Centro Internet Segura

JUNTOS POR UMA INTERNET MAIS SEGURA

CNCS Centro Nacional de Cibersegurança PORTUGAL

www.internetsegura.pt.

Co-financiado pela União Europeia
O Mecanismo Interligar a Europa


C I S

Os responsáveis pela educação dos utilizadores mais jovens devem participar nas atividades *online* dos seus educandos e estar atentos às tendências digitais.

Mantenha um diálogo aberto em família e aborde as melhores práticas e comportamentos *online*.

Procure manter uma atitude empática, coloque-se no papel do outro e ajude a esclarecer possíveis dúvidas.

Defina direitos, responsabilidades, deveres e limites relativos ao uso da Internet e dos diferentes dispositivos eletrónicos.

Estabeleça um paralelo entre a vida *online* e *offline* e tire o melhor partido de ambas.

Procure promover conteúdos *online* pedagógicos e positivos. Saiba como os identificar e onde os encontrar na plataforma Europeia “Better Internet for Kids”.

Analise sempre as classificações de uma aplicação, jogo ou conteúdo *online*, bem como a adequabilidade à idade do utilizador.

Sempre que necessário entre em contacto com a Linha Internet Segura - 800 219 090 e exponha as suas questões de forma gratuita e anónima.

As associações de pais ou similares podem requisitar sessões de sensibilização em www.internetsegura.pt

A exposição a conteúdos impróprios é prejudicial ao desenvolvimento da criança. Acompanhe as suas explorações online e negocie o tempo de utilização dos dispositivos móveis.

Denuncie conteúdos ilegais na Internet de forma anónima ou identificada. Combata todas as ameaças à integridade de cada um.

https://www.internetsegura.pt/lis/denunciar-conteudo-ilegal

Proteja os seus dispositivos. É essencial para toda a atividade *online* ter um programa antivírus atualizado e uma *firewall* ativada.

Utilize redes seguras para fazer compras *online*, ou use VPN. Evite redes Wi-Fi públicas.

Diminua o risco de os seus dados bancários serem expostos. Opte por pagamento multibanco ou à cobrança, cartões temporários ou carteiras digitais.

Verifique na barra de endereço se surge a indicação “https://“. Se o site for seguro estará acompanhado de um cadeado.

Faça uma pesquisa sobre a reputação e a classificação da loja *online* nos motores de busca, nas redes sociais e nos portais de queixa.

Confirme a veracidade do site. Verifique se existem informações sobre o vendedor, avaliações do site e esteja atento a erros ortográficos e gramaticais.

Antes de efetuar uma compra leia as informações da loja e os termos de venda. Informe-se das condições de devolução e reembolso, prazos e custos de entrega.

Coloque os seus dados pessoais apenas nos campos obrigatórios e salte os opcionais. A política de privacidade indica onde poderá ser utilizada a sua informação, leia-a.

Se numa loja *online* os preços dos produtos forem muito baixos, desconfie e compare com os valores praticados noutras lojas *online*.

Aprenda dicas essenciais que lhe permitam identificar se um website de compras *online* é seguro com o curso *e-learning* gratuito, Consumidor Ciberseguro, promovido pelo Centro Internet Segura | CNCS.

https://www.internetsegura.pt/cis/cursos-e-learning

Procure classificar a compra e deixar o seu testemunho. Desta forma, ajudará outros utilizadores a conhecerem a fiabilidade do site.

Conheça os seus direitos em https://europa.eu/youreuright/your-rights_pt e siga a campanha #yourEUright da União Europeia.

Proteja-se das ameaças digitais. Saiba como atuar e identificá-las no curso *e-learning* gratuito, Cidadão Ciberseguro, promovido pelo Centro Internet Segura | CNCS.

https://www.internetsegura.pt/cis/cursos-e-learning

Se for vítima de *Ransomware* procure ajuda em **www.nomoreransom.org**

Engenharia Social é o processo de tentar manipular uma pessoa ou um sistema, recorrendo a informação falsa. Procure verificar a veracidade dos conteúdos *online*.

Malware ou código malicioso, é um *software* destinado a infiltrar-se em dispositivos de forma ilícita, com o intuito de causar danos ou furto de informação. Proteja os seus dispositivos com a instalação de um antivírus.

Nenhum sistema *antimalware* é 100% eficaz. Esteja atento quando descarrega ficheiros e/ou instala aplicações.

O phishing consiste em utilizar métodos tecnológicos que levam o utilizador a revelar dados pessoais e/ou confidenciais. Evite clicar em *links* e anexos desconhecidos.

Apague as mensagens de correio eletrónico não solicitadas, sobretufo as enviadas de forma massiva e indiscriminada.

Faça da *firewall* a sua “parede de fogo” de modo a bloquear o acesso não autorizado às suas redes privadas.

Não clique em *links* ou anexos de emails e SMS suspeitos, nem partilhe os seus dados em resposta a essas mensagens.

Garanta que o seu *software* se encontra devidamente atualizado e utilize mais do que um fator de autenticação quando acede às suas contas.

