COMUNICAR EM SEGURANÇA

PAIS /ENCARREGADOS DE EDUCAÇÃO

O **Guia Comunicar em Segurança** para pais e educadores pretende transmitir informações, dicas e boas práticas no uso das Novas Tecnologias para os adultos poderem acompanhar as crianças e jovens na utilização diária de Internet e telemóvel.

Os computadores e a Internet alteraram a vida diária das famílias, e são uma ferramenta imprescindível para adultos, crianças e jovens aprenderem, pesquisarem, fazerem amigos e divertirem-se.

Torna-se fundamental dotar os pais e educadores de competências para que não exista uma exclusão digital dos adultos, podendo ser as Novas Tecnologias o elo de ligação entre gerações.

Nesse sentido, neste guia serão abordados três tópicos - **Segurança; Comunicação e Cyberbullying,** e transmitidas dicas e boas práticas para um uso correto e seguro da Internet e telemóveis.

COMUNICAR EM SEGURANÇA

PROTEGER O PC

O computador e a Internet são excelentes ferramentas para as crianças/jovens aprenderem, brincarem, pesquisarem, ouvir música, fazer amigos, etc.

Adopte uma atitude consciente quanto à utilização do computador:

@ **COLOQUE O COMPUTADOR NUMA ÁREA PÚBLICA DA CASA**, por exemplo, na sala de estar. Assim, poderá ir acompanhando os sites visitados pela criança.

@ **DEFINA REGRAS E HORÁRIOS DE UTILIZAÇÃO DO COMPUTADOR E INTERNET.**

@ **NÃO PROÍBA O USO DA INTERNET**, uma vez que os computadores estão por todo o lado – escola, casa dos amigos, bibliotecas. Por este motivo, há que ensinar comportamentos adequados às crianças para uma utilização correta e segura das Novas Tecnologias.

@ No seu computador, **INSTALE SEMPRE UM ANTIVÍRUS** e mantenha-o atualizado. Os antivírus protegem o seu computador de algumas ameaças online. É fundamental ir atualizando o antivírus, pois diariamente surgem novos vírus, e caso não seja realizada a atualização do software, o computador ficará desprotegido.

@ **TENHA A FIREWALL SEMPRE ATIVA**, uma vez que esta funciona como uma parede; uma porta contra-fogo que "não deixa entrar o perigo". Todavia, mesmo tendo estas ferramentas ativas, é sempre necessário continuar a ter cuidado e uma postura preventiva.

@ **NÃO FAÇA O DOWNLOAD OU INSTALE OS PROGRAMAS** que apareçam no computador, sem ter solicitado. Em muitos casos, ao fazer-se o download do programa, está a instalar-se um programa de vírus no computador, que pode copiar toda a informação que tem no computador, desde as passwords até às fotos e vídeos.

@ **TENHA ATENÇÃO AOS LINKS ENVIADOS POR EMAILS**, pois podem ser também uma forma de vírus. Não deverá carregar nos links. Se quiser aceder à página, deve escrever o endereço na barra do Internet Explorer e ver para onde é encaminhado. Em muitos casos, as páginas/sites parecem ser verdadeiros, mas são um "espelho", que pretendem obter os dados pessoais. Não deve confirmar os seus dados pessoais. Se algumas destas mensagens lhe pedir password, nunca deverá dar.

COMUNICAR EM SEGURANÇA

PHISHING E SPAM

***Phishing e Spam* são duas palavras de origem inglesa e ambas correspondem a esquemas de fraude online**

@ O ***Phishing*** trata-se de um esquema de fraude online cujo objetivo é obter dados pessoais e confidenciais, para posteriormente ser realizada uma fraude, como aceder a contas bancárias (por exemplo). O *phishing* bancário é um dos mais conhecidos.

@ Em grande parte dos casos, os emails de *phishing* solicitam sempre o encaminhamento para uma página falsa, onde são solicitados os dados pessoais. **Não deve carregar nos *links*.** Para ver a página para onde serão encaminhados, deve colocar o cursor em cima do *link* e ver qual o endereço associado a esse *link.*

@ Muitas situações de *phishing* chegam através de e-mails. Assim, não deverá responder a e-mails desconhecidos; nem carregar em *links* que encaminham para páginas que parecem verdadeiras, porque, no final, são sempre solicitados os dados pessoais, como por exemplo nome, números de telefone/telemóvel, e-mail, números da conta bancária ou códigos de acesso.

