

- Fichas de trabalho impressas com exemplos de atividades online
- Computadores ou *tablets* com acesso à Internet
- *Flipchart* ou quadro branco para registar e partilhar as ideias discutidas pelo grupo

5. Ferramentas de avaliação

Perguntas de reflexão

Peça aos participantes que respondam a questões sobre sentimentos e perceções em relação às pegadas digitais, promovendo uma análise mais aprofundada.

Ficha de autoavaliação

Disponibilize uma lista de verificação para que os participantes avaliem práticas atuais relacionadas com a pegada digital e definam objetivos para melhorar a gestão online.

Pode encontrar as Ferramentas de Avaliação no IPAD Currículo de formação

4.3. *Role-play* sobre definições de privacidade

1. Objetivos de aprendizagem

1. Explorar as definições de privacidade em diferentes plataformas através de uma abordagem prática baseada na realidade
2. Desenvolver competências para configurar definições de privacidade que permitam gerir a visibilidade online e proteger informações pessoais
3. Capacitar formadores de adultos para orientar famílias na criação e aplicação de definições de privacidade eficazes em várias plataformas digitais

2. Descrição

DURAÇÃO: 60 minutos

PREPARAÇÃO:

Crie contas de demonstração em plataformas como Facebook, Instagram e WhatsApp para simular e explorar diferentes definições de privacidade. Prepare cartões de funções com várias personas de utilizadores, como um pai que partilha fotografias de família, um adolescente que interage com amigos ou um profissional que utiliza as redes para *networking*.

DESCRIÇÃO DO PROCESSO:

Etapa 1: Introdução (10 minutos):

Comece por introduzir a importância de utilizar as definições de privacidade para gerir a presença digital e explicar os diferentes tipos de opções disponíveis nas várias plataformas. Apresente a atividade de dramatização, explicando como esta permitirá aos participantes compreender as definições de privacidade aplicadas a situações do dia-a-dia.

Etapa 2: Atividade de dramatização (30 minutos):

Divida os participantes em grupos e atribua a cada grupo uma personalidade de utilizador, como um pai, um jovem adulto ou um profissional. Forneça a cada grupo um cenário específico para configurar as definições de privacidade numa das contas de demonstração (por exemplo, um pai a decidir que fotografias de família partilhar ou um adolescente a controlar quem pode ver as suas publicações). Após configurar as definições, cada grupo apresenta a sua abordagem e explica as razões por detrás das escolhas feitas, justificando as configurações de privacidade selecionadas.

Etapa 3: Balanço e reflexão (20 minutos):

Facilite um debate sobre as experiências vividas durante a dramatização, incentivando os participantes a partilhar os desafios que enfrentaram e as soluções que encontraram ao configurar as definições de privacidade. Promova um debate sobre como estas configurações podem ser ajustadas para famílias com diferentes necessidades e preferências.

RECOMENDAÇÕES METODOLÓGICAS:

- Utilizar cenários realistas: desenvolva personas e situações que representem desafios comuns na gestão da privacidade, tornando a atividade mais próxima da realidade dos participantes
- Incentivar a colaboração: promova debates dentro de cada grupo para que partilhem as suas definições e abordagens, fomentando a aprendizagem entre pares e a troca de diferentes perspetivas
- Fornecer exemplos contextuais: apresente exemplos práticos de como as definições de privacidade podem evitar a partilha excessiva ou reduzir a exposição de dados, especialmente no caso de menores

3. Recursos úteis

Como alterar as definições de privacidade no Instagram

4. Material necessário

- Contas de demonstração no Facebook, Instagram e WhatsApp
- Cartões de funções impressos com personas e cenários de utilizadores
- *Flipchart* ou quadro branco para registar e partilhar ideias discutidas pelo grupo

5. Ferramentas de avaliação

Ficha de análise do cenário

Ficha com perguntas para cada grupo avaliar a compreensão e a aplicação das definições de privacidade no cenário atribuído.