Evite executar ficheiros que provêm de origens desconhecidas ou pouco confiáveis, especialmente ficheiros que acabem com a extensão “.exe”.

A Linha Internet Segura faculta uma plataforma de denúncia de conteúdos ilegais através do formulário disponível em **www.internetsegura.pt/lis/denunciar-conteudo-ilegal**

Denuncie o incitamento ao ódio, bem como todo o conteúdo que promova a violência por causa da cor, origem étnica, ascendência, religião, sexo, ou orientação sexual.

Os serviços *Peer-to-Peer* (P2P) são sistemas que permitem a partilha de ficheiros entre utilizadores de forma direta. Certifique-se sobre os direitos de autor.

Antes de fazer *download* de novas versões de aplicações, jogos ou antivírus, deverá confirmar se são verdadeiros, uma vez que podem tratar-se de *software* malicioso.

Se trocar ou transferir ficheiros com outros utilizadores esteja atento à presença de programas maliciosos, uma vez que podem estar disfarçados de filmes, álbuns, jogos ou programas populares.

Não partilhe fotografias de outras pessoas sem autorização das mesmas.

Não confie em janelas de *pop-up* que lhe solicitem a transferência de *software*.

Antes de descarregar conteúdos, verifique se estão disponíveis críticas ou revisões ao ficheiro, que poderão sinalizar *malware*.

Verifique as classificações e leia as opiniões dos jogos, aplicações, redes sociais... Certifique-se de que são ambientes seguros.

As redes sociais podem ser plataformas de disseminação de conteúdos que promovem o racismo, a xenofobia e o discurso de ódio. Denuncie e quebre a corrente.

Numa situação de *ciberbullying* guarde registo do que aconteceu e procure apoio. A reação e a procura de vingança só alimentam os *bullies*.

Não partilhe através da Internet dados como as palavras-passe de acesso a contas.

Configure as definições de privacidade nas suas redes sociais e limite quem pode ver os conteúdos que partilha.

Confirme se as plataformas que utiliza são seguras, não partilhe os locais que frequenta habitualmente e evite usar redes Wi-Fi públicas.

Informe-se sobre o Regulamento Geral sobre a Proteção de Dados (RGPD) que estabelece as regras relativas ao tratamento dos seus dados pessoais.

Defina diferentes palavras-passe para as diversas plataformas digitais e instale um gestor de palavras-passe.

https://bit.ly/3hyG5do

Lembre-se de que “uma vez na internet, para sempre na internet”.

Se a sua reputação for alvo de atentado, denuncie as fotos e/ou publicações de cariz difamatório junto do site, aplicação ou rede social.

Denuncie perfis falsos criados em seu nome ou do seu negócio para que os mesmos sejam removidos.

Não faça *login* a outros serviços através de contas das redes sociais.

Não indique o número de telemóvel ou morada no seu perfil ou em publicações.

Procure perceber como é utilizada a sua informação pessoal e como a pode apagar, ou corrigir dados errados.

http://bit.ly/3HL5ACT

Conheça os riscos dos videojogos, não clique em links partilhados por outros jogadores.

Crie um equilíbrio entre as horas que passa a jogar e a fazer outras atividades. Seja saudável nessa gestão!

http://bit.ly/3FCFxLs

Evite que os jogos de apostas se tornem numa prática obsessiva. Estabeleça limites e torne-se num jogador responsável!

Nunca partilhe informação pessoal e/ou sensível com outros jogadores.

Utilize cartões temporários ou carteiras digitais como meio de pagamento.

O *gambling online* não tem limites de horários, estabeleça os seus.

Defina uma palavra-passe do jogo forte, única e altere-a regularmente.

Saiba identificar os sinais de alerta. Algumas consequências como falta de pré-disposição para fazer outras atividades e falta de concentração nas mesmas, assim como apatia fora do ambiente de jogo podem indicar um problema.

Autorize o acesso das aplicações de jogos apenas às funcionalidades necessárias. Nem todas as aplicações necessitam de aceder às suas informações pessoais, câmara, lista de contactos, galeria, para o seu normal funcionamento.

Se jogar online procure conhecer primeiro as regras e os regulamentos dos jogos. Estabeleça também as suas próprias regras e limites de utilização para um maior autocontrolo.

Verifique sempre se a fonte de informação é fidedigna, consulte apenas meios de comunicação oficiais e cruze os conteúdos de diferentes plataformas.

A maior parte das organizações, entidades e empresas já estão presentes *online*. Procure sempre informação a partir do site oficial para garantir a fiabilidade da mesma.

Tenha sempre uma postura crítica face aos conteúdos que encontra, dentro e fora da Internet. Desconfie e leia o artigo completo.

Preste atenção à data de publicação, autoria e fontes dos conteúdos publicados e questione sempre as potenciais motivações dessa partilha.

Na dúvida recorra a ferramentas de *factchecking* para verificar a informação publicamente divulgada.