@ Pergunte-se ” Conheço alguém que tenha ganho o euromilhões, ou que tenha ganho uma viagem de sonho? **Na verdade, ninguém dá nada a ninguém e o objectivo deste tipo de emails/jogos/mensagens é sempre ter alguma coisa em troca.**

COMUNICAR EM SEGURANÇA

PHISHING E SPAM

@ ***Spam*** é um esquema de fraude *online* que consiste no envio não solicitado de emails, sendo a grande maioria de carácter comercial.

@ **Os *emails* veem sempre de origem desconhecida**, com assuntos aliciantes, tendo um forte cariz publicitário. Grande parte deste tipo de *emails* vem escrito noutras línguas.

@ Além das mensagens para fins comerciais, existem outros tipos de *spam* . Por exemplo, mensagens maliciosas que tentam induzir o utilizador a informar os seus dados pessoais ou da sua conta bancária ou ainda, executar algum programa que contém vírus.

@ Outros tipos de *spam* como boatos ou correntes, que estimulam ou forçam o utilizador a reencaminhar para os seus contatos, têm ,geralmente ,o objetivo de expandir a base de dados de email do *spammer*. Em muitos casos, os utilizadores não têm o cuidado de ocultar os endereços de *e-mail* quando reencaminham este tipo de mensagem.

NÃO RESPONDER A ESTE TIPO DE EMAILS

NÃO REENCAMINJAR ESTES EMAILS PARA OUTRAS PESSOAS

USAR AS FERRAMENTAS "ANTI-SPAM"

NÃO DAR OS DADOS PESSOAIS

NÃO CARREGAR NOS LINKS QUE ESTEJAM NO EMAIL

COMUNICAR EM SEGURANÇA

FIQUE A SABER...

O **SAPO** tem disponível um novo serviço de *email* especialmente pensado para os mais novos.

É uma conta com dois acessos, um para a criança e outro para o pai/educador. Este vai poder definir, se assim entender, uma lista de *email* autorizados a enviar mensagens para o seu filho. Desta forma o *email* da criança fica protegido de contactos indesejáveis, nomeadamente de *spam,* vírus ou *phishing.*

A criação/configuração desta conta é bastante simples, na criação de uma conta normal SAPO Mail, sempre que a data de nascimento corresponda a um menor de 13 anos é automaticamente pedido o *email* do pai ou encarregado de educação, que recebe no seu *e-mail* um *link* para autorizar a criação da conta. Depois nas configurações o pai vai poder definir os endereços autorizados, todos os *emails* fora desta lista ou são eliminados ou colocados numa pasta adicional para posterior validação.

O aspecto do SAPO *Mail* também foi trabalhado para os mais novos, com a possibilidade de personalizarem o ambiente de trabalho com diferentes cores e com acesso mais directo a *emoticons* (caras engraçadas de sapos) na janela de composição de novas mensagens.

Adicionalmente a criança pode ainda subscrever uma *newsletter* diária com notícias especialmente escolhidas para eles, com dicas de segurança e actividades de lazer, vídeos engraçados ou notícias sobre os ídolos infantis.

O SAPO recomenda a todos os pais/educadores de crianças pequenas a criação ou configuração de uma **conta SAPO Mail Kids** para os seus filhos. É uma nova forma bastante mais segura de os iniciar no mundo das comunicações online e assim os colocar em contacto directo com familiares, amigos e colegas de escola.

Mais informações sobre este novo serviço do Mail do SAPO em:

http://mail.sapo.pt ; http://kids.sapo.pt

COMUNICAR EM SEGURANÇA

CONTROLO PARENTAL

Como no dia-a-dia, é difícil controlar uma criança, o mesmo acontece com a utilização de computadores e Internet. Todavia, poderá educar as crianças para uma utilização segura, consciente e correta das Novas Tecnologias, falando abertamente e explicando que devem pedir ajuda quando se sentem incomodados.

Os pais podem ter uma atitude preventiva, nomeadamente:

@ Instalar um *software* que bloqueie e filtre conteúdos impróprios para crianças.

@ Ver o histórico dos sites visualizados.

@ Colocar os sites mais vistos pelas crianças nos Favoritos, para evitar novas pesquisas.

@ Ter o computador numa zona partilhada da casa – ex: sala de estar.

@ Identificar tempos de utilização do computador e Internet, de modo a evitar a adição.

