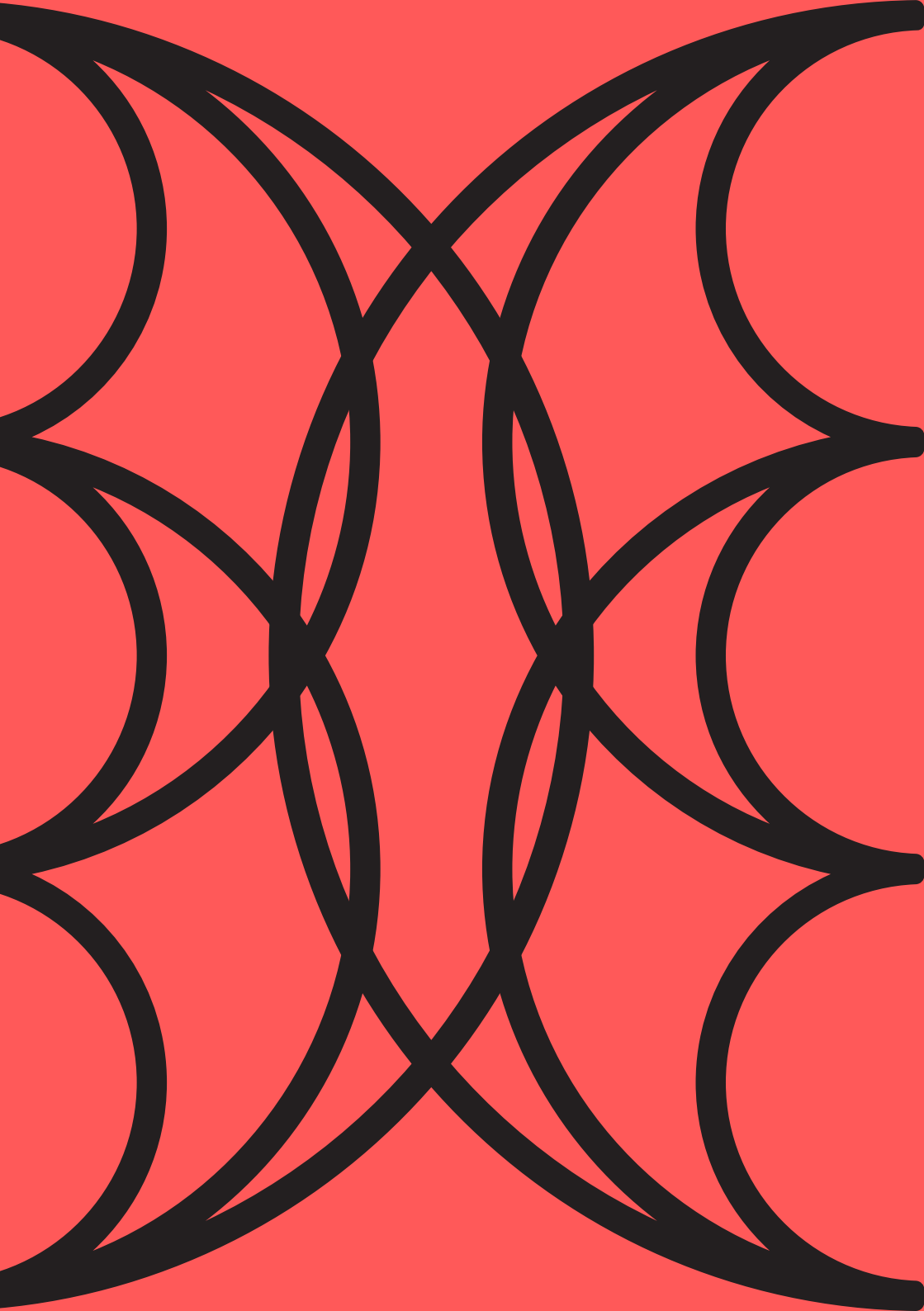


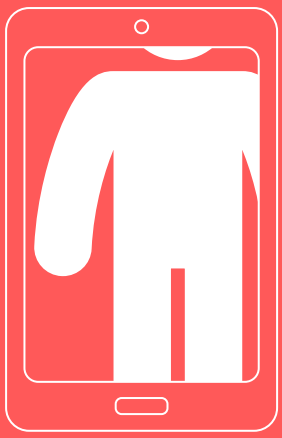
Para escrever tudo o que não faz sentido guardar numa pasta no computador

Permissões a mais?