Identificou uma notícia falsa? Denuncie e contribua positivamente para a reputação de uma pessoa ou marca, e para que a informação falsa não chegue a mais pessoas.

https://combatefakenews.lusa.pt/verificadores-em-portugal/

Prepare-se para as notícias falsas! Saiba como atuar e identificá-las no curso *e-learning* gratuito, Cidadão Ciberinformado, promovido pelo Centro Internet Segura | CNCS.

https://www.internetsegura.pt/cis/cursos-e-learning

Confirme a veracidade da informação que está a partilhar, especialmente em grupos privados. Procure ser uma fonte segura para os seus amigos e familiares.

Períodos de guerra ou crises propiciam a criação de conteúdos falsos para incitamento ao ódio e à violência. Não se limite apenas a uma fonte informativa, vários meios trazem várias perspetivas. Fuja das bolhas de informação.

Uma notícia deverá conter sempre autor e data, caso contrário desconfie.

Leia qualquer informação ou notícia com sentido crítico, mesmo que a tenha recebido da parte de alguém conhecido.

Descarregue aplicações apenas a partir de plataformas reconhecidas e tome atenção às permissões pedidas.

Nas plataformas e aplicações online aceite apenas ligações de pessoas conhecidas.

Aprenda as melhores práticas para mitigar os riscos das redes sociais no curso e-learning gratuito, Cidadão Cibersocial, promovido pelo Centro Internet Segura | CNCS.

https://www.internetsegura.pt/cis/cursos-e-learning

Aproveite ao máximo as oportunidades que a Internet oferece sem perder de vista a segurança. Saiba mais em www.internetsegura.pt.

Aprenda a identificar contas de seguidores falsos nas redes sociais: verifique se têm poucas ou nenhuma publicação; se têm foto de perfil; se seguem muitas pessoas, mas têm poucos seguidores.

Utilize palavras-passe únicas e complexas para aceder às redes sociais e altere-as com frequência.

Qualquer que seja a rede social escolha um perfil fechado. Ao limitar o acesso ao seu perfil, está a limitar o acesso aos seus dados pessoais e ao conteúdo publicado.

Aproveite e faça uma limpeza à sua lista de seguidores, nem todos os utilizadores têm boas intenções. Assegure a sua privacidade e mantenha-se seguro.

No Instagram e Facebook pode desativar as identificações em fotografias ou as menções em comentários.

Oculte o seu estado. O Instagram e o Facebook permitem limitar a visibilidade do seu estado, ou seja, ninguém saberá que está (ou esteve) *online*.

Pode desvincular as contas de *Instagram* e de *Facebook* para impedir que o que publica numa seja replicado na outra.

Evite ter o *bluetooth* e a localização do seu *smartphone* ligados desnecessariamente.

Ative os mecanismos de bloqueio do seu *smartphone* através de um PIN, palavra-passe ou de outra funcionalidade de autenticação.

Utilize uma VPN sempre que se ligar a uma rede Wi-Fi pública ou opte por utilizar os dados móveis para aceder à Internet em lugares sem Wi-Fi doméstico ou profissional.

Use o *AdBlock* para filtrar conteúdos e anúncios. Pode encontrá-lo nos navegadores *Chrome, Opera, Edge e Safari.*

Para tornar o seu Wi-Fi doméstico mais seguro: altere a sua palavra-passe de acesso à rede e ao equipamento.

Se usar dispositivos comuns a outros utilizadores garanta que terminou sessão em todas plataformas utilizadas.

Abra apenas emails de origem conhecida.

Nos seus dispositivos móveis ative as opções de bloqueio remoto, auto-localização e *software* antiroubo.

Limpe o histórico do seu navegador e os *cookies* em todos os dispositivos.

Mantenha o seu sistema operativo e as aplicações atualizadas. As novas versões de *software* trazem melhores ferramentas para combater as ameaças à sua segurança e colmatar anteriores falhas do mesmo.

Cubra ou desative a câmara de portátil. Ative-a apenas quando necessário.

A vida *online* e *offline* estão interligadas, a segurança dos seus dispositivos e dados são fundamentais para garantir a sua segurança. Faça escolhas ciberseguras e aplique boas práticas…

GLOSSÁRIO

1. PARENTALIDADE DIGITAL

2. COMPRAS ONLINE

3. AMEAÇAS E VULNERABILIDADES DIGITAIS

4. CONTEÚDOS ILEGAIS

5. DIREITOS E PRIVACIDADE ONLINE

6. JOGOS ONLINE

7. DESINFORMAÇÃO E VERACIDADE DOS CONTEÚDOS

8. PLATAFORMAS E APLICAÇÕES

9.TECNOLOGIAS E SERVIÇOS ASSOCIADOS ÀS COMUNICAÇÕES ONLINE

CNCS|CIS

Morada:
Centro Nacional de Cibersegurança
Rua da Junqueira 69
1300-342 Lisboa
Portugal

Telefone:
(+351) 210 497 400

Endereço de Email:
internetsegura@cncs.gov.pt