@ Não instalar programas "*free*" ou fazer *downloads* de programas e *softwares* não oficiais da Internet.

@ Ter perfil de administrador e não partilhá-lo com as crianças e jovens.

@ Alertar os menores para a utilização de computadores públicos, principalmente em questões de *passwords*, partilha de informação ou compras online.

@ Ter *passwords* seguras e fortes, para minimizar os riscos de outros acederem ao computadores e a determinados aplicações ou sites. Não utilizar nomes, moradas, só números, o nome dos filhos, o nome do clube de futebol, etc.

COMUNICAR EM SEGURANÇA

LEMBRE-SE.....

Tendo uma atitude preventiva e instalando ferramentas de *controlo parental*, as pesquisas das crianças poderão levá-los a sites impróprios para menores. Nestes casos, incentive a criança a falar sempre com um adulto e pedir ajuda.

Procure ensinar à criança que nem todos os sites são seguros e que nem tudo o que aparece na Internet é verdadeiro.

A INTERNET É UM MUNDO VIRTUAL!

TODOS OS CUIDADOS QUE AS CRIANÇAS TÊM NO SEU DIA-A-DIA, DEVEM CONTINUAR A TER QUANDO ESTÃO NA INTERNET!

COMUNICAR EM SEGURANÇA

A COMUNICAÇÃO ATRAVÉS DA INTERNET

As crianças/jovens têm muitos amigos e a Internet possui muitas ferramentas que facilitam o contato com mais pessoas, tornando-nos mais próximos uns dos outros e permitindo conhecer mais pessoas.

Exemplos deste fato são os *e-mails, blogs*, redes sociais, etc. As crianças/jovens usam a tecnologia para se conhecerem e vêem estes sites como ”privados” e sem controlo dos pais.

Esta nova realidade alterou alguns conceitos, tais como, a partilha de informação pessoal e privacidade.

Nesse sentido, pais/educadores e crianças devem ter uma atitude consciente para não colocarem a sua integridade física em risco.

COMUNICAR EM SEGURANÇA

DADOS PESSOAIS

- Não colocar fotografias ou proteger as fotografias apenas para certos grupos de pessoas verem.
- **TER *PASSWORDS* SEGURAS :**
  - Combinar letras maiúsculas com minúsculas, números, e carateres especiais.
  - Ter *passwords* diferentes para serviços/acessos diferentes.
  - Não memorizar a *password.* É mais fácil, mas caso alguém aceda ao computador e as *passwords* tiverem memorizadas, entra imediatamente nas páginas.
  - Não escrever a *password* em papéis ou contatos de telemóvel.
  - Não partilhar a *password.* A *password* é como a escova de dentes, não se partilha com ninguém.
- Não partilhar informação pessoal como telefone, telemóvel, moradas, nome de escola, passatempos.
- Não aceitar pedidos de amizade de pessoas que não conhecem.
- Não falar em *chats* com pessoas desconhecidas.
- Pedir autorização aos pais se quiserem colocar na Internet fotografias ou informação pessoal ou de outras pessoas.

COMUNICAR EM SEGURANÇA

FOTOGRAFIAS

Informe a criança/jovem que toda a informação ou fotografia colocada na Internet, sem restrições, fica acessível a todas as pessoas. Pessoas desconhecidas podem modificar a imagem, enviá-la por telemóvel, criar blogs ofensivos, etc.

Procure que nas fotos colocadas na Internet não exista uma identificação do local de onde são as crianças. Por exemplo, se estiver uma praia, é quase impossível localizá-lo, mas se a criança colocar uma fotografia com a sua escola por trás, facilmente localizamos o menor.

Tenha também atenção às webcams. Não deixe que as crianças as utilizem sem supervisão, pois poderão passar a sua imagem a pessoas que não conhecem na realidade.

COMUNICAR EM SEGURANÇA

CONTACTO COM ESTRANHOS

Como no dia-a-dia, as crianças não devem aceitar coisas de estranhos ou falar com pessoas desconhecidas, o mesmo se aplica ao mundo virtual.

A internet permite às pessoas criarem identidades falsas.

Por esse motivo, ensine a criança a:

- **Não falar com estranhos em chats, redes sociais, ou por *e-mail***
- **Não aceitar pedidos de amizade de desconhecidos ou de figuras públicas.**

Por exemplo, se receber um pedido de amizade de um ator conhecido, a criança poderá ter tendência a aceitar. Agora, se o ator não conhece a criança, porque motivo está a enviar um pedido de amizade?