Emprestaria a sua chave de casa a um desconhecido? A maioria das pessoas não emprestaria por diferentes motivos: estariam a dar acesso aos seus bens e informação, à sua casa e colocariam a sua segurança em risco...

O mesmo acontece com as permissões que damos para instalar *apps* nos nossos dispositivos eletrónicos. As permissões, podem dar acesso a informação crítica, que coloca a privacidade e segurança dos próprios utilizadores em risco.

Reveja as aplicações que está a utilizar e verifique sempre as permissões necessárias antes de instalar uma *app*



Prefira *Smart Sexting*

Atualmente a partilha de conteúdos de cariz erótico ou pornográfico através de tecnologias online é uma realidade. Esta prática designa-se por *sexting* e é um fenómeno cada vez mais frequente entre jovens e adultos.

Existe um conjunto de riscos quando partilhamos este tipo de conteúdos que podem colocar em causa a nossa integridade online e dar origem a outras consequências graves, como a replicação sem fim de conteúdos partilhados.

Se vai partilhar conteúdos íntimos através da Internet, pense muito bem antes de o fazer e garanta que os mesmos não o identificam e opte pelo uso de aplicações com envio temporizado de conteúdos.

Relembre-se que nunca deverá partilhar conteúdos de terceiros, sem o seu consentimento explícito!

Vá de férias sem “seguidores”!

Está a planear tirar férias ou viajar para fora do país?

Ao partilhar detalhes, está a informar que a sua casa se encontra vazia, colocando em risco a segurança dos seus bens. Relembramos que os seus seguidores não precisam de saber desta informação.

Se pretende partilhar momentos das suas férias, opte por enviar mensagens para grupos privados em vez de realizar publicações ou *stories* dirigidas a todos os seus contactos

Uma foto vale mais do que 1000 palavras...

Sempre que publicar uma fotografia, certifique-se que esta não contém informações sensíveis como cartões de identidade, cartões bancários, bilhetes de avião, pulseiras de hospitais e outros dados pessoais.

Ao publicar ou partilhar este tipo de fotografias, está a permitir que todos os utilizadores que visualizam o conteúdo, recolham informação e a utilizem, com boas ou más intenções...

Reveja as fotografias que já publicou e evite partilhar conteúdos que exponham os seus dados pessoais

Até onde vai a sua Pegada Digital?

Pegada Digital é o termo utilizado para definir todas as informações existentes na Internet, que pertencem a um utilizador.

Na maioria das vezes, estas informações encontram-se concentradas nas redes sociais. No entanto, podem existir outros dados em páginas pessoais, fóruns ou até anúncios online.

Estas informações podem já não ser representativas ou benéficas para a reputação dos utilizadores e constituírem possíveis fragilidades à privacidade dos mesmos.

Realize várias pesquisas utilizando o seu nome, alcunhas e nomes de utilizadores, de modo a rever e/ou eliminar parte da sua pegada digital

Como trata a sua *password*?

Uma *password* ou palavra-chave é a primeira linha de defesa das suas contas, tendo como objetivo limitar o acesso da conta apenas ao utilizador responsável por ela.

Para além dos cuidados ao criar uma password (que inclua min. de 8 carateres com letras minúsculas, maiúsculas, números e símbolos), deverá também ter o cuidado de não partilhar esta *password* com ninguém e alterá-la com regularidade.

Lembre-se que cada conta deverá ter uma *password* diferente. Reforce a sua segurança através dos métodos de dupla autenticação

Lidar com um perfil falso

As falsificações de contas de utilizadores são muito frequentes e podem ocorrer por diferentes motivos:

- Gerar *likes*, comentários e visualizações, recorrendo à utilização não-autorizada da imagem de uma figura pública;

- Contactar outros utilizadores assumindo uma identidade falsa;

- Ganhar acesso a informações privadas ou como forma de extorquir dinheiro a amigos/seguidores do utilizador original.