Formulário de *feedback* da dramatização

Após a atividade, os participantes preenchem um formulário onde refletem sobre a sua abordagem e o que aprenderam com a experiência.

Sessão de reflexão em grupo

Facilite uma breve discussão em que cada grupo partilha as lições aprendidas e as principais ideias retiradas das abordagens dos outros grupos.

Pode encontrar as Ferramentas de Avaliação no IPAD Currículo de formação

UNIDADE 5.

NETIQUETA: PROMOVER A PARTICIPAÇÃO NA SOCIEDADE E A CAPACITAÇÃO

5.1. Analisar as interações online

1. Objetivos de aprendizagem

1. Definir o conceito de netiqueta e identificar os seus princípios fundamentais
2. Analisar exemplos de interações online (e-mails, mensagens em redes sociais, debates em fóruns) para distinguir práticas de netiqueta adequada e inadequada
3. Compreender as responsabilidades éticas nas interações digitais, incluindo respeito pela privacidade, pela propriedade intelectual e pelas normas comunitárias
4. Reconhecer os riscos comuns online associados à falta de netiqueta, como *trolling, flaming* e *cyberbullying*
5. Desenvolver e apresentar estratégias para responder a interações negativas online de forma respeitosa e construtiva

2. Descrição

DURAÇÃO: 180 minutos (pode ser repartida por duas sessões)

PREPARAÇÃO:

O formador deve preparar um conjunto diversificado de cenários de interação online, garantindo, pelo menos, dois para cada grupo de três formandos. Estes cenários devem incluir várias plataformas, como email, redes sociais e fóruns e abranger diferentes níveis de gravidade, desde infrações ligeiras da netiqueta até violações mais graves.

É essencial que os cenários explorem dilemas éticos relacionados com a comunicação online, incluindo questões de privacidade, propriedade intelectual e normas comunitárias. Pode considerar a utilização de exemplos anónimos da vida real ou elaborar exemplos fictícios cuidadosamente criados para refletir situações reais. Adicionalmente, deve assegurar que os cenários representam uma diversidade de idades, géneros e origens culturais, promovendo uma abordagem inclusiva.

DESCRIÇÃO DO PROCESSO:

Etapa 1: Introdução (30 minutos):

Comece com uma breve revisão dos princípios fundamentais da netiqueta, utilizando métodos interativos para captar a atenção dos participantes. Pode optar por um pequeno questionário ou uma sessão de *brainstorming* para estimular a participação ativa. Em seguida, debata a importância da netiqueta na criação de comunidades online positivas, destacando como o respeito e a boa comunicação promovem interações saudáveis e construtivas.

Etapa 2: Análise de cenários (60 minutos):

Divida os participantes em grupos de 3-4 pessoas e atribua a cada grupo um conjunto de cenários. Cada cenário deverá ser analisado com base nos seguintes aspetos:

- Identificação do tipo de comunicação online envolvido (por exemplo, email, publicação nas redes sociais, mensagem em fórum)
- Identificação de eventuais violações da netiqueta presentes no cenário
- Explicação de como e por que motivo essas ações violam os princípios da netiqueta, com base no material de formação disponibilizado
- Identificação das potenciais consequências das ações representadas no cenário, tanto para as pessoas envolvidas como para a comunidade online

Etapa 3: Apresentação e debate em grupo (30 minutos):

Cada grupo apresenta a sua análise de um ou dois cenários ao restante dos participantes. Segue-se um debate para comparar as análises, explorar diferentes perspetivas e destacar interpretações alternativas.