COMUNICAR EM SEGURANÇA

CONTACTO COM ESTRANHOS

Faça um pequeno exercício com a criança:

Veja quantas páginas existem do Cristiano Ronaldo….MUITAS, CERTO?

Certamente, o Cristiano Ronaldo apenas tem uma página oficial.

Devido aos inúmeros perfis falsos que existem nas redes sociais, incentive as crianças a **confirmar sempre os pedidos de amizade**, mesmo que venham dos amigos. Basta um telefonema para o amigo ou esperar pelo dia seguinte, para confirmar se o pedido de amizade é verdadeiro.

COMUNICAR EM SEGURANÇA

CYBERBULLYING

Com o crescente uso da Internet e telemóveis, **as crianças comunicam muito através de emails, chat, redes sociais ou telemóveis.**

Estes novos meios estão a ser utilizados para situações de *cyberbullying*, sendo um dos temas a par com o *bullying* que mais preocupa os pais e incomoda as crianças que são vítimas deste tipo de situações.

A palavra ***CYBERBULLYING*** deriva do termo ***bullying*** e conforme o *bullying*, também é uma agressão, mas é praticada através da **Internet e dos Telemóveis**. **Os agressores ofendem e agridem as vítimas, recorrendo aos emails, ao chat, às redes sociais, blogs e mensagens de telemóvel, mantendo-se assim no anonimato.**

Sabe como ajudar o seu filho?

COMUNICAR EM SEGURANÇA

COMO AJUDAR....

- **É importante que diga à criança que esta não tem culpa da situação** e que não fez nada para estar a ser vítima deste tipo de situação. É fundamental incentivar a criança a falar consigo ou com alguém mais velho sobre as agressões e ofensas, porque os adultos podem ajudar a ultrapassar a situação.

- Outra informação importante que deve transmitir à criança é que não deverá responder ao agressor, porque na maioria dos casos, os agressores querem ter uma reação para continuarem a agredir.

- Como o *cyberbullying* é efetuado através da Internet e telemóveis, **é fundamental guardar as mensagens de telemóvel, emails, conversas de chat ou fotografias uma vez que poderão constituir a prova da agressão.**

- **É muito importante transmitir às crianças que devem tratar os outros como gostariam de ser tratadas, e no caso, de pensarem dizer ou fazer alguma coisa aos colegas, pensarem antes: *"EU GOSTAVA QUE ME FIZESSEM ISTO?"***

COMUNICAR EM SEGURANÇA

COMO AJUDAR....

- **A partilha excessiva de fotografias e dados pessoais pode conduzir a situações de *cyberbullying***, pelo que deverá transmitir esta informação á criança. Quanto mais informação colocam na Internet, mas expostos ficam perante os outros.

- **É importante que não minimize situações de agressão ou as conversas dos filhos, pensando que "são coisas de miúdos" e que passa o tempo.** A criança irá sentir que não tem apoio dos pais/educadores e que não vale a pena partilhar a situação com os adultos. Muitas crianças contam "histórias dos amigos", mas a história é com eles mesmos, por isso, escutar as "histórias" das crianças/jovens é essencial.

- **Por outro lado, não é proibindo a internet ou os telemóveis que a situação vai passar**. Pelo contrário, tem de existir um uso consciente destes meios. Nesse sentido, opte por ter o computador numa área pública da casa, aceda ao histórico dos sites visualizados e defina tempos máximos de utilização da Internet.

- **Reforce que devemos tratar os outros como gostaríamos de ser tratados e que devemos passar esta "máxima" às crianças/jovens.**

COMUNICAR EM SEGURANÇA

GLOSSÁRIO

Anti-Vírus

Aplicação que detecta e bloqueia vírus informáticos. As aplicações antivírus são, atualmente, essenciais para manter a segurança dos computadores, cada vez mais sujeitos a ataques informáticos sobretudo pela ligação permanente à Internet.

Blog

Designa um diário mantido na Internet através de sistemas de publicação fáceis de utilizar. Os blogs popularizaram-se nos últimos anos, criando sites pessoais que se tornaram verdadeiras referências de opinião e informação na Internet.

Bluethooth

Sistema de comunicação sem fios de pequeno alcance (até 100 metros) que torna possível transmitir sinais entre telefones, computadores e outros dispositivos, sem recorrer a fios (wireless).

