



# Compras Online e Oniomania

Online Shopping  
and Oniomania

Comunicar  
em Segurança

fundação  
**III E O**



# O que é?

## O impulso para as compras online e a oniomania

As compras online tornaram-se uma parte comum do dia a dia de crianças, jovens e adultos, oferecendo acesso imediato a uma vasta gama de produtos. Numa fase da vida em que a construção da identidade e a procura por aprovação são tão importantes, a conveniência das compras digitais pode tornar-se numa fonte de satisfação instantânea.

No entanto, esta facilidade esconde perigos. A constante exposição a publicidade e a modelos de vida irreais nas redes sociais pode gerar o desejo compulsivo de comprar, levando a um comportamento de risco conhecido como oniomania. O desejo de ter o último equipamento eletrónico ou de imitar a vida idealizada dos influenciadores pode escalar rapidamente, resultando em dificuldades financeiras e ansiedade.

É fundamental que pais e educadores falem abertamente sobre as formas de gerir o dinheiro, a diferença entre necessidades e desejos, e os riscos associados ao consumismo desenfreado. Ao estabelecer limites claros e ao incentivar o uso mais consciente da internet, é possível ajudar os jovens a desfrutar de uma experiência online positiva e a desenvolver uma relação saudável com o consumo, ajudando-os a alcançar um estilo de vida mais equilibrado.

# Sugestões



1

## Comunicar... Comunicar e... Comunicar

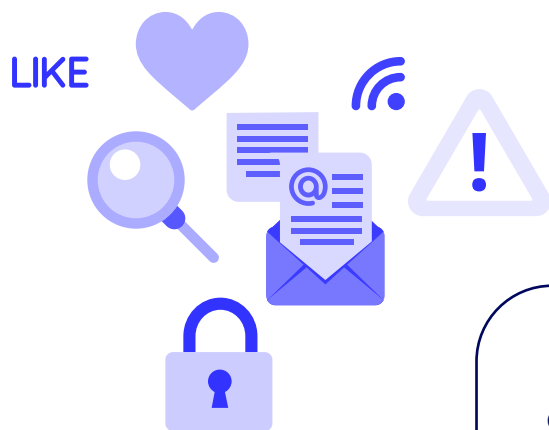
A utilização da internet não deve ser um tema que se deva evitar. É fundamental falar abertamente com as crianças e os adolescentes, incentivando-os a contar o que veem, o que gostam, se algum conteúdo os incomoda ou provoca ansiedade.

## Instalar um antivírus e atualizar regularmente o sistema operativo

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 conteúdos com malware. Devem ser sempre utilizadas fontes oficiais e seguras, como o Google Play Store (Android) ou a App Store (iOS).

Além disso, a atualização regular do sistema operativo não só melhora o desempenho do equipamento, tornando-o mais rápido e eficiente, como também inclui correções de vulnerabilidades e falhas de segurança, protegendo o utilizador de possíveis ataques informáticos.

2



3

### Estar atento a sites falsos

Com o aumento de eventos como a Black Friday e a Cyber Monday, o número de sites fraudulentos, que simulam páginas de lojas legítimas, tem crescido significativamente. O seu objetivo é enganar os consumidores, levando-os a crer que estão a realizar uma transação segura.

Ao ler-se o URL do site deve ter-se em atenção a existência de extensões suspeitas (ex.: ".ws" ou ".tk"), erros de ortografia ou palavras estranhas, números aleatórios ou imitação de sites conhecidos (sendo neste caso muito importante validar o endereço completo).

Para verificar a segurança de um site, é preciso ver se ele começa com "https://". Isso significa que é seguro porque usa o protocolo https, ou seja, que permite transmitir dados de forma criptografada e incompreensível para qualquer hacker.

### Não guardar informações pessoais num site

Apesar da conveniência, é desaconselhado guardar as credenciais de login e dados bancários nos sites. Esta prática aumenta o risco de exposição a ataques informáticos. Para se proteger, evite memorizar estas informações nos navegadores, independentemente de o site utilizar, ou não, o protocolo de segurança https.

Privilegie sempre as redes WiFi seguras.

4



## Passwords fortes e autenticação em 2 fatores

As passwords são senhas de acesso a conteúdos privados, devem ser fortes e não podem ser partilhadas. Uma password forte é aquela que é difícil de adivinhar ou decifrar por outras pessoas. Recomenda-se que sejam longas (com letras, números e caracteres especiais) e não devem conter informações pessoais. Utilize programas de gestão de passwords como o Keeper, o Bitwarden, ou o 1Password.

A autenticação em 2 fatores aumenta a segurança, impedindo que alguém acesse e utilize a sua conta mesmo que tenha acesso à palavra-passe. Para ativar esta opção deve: 1) aceder às configurações de segurança da sua conta (Google, Apple, Facebook, etc.); 2) procurar a opção de A2F, 2FA, verificação em duas etapas ou 2-Step Verification; 3) escolher a forma como pretende receber o código (SMS, Google Authenticator, ou códigos de reserva).

## Utilizar cartões de crédito virtuais

Para uma maior segurança nas transações online, recomenda-se a utilização de um cartão de crédito virtual. Estes cartões permitem definir limites de valor específicos para cada compra, minimizando os riscos em caso de fraude.