Etapa 4: Desenvolvimento de estratégias de resposta (30 minutos):

Centrar a atividade em cenários que ilustrem interações negativas online. Os participantes trabalham nos seus grupos para debater respostas adequadas e construtivas, com foco em estratégias de comunicação respeitosas e assertivas. Oriente-os a considerar os seguintes aspetos:

- Empatia: tentar compreender a perspetiva da outra pessoa antes de responder
- Clareza: exprimir ideias ou pontos de vista de forma clara e direta, evitando ambiguidades
- Respeito: manter um tom respeitoso, mesmo quando surgem desacordos
- Assertividade: exprimir opiniões com confiança, sem cair em atitudes agressivas
- Resolução de problemas: focar-se em encontrar soluções que sejam aceitáveis para todas as partes envolvidas

Etapa 5: Balanço e reflexão (30 minutos):

Promova um debate em grupo para consolidar a aprendizagem. Aborde quaisquer questões ou preocupações que possam ter ficado por esclarecer. Peça aos participantes que reflitam sobre os seus próprios hábitos de comunicação online, identificando áreas onde possam melhorar e aplicar os princípios discutidos.

3. Recursos úteis

Netiqueta para menores

www.youtube.com/watch?v=v1QFaFimVSk&t=18s

O que é a netiqueta?

www.youtube.com/watch?v=CWbtbycHZok

4. Material necessário

- Cenários preparados (em formato impresso ou digital)
- Quadros brancos ou *flipcharts* para registo de ideias
- Marcadores para escrita em grupo
- Notas adesivas para *brainstorming* ou reflexões individuais
- Computadores com acesso à Internet, caso sejam utilizadas ferramentas de colaboração online.

5. Ferramentas de avaliação

Rubrica de análise de cenários

Uma ferramenta de avaliação que mede a exaustividade e a precisão das análises realizadas pelos grupos.

Pode encontrar as Ferramentas de Avaliação no IPAD Currículo de formação

5.2. Criar um guia de netiqueta para as famílias

1. Objetivos de aprendizagem

1. Compreender, de forma abrangente, os princípios da netiqueta e a sua aplicação em diferentes contextos online, como redes sociais, email e jogos online
2. Reconhecer a importância do comportamento ético online no contexto familiar, promovendo interações digitais saudáveis
3. Criar um guia de netiqueta prático e acessível, adaptado às necessidades das famílias
4. Apresentar informações complexas de forma clara e concisa, ajustando o conteúdo a diferentes grupos etários e níveis de literacia digital
5. Assumir a responsabilidade pelo conteúdo do guia, assegurando a sua exatidão e representando as diversas dinâmicas familiares

2. Descrição

DURAÇÃO: 240 minutos (pode ser repartida por duas sessões)

PREPARAÇÃO:

Apenas a recolha de recursos e exemplos que possam apoiar a atividade, como ligações para guias de netiqueta existentes ou artigos sobre comunicação familiar.

DESCRIÇÃO DO PROCESSO:

Etapa 1: Introdução e debate de ideias (30 minutos):

Inicie com um debate sobre a relevância de estabelecer diretrizes claras de netiqueta no contexto familiar. Promova uma tempestade de ideias para identificar as principais áreas a incluir no guia de netiqueta familiar, como: utilização responsável das redes sociais, comportamento em jogos online, comunicação ética, proteção da privacidade e estratégias para prevenir o *cyberbullying*.

Etapa 2: Trabalho de grupo e criação de conteúdos (90 minutos):

Divida os participantes em pequenos grupos, atribuindo a cada a responsabilidade de desenvolver uma parte específica do guia. As possíveis partes incluem:

- Boas práticas nas redes sociais
- Etiqueta em email e mensagens
- Orientações para jogos online
- Proteção da privacidade online
- Lidar com conflitos online
- Prevenção e resposta ao *cyberbullying*

Etapa 3: Refinamento da estrutura do guia e do conteúdo (60 minutos):

Debata a estrutura e o formato do guia de netiqueta, garantindo que seja coerente e fácil de compreender. Cada grupo apresenta o seu trabalho ao grupo maior, recolhendo *feedback* para possíveis melhorias e ajustes. Debata também a inclusão de elementos visuais, como ícones ou ilustrações, para tornar o guia mais apelativo e melhorar a compreensão dos conteúdos.