Quando se deparar com um perfil que lhe pareça ser falso, informe o utilizador original, não comunique com a conta falsificada e denuncie esse perfil/conta, através dos mecanismos específicos da rede social

Comprar online com confiança

Comprar online não tem de representar um perigo se seguir algumas recomendações práticas:

1) Verifique que a loja online em questão é fidedigna, através de uma pesquisa;

2) Pesquise se existe algum histórico de incidentes reportados;

3) Realize compras apenas em websites que detêm uma ligação encriptada (https);

4) Utilize sistemas de pagamento como as referências multibanco, PayPal ou MBNet que permitem a criação de cartões de crédito virtuais;

5) Verifique sempre as politicas de cancelamento e devolução da compra, antes de a efetuar.

A sua câmara está destapada?

A câmara do seu portátil ou dispositivo móvel pode aparentar estar desligada, mas saiba que existem maneiras de a ligar, sem a intervenção do utilizador.

Uma das formas mais comuns de ciberataques, consiste na captura de informações armazenadas num dispositivo ou na captura de imagem e/ou som, através dos seus dispositivos periféricos.

Um invasor experiente, pode recolher imagens da sua câmara, sem que se aperceba.

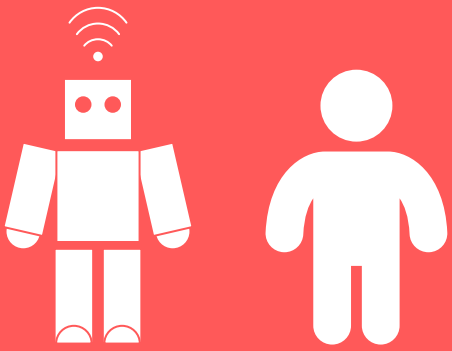
Para proteger a sua privacidade, utilize um protetor específico para a câmara ou um material totalmente opaco, como o cartão ou plástico

Cuidados na era da desinformação

A desinformação é um fenómeno cada vez mais frequente, potenciado pela facilidade em partilhar quaisquer informações online e pela falta de pensamento crítico dos utilizadores.

Relembre-se que, antes de publicar ou partilhar um conteúdo online, deve verificar as suas fontes e reputação das mesmas, bem como se existem fontes diferentes a validar a informação.

É igualmente importante contrariar o impulso de partilhar um conteúdo sem o ler, ou retirado do seu contexto.Podemos estar a replicar conteúdos falsos ou que pretendem manipular os utilizadores



Um brinquedo ou um risco?

Brinquedos que atuam de forma inteligente – este é um mercado emergente dentro do ecossistema da Internet das Coisas.

Equipados com sensores e softwares específicos, os brinquedos interagem com as crianças através da recolha e transmissão de dados.

Estes dispositivos apresentam fragilidades e são suscetíveis a sabotagem, podendo tornar-se interfaces de ataque a outros dispositivos na mesma rede ou permitir a interação entre crianças e invasores.

Antes de adquirir um brinquedo inteligente, informe-se sobre os riscos e problemas que apresenta

800 219 090 Linha Internet Segura

E se precisar de ajuda...?

É fácil pedir recomendações a um familiar ou amigo, quando temos alguma dúvida na nossa utilização da Internet.

No entanto, nem sempre as respostas que encontramos são satisfatórias ou as mais indicadas.

Deverá ser uma prioridade procurar ajuda especializada, quando gerimos riscos da nossa atividade online.

Se precisa de ajuda para lidar com alguma situação relacionada com a sua navegação ou a da sua família e amigos, contacte a Linha Internet Segura, através do número 800 21 90 90

FCT
Fundação
para a Ciência
e a Tecnologia

www.internetsegura.pt

internetsegura@fct.pt

Co-financiado pela União Europeia
O Mecanismo Interligar a Europa