Pode criar um cartão de crédito virtual através da app ou do site do seu Banco. Geralmente, este processo é simples não tem custos adicionais, bastando seguir os seguintes passos:

- 1) aceder virtualmente à conta do Banco;
- 2) procurar a opção "Cartões Virtuais";
- 3) criar o tipo de cartão que se pretende (cartão de uso único ou um com um limite de valor específico).

Uma alternativa, para quem não quer usar cartões de crédito virtuais, é efetuar o pagamento através do PayPal, uma plataforma conhecida pela sua segurança e facilidade de uso.

6



7

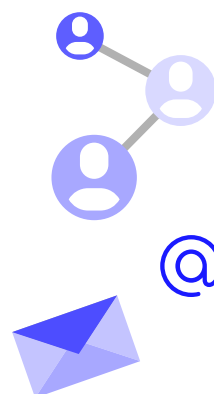
### Campanhas de descontos

Sempre que receber ofertas ou descontos por email ou SMS, deve confirmar a identidade do remetente. Verifique o endereço de email e o número de telefone, num motor de buscar (ex.: Google) para garantir que os dados são verdadeiros.

### Denunciar caso seja vítima de fraude

Em caso de suspeita ou confirmação de fraude online, é importante agir rapidamente. Contactar a Linha Internet Segura (800 21 90 90 ou [linhainternetsegura@apav.pt](mailto:linhainternetsegura@apav.pt)) para obter apoio especializado e denunciar o crime à Polícia Judiciária.

8





# Sinais de Alerta

Para proteger as crianças e adolescentes de perigos online, como o vício em compras, é crucial que os adultos estejam atentos a determinados sinais. Ao identificar os sinais precocemente, é possível intervir a tempo e protegê-los de riscos de utilização da internet.

Esteja atento a:

- 1 **Mudanças repentinas de comportamento**  
(ex.: comportamento repetitivo, uso das compras para gerir as emoções negativas como ansiedade, tristeza, stress ou solidão);
- 2 **Relutância ou medo em mostrar despesas, dívidas ou o comportamento de compra;**
- 3 **Partilha de pensamentos constantes e obsessivos que são incapazes de controlar o que querem comprar, mesmo sem necessidade;**
- 4 **Dificuldade em resistir ao impulso de efetuarem compras (ex.: add-ons de jogos ou de produtos desnecessários ou repetidos);**
- 5 **Acumulação de produtos que não são utilizados ou que permanecem com etiqueta.**

# Como Iniciar o Diálogo

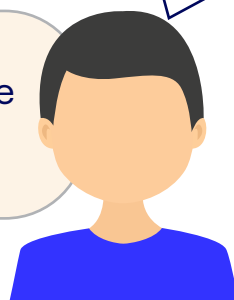
Conversar abertamente com as crianças e os adolescentes sobre os riscos associados às compras por impulso é crucial para garantir que utilizam a internet de forma segura e responsável.

Seguem-se algumas perguntas que poderão ajudar a iniciar o diálogo:



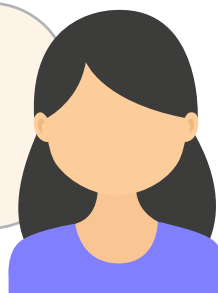
Hoje ouvi uma palavra que não conhecia “onimania”. Sabes o que significa?

Já tentaste parar de comprar e sentiste que não conseguias?



Conheces a “regra dos 10 segundos”? Ou seja, normalmente, quando fazes uma compra na internet, perguntas-te se realmente precisas do que vais comprar? Pensas que poderias usar o dinheiro das compras para outra coisa que te deixasse mais feliz?

Como te sentes após fazeres compras? Ficas entusiasmado/a ou arrependido/a?

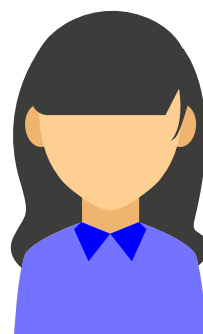






O que costumavas fazer quando te sentes stressado/a ou aborrecido/a?

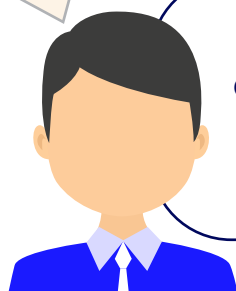
Como tens gerido o teu dinheiro ultimamente?



Antes de fazeres uma compra, comparas os preços para ver se há uma alternativa mais barata?



Imagina que estás num site para comprar um casaco, como é que sabes se precisas mesmo de comprar ou se apenas desejas ter?



Conheces algum influencer que divulgue códigos de desconto?  
Tens encontrado novas lojas ou sites interessantes?

Escondes as compras que fazes dos teus pais/amigos?

**Centro Internet Segura**  
Esclarecimentos e Denúncias

Contacto telefónico gratuito:  
**800 21 90 90**

Correio eletrónico:  
**[linhainternetsegura@apav.pt](mailto:linhainternetsegura@apav.pt)**



Comunicar  
em Segurança

fundação  
**III E O**