Etapa 4: Finalização, revisão e edição (30 minutos):

Compile todas as contribuições dos grupos num documento unificado, garantindo que o conteúdo seja claro, coerente e exato. Revise e edite o guia para assegurar que é fácil de ler e inclusivo, adaptando o tom e o formato às diferentes faixas etárias e níveis de literacia digital das famílias.

Etapa 5: Apresentação (30 minutos):

Os grupos podem apresentar as suas partes do guia. Esta partilha permite uma revisão pelos pares, destacando diferentes perspetivas e abordagens.

3. Recursos úteis

Não aplicável

4. Material necessário

- Papel grande ou quadro branco para *brainstorming*
- Marcadores
- Notas adesivas
- Computadores com software de processamento de texto, como Google Docs ou outras plataformas de colaboração
- Impressoras (opcional)

5. Ferramentas de avaliação

Questionário de autorreflexão

Pode encontrar as Ferramentas de Avaliação no IPAD Currículo de formação

UNIDADE 6.

MEDIAÇÃO PARENTAL PARA UMA ABORDAGEM REFLEXIVA

6.1. Minimizar o risco online dos menores e evitar danos através de estratégias de mediação ativa e restritiva

1. Objetivos de aprendizagem

1. Analisar os principais riscos online que os menores enfrentam e apresentar recomendações para minimizar potenciais danos
2. Descrever a importância de os adultos manterem uma comunicação aberta e contínua com os seus filhos sobre as suas experiências no ambiente digital
3. Assumir o compromisso de educar e apoiar os pais no processo de proteger os menores enquanto estes utilizam a Internet
4. Elaborar estratégias práticas que os pais possam implementar para assegurar uma utilização responsável e segura da Internet pelos seus filhos

2. Descrição

DURAÇÃO: 90 minutos

Preparação prévia: imprima o folheto e corte-o ao meio para criar uma atividade de leitura em puzzle. Certifique-se de que há cópias suficientes para que cada pai ou mãe receba uma parte: secção A e secção B.

Durante a atividade prática, os formadores de adultos irão apresentar dois tipos diferentes de estratégias de mediação que os pais podem adotar para reduzir os riscos online enfrentados pelos seus filhos. A sessão começará com uma exploração dos riscos que os menores enfrentam enquanto estão online.

DESCRIÇÃO DO PROCESSO:

Etapa 1: Apresentação de estatísticas

Inicie a sessão apresentando aos pais algumas estatísticas sobre a utilização da Internet pelas crianças. Por exemplo, de acordo com a Comissão Europeia, os jovens passam mais tempo online do que os adultos, com 69% dos jovens entre os 9 e os 22 anos a despender, em média, 3 horas diárias online. Além disso, segundo um relatório da Cybersafekids, uma instituição de caridade irlandesa, 42% dos jovens entre os 8 e os 12 anos e 62% entre os 12 e os 14 anos não falam com os pais sobre a sua atividade online.

Peça aos pais para refletirem sobre os potenciais riscos do mundo digital para as crianças. Forneça a cada pequeno grupo uma folha grande de papel e canetas. Em grupos, devem realizar uma sessão *brainstorming* sobre os riscos associados à presença digital dos menores e organizar as suas ideias num diagrama-aranha.

Etapa 2: Partilha de ideias

Peça a cada grupo que partilhe as suas ideias e realize um debate em grupo sobre os vários riscos sugeridos.

Etapa 3: Apresentação de estratégias de mediação

Explique aos pais que irá apresentar-lhes dois tipos diferentes de estratégias de mediação que podem adotar para proteger os filhos de riscos online: Mediação Ativa e Mediação Restritiva. Divida o grupo em dois. Um dos subgrupos irá ler sobre Mediação Ativa, enquanto a outro sobre Mediação Restritiva. Após a leitura, os participantes devem formar pares com alguém do outro subgrupo. Cada pessoa partilha o que aprendeu sobre a estratégia que leu e ouve a explicação do parceiro sobre a estratégia oposta.