Browser

É um navegador. É um programa de computador que permite aos
navegarem na Internet, passarem de páginas à distância de um cliq
O **browser** mais conhecido e usado é o Internet Explorer, mas existem outros programas – Firefox; Safari; Chrome

Bully

Indivíduo que pratica situações de bullying ou cyberbullying.

COMUNICAR EM SEGURANÇA

Cyberbullying

Comportamento de violência física e psicológica exercida através da Internet e telemóveis. Termo que deriva de bullying. Cyber porque acontece no meio tecnológico.

Download

Transferência de um ficheiro/programa de um computador remoto para outro computador através da rede. O ficheiro/programa recebido é gravado em disco no computador local. O computador de onde os dados são copiados é subentendido como "maior" ou "superior", enquanto o computador para o qual os dados são copiados é subentendido como "menor" ou "inferior", daí a designação Download, que literalmente significa “puxar para baixo”.

Firewall

Define-se como um mecanismo de defesa. É como uma barreira de proteção que controla o tráfego de dados entre um computador e a Internet. O objetivo de uma **firewall** é permitir a recepção e a transmissão de dados autorizados. Por exemplo, estar ligado à Internet sem ter a **firewall** ligada, é como deixar a porta de casa aberta. Pode acontecer ninguém reparar, mas é possível que alguém se aperceba e aproveite a oportunidade.

A **firewall** bloqueia exatamente e apenas o que tiver definido para ser bloqueado. Técnica e concretamente cada computador do mundo tem um IP, um Mac Adress e muitas portas para comunicar. Por exemplo, vemos páginas pela porta 80, enviamos emails pela porta 25, etc. A firewall abre e fecha certas portas específicas, bloqueia ou permite dados vindos de ips ou mac adress específicos

COMUNICAR EM SEGURANÇA

Hacker

Indivíduo que gosta de explorar todos os aspectos dos sistemas informáticos, incluindo sistemas de segurança. Hackar é um verbo normalmente utilizado para descrever a violação de um sistema informático. A palavra 'hacker' significa, para a maioria dos utilizadores, a pessoa que viola a segurança de sistemas informáticos.

Homepage

Página principal. Página web principal ou de apresentação num sítio (site) da web. O site pode conter múltiplas páginas web, mas apenas uma será a homepage.

Hyperlink

Hiperligação. Muitas vezes abreviado apenas para link. É uma parte fundamental do HTML e permite a navegação fácil e rápida entre páginas de Internet. As hiperligações distinguem-se normalmente por serem palavras ou frases destacadas em azul e sublinhadas

Keylogger

É um programa ou um dispositivo físico desenvolvido para registar a sequência de teclas digitadas por um utilizador. Pode registar tudo o que se digita, incluindo passwords, emails, números de cartão de crédito.

COMUNICAR EM SEGURANÇA

Password

Palavra inglesa que significa palavra – chave e que é necessário para entrar no computador e aceder a determinados serviços online. A **password** deve ser deve ser fácil de decorar mas difícil de descobrir.

Phishing

Tipo de fraude online cujo objetivo é obter os dados pessoais dos utilizadores, como números de cartão de crédito, palavras -passe, dados de contas ou outras informações. O phishing chega aos utilizadores através de emails que parecem reais, uma vez que têm origem em bancos, empresas ou pessoas nos quais os utilizadores confiam. Pode também ter origem numa página web, que quase sempre acaba num formulário numa página de internet, que os utilizadores são convidados a preencher.

Pop-up

Carateriza-se por ser um tipo de publicidade online. A publicidade em forma de Pop-up é aquela que abre numa nova janela do browser (navegador), de forma automática e sobrepondo-se à página que estamos a visualizar

Redes Sociais

São plataformas que permitem ao utilizador, partilhar conteúdos, páginas, links, ou ficheiros multimédia como vídeo e imagens com outros utilizadores que estejam na mesma plataforma. As redes sociais servem para partilhar ideias, gostos e o que se faz na vida. É uma rede porque faz a ligação entre as pessoas, tendo como elo de ligação as próprias pessoas ou interesses comuns.

COMUNICAR EM SEGURANÇA

Router

É um equipamento usado para fazer a comunicação entre diferentes redes de computadores. A principal característica desses equipamentos é selecionar a rota mais apropriada para encaminhar os pacotes recebidos. Ou seja, escolher o melhor caminho disponível na rede para um determinado destino.