Depois desta troca de informações, os pares discutem algumas questões, como se já utilizam alguma destas abordagens de mediação, qual ou quais utilizam, o que fazem especificamente e o impacte que isso tem nos filhos. Caso ainda não utilizem estas estratégias, devem refletir sobre qual acham que funcionaria melhor com os filhos e porquê, bem como identificar qual delas poderia não funcionar tão bem e os motivos para isso.

Etapa 4: Debate:

Reúna o grupo novamente e promova um debate geral. Peça aos participantes que partilhem as suas opiniões sobre o que acreditam que funciona bem ou funcionará melhor na aplicação das estratégias de mediação discutidas.

Etapa 5: Conclusão

Para concluir, distribua aos pais uma cópia dos dois textos utilizados na atividade, para que os possam levar para casa e consultar posteriormente. Encoraje-os a aplicar algo novo que aprenderam durante a sessão com o(s) seu(s) filho(s) e a refletir sobre os resultados dessa experiência.

3. Recursos úteis

Os formadores podem consultar o curso de *e-Learning* do IPAD, Unidade de Aprendizagem 6: Mediação Parental para uma abordagem reflexiva (lições 1 - 3) e obter informações sobre os riscos online para os menores (para a parte introdutória da atividade) e a Mediação Ativa e Restritiva (para a parte principal desta atividade). Utilize esta informação para criar dois textos que expliquem as diferentes estratégias de mediação.

4. Material necessário

Os formadores devem criar uma folha de apoio para cada uma das estratégias: A. Mediação Ativa e B. Mediação Restritiva. Estas folhas devem conter explicações claras e exemplos práticos de cada abordagem. É importante fazer cópias suficientes para que todos os participantes recebam ambos os documentos no final da atividade. No entanto, no início da atividade de leitura em puzzle.

Além disso, os participantes precisarão de uma folha de cartolina grande (uma para cada grupo de três pessoas) e de marcadores.

5. Ferramentas de avaliação

Debate

Realize um breve debate com os participantes após a conclusão da atividade, utilizando as seguintes perguntas para avaliar o impacte e promover a reflexão:

- Tinha conhecimento de todos os riscos potenciais online para os menores antes desta atividade? Se não, o que aprendeu durante a sessão?
- As estratégias de mediação ativa e restritiva eram novas para si? O que aprendeu sobre estas abordagens e o que pretende implementar no seu dia a dia a partir de agora? Se já utiliza várias estratégias para proteger os seus filhos online, quais pretende continuar a aplicar?
- Em que medida considera que esta atividade foi bem-sucedida em ensiná-lo(a) sobre os potenciais riscos online para os menores e sobre como proteger o(s) seu(s) filho(s) de danos?

Pode encontrar as Ferramentas de Avaliação no IPAD Currículo de formação

6.2. Apoiar a utilização segura e responsável da tecnologia

1. Objetivos de aprendizagem

1. Identificar os principais benefícios que os recursos e atividades online podem trazer para o desenvolvimento das crianças, como a aprendizagem interativa, o desenvolvimento de competências digitais e o acesso a conhecimentos globais
2. Descrever a importância de os adultos manterem uma comunicação aberta e contínua com os filhos sobre as suas experiências online
3. Fornecer recomendações práticas sobre como os adultos podem responder a potenciais conflitos

2. Descrição

DURAÇÃO: 90 minutos

Esta atividade deve ser ministrada aos pais por Educadores de Adultos.

Etapa 1: Análise de riscos

Analise os riscos a que os menores estão expostos online. Dê seguimento à tarefa definida na atividade anterior, se aplicável. Pergunte aos pais como é que se têm saído com a implementação de estratégias de mediação ativa e/ou restritiva. Que resultados obtiveram? Partilhe as suas experiências e incentive uma troca de ideias entre os participantes, para que possam aprender uns com os outros e identificar boas práticas que possam aplicar no futuro.

Etapa 2: Exploração das oportunidades de aprendizagem

Explique que esta atividade será uma oportunidade para explorar os benefícios de estar online, como aprendizagem online, aprendizagem de línguas, jogos de matemática, comunicação e jogos. Divida os participantes em pequenos grupos ou pares e atribua a cada grupo uma categoria específica, como aprendizagem de línguas, ou permita-lhes escolher a sua própria categoria.

Cada grupo deverá pesquisar as melhores aplicações, recursos e sítios web para a sua categoria e tomar notas sobre as funcionalidades e benefícios que encontram. Após a pesquisa, cada grupo apresentará as suas descobertas ao restante grupo, o que levará a um debate sobre as recomendações.

O debate deve incluir a partilha de recursos úteis, aplicações recomendadas e dicas para promover a segurança online. Por exemplo, uma abordagem Restritiva pode incluir a desativação da funcionalidade de conversação em jogos online para evitar contactos indesejados, enquanto uma abordagem Ativa pode centrar-se na importância de manter uma comunicação aberta com os filhos, discutindo a razão pela qual não devem adicionar estranhos como amigos e incentivando-os a falar com os pais sobre pedidos de amizade que possam receber.

Etapa 3: Estímulo à comunicação aberta

Releve a importância de uma comunicação aberta entre pais e filhos. Um estudo concluiu que, embora a mediação restritiva possa reduzir o tempo passado online e limitar os riscos, também aumenta a probabilidade de conflitos entre pais e filhos. Para evitar esses conflitos, especialmente com os mais velhos, é fundamental construir uma relação baseada em confiança e diálogo. Ter conversas abertas e honestas numa base regular é a chave para fomentar uma relação saudável.

Peça aos pais que reflitam sobre algumas questões importantes, como se sabem sempre o que os filhos estão a ver, ouvir ou ler online e se falam abertamente com eles sobre a utilização da Internet. Pergunte se discutem regularmente o que os filhos estão a ver, ler ou ouvir e se estas conversas acontecem de forma consistente. Questione também se o filho alguma vez se sentiu incomodado por algo online e como reagiram nessa situação, bem como se já falaram sobre os riscos e perigos online e as formas de se protegerem.

Etapa. 4: Conclusão

Conclua a sessão com um debate em grupo para refletir sobre as principais conclusões discutidas ao longo do dia. Aborde os benefícios identificados no uso de recursos online e as recomendações partilhadas pelos participantes, destacando as melhores práticas. Enfatize a importância de evitar conflitos, sublinhando como uma comunicação regular, aberta e honesta.

4. Recursos úteis

Ver unidade de aprendizagem 6. Mediação parental para uma abordagem reflexiva.

5. Material necessário

- Acesso à Internet, utilizando telemóveis ou computadores portáteis
- Papel e canetas para anotações
- As perguntas de autorreflexão podem ser disponibilizadas em formato impresso num folheto ou escritas num quadro branco para fácil visualização

6. Ferramentas de avaliação

Autoavaliação

A avaliação será feita através de uma autoavaliação pelos participantes, refletindo sobre o impacte da atividade. Peça-lhes que considerem os seguintes aspetos:

- Aprendi alguns recursos e ferramentas úteis online que pretendo partilhar com o(s) meu(s) filho(s) para apoiar o seu desenvolvimento online
- Comprometo-me a discutir regularmente as atividades online do meu filho com ele
- Estarei atento às suas atividades digitais e incentivarei um diálogo aberto e honesto
- Pretendo dar o exemplo, reduzindo o tempo que passo online ou a olhar para o meu telemóvel

Pode encontrar as Ferramentas de Avaliação no IPAD Currículo de formação

Parceria

Página de rosto e capa
Image by freepik

Innovative digital awareness resources for parents on Social Media Literacy and Internet Safety