É o aparelho que todos temos em casa para distribuir internet e dados por e entre os computadores que temos. Sendo na sua maioria routers com e sem fios, permitindo que os pcs se liguem diretamente ou via wireless à internet e entre si.

Servidor

É o computador central, que administra e fornece informação a outros computadores -clientes. Existem servidores Web que disponibilizam páginas online, servidores de mail que distribuem mensagens, etc.

Spam

Consiste numa mensagem de correio eletrónico não solicitada enviada em massa com fins publicitários. Por norma, os emails enviados são bastante apelativos. Os emails de **Spam** podem ser enviados por pessoas ou por pcs que são programadas para automaticamente fazerem o envio desse spam. A quase totalidade do **Spam** atual é enviado através de pcs infetados de utilizadores que não se apercebem do que os seus pcs estão a fazer quando ligados à internet.

COMUNICAR EM SEGURANÇA

Spammer

Pessoa que envia mensagens de spam

Spim

Consiste numa mensagem publicitária ou indesejada enviada em massa que chegam aos utilizadores através de mensagens instantâneas.

Trojan

Trojan ou Cavalo de Tróia é um programa que age como a lenda do cavalo de Tróia, entrando no computador e abrindo uma porta para um possível invasor. Os trojans atuais são disfarçados de programas legítimos embora, ao contrário do vírus, não criem réplicas de si. Normalmente o trojan está oculto em algum ficheiro, e no momento que esse ficheiro é executado, instala-se e oculta-se no computador da vítima. O trojan é também muitas vezes instalado no computador com o auxílio de um ataque de engenharia social, com apelos para convencer a vítima a executar um ficheiro.

Tipo de danos ou utilizações podem os trojans causar no seu computador:

- Ver, alterar, copiar e apagar os seus ficheiros.
- Monitorizar e registar as suas atividades e enviar essa informação para outro computador. Este processo ajuda os criminosos a descobrir os códigos de utilizador e passwords que introduziu no seu computador;
- Utilizar o seu computador para atacar outros computadores normalmente com o objetivo de sobrecarregar servidores com mensagens, espalhar vírus ou spyware;
- Alterar as funções do computador;
- Criar janelas pop-up com o objetivo de o aborrecer ou para se a ligar a sites maliciosos;

- Executar ou encerrar um programa, processo ou ligação no seu computador;
- Captar vídeo e áudio de dispositivos que tenha ligado ao seu computador.

Troll

Indivíduo que na Internet, causa destabilização, faz insultos, provoca discussões, faz comentários maliciosos. Este tipo de situações está muito presente nos blogs, uma vez que a seguir a cada post há o espaço dos comentários, e existem pessoas que colocam comentários apenas para destabilizarem e verem as reacções do autor e dos outros comentadores.

Upload

Significa Carregar. Upload é enviar um ficheiro do próprio computador para uma rede, que pode ser a Internet. Contrário de download, que se refere a descarregamento de informação de uma rede

Username

É o nome do utilizador que o identifica e é normalmente conjugado com a palavra passe (password).

COMUNICAR EM SEGURANÇA

Vírus

É um programa que atua no computador e no software de forma similar à de um vírus num organismo vivo. O objetivo de um vírus informático é propagar-se, ou seja, chegar a qualquer tipo de meio de comunicação entre computadores, transportado em ficheiros de programas, e modificá-los, a maioria das vezes criando efeitos negativos.

A forma de disseminação dos vírus depende dos objetivos dos seus criadores, mas atualmente o correio electrónico é o método mais utilizado por garantir uma infeção rápida de muitos sistemas. Um vírus pode ser eliminado com programas antivírus, embora para isto seja importante que estes estejam sempre atualizados.

Wireless

Significa "rede sem fio. Permite o acesso a redes e por sua vez à Internet através de ondas de rádio, evitando o uso de cabos para aceder a Internet.

COMUNICAR EM SEGURANÇA

MAIS INFORMAÇÕES:

1. **Guia de Segurança MEO -** http://meo.pt/suporte/net/navegar-em-seguranca/
2. **Antivírus grátis para clientes SAPO** - http://antivirus.sapo.pt
3. **Antivírus grátis para clientes MEO -** http://antivirus.meo.pt
4. **Antivírus grátis para clientes TMN** - http://antivirus.tmn.pt
5. **Funcionalidades de Controlo Parental Bitdefender -**

   http://www.bitdefender.com/solutions/parental-control.html