altice fundação

POLÍCIA
SEGURANÇA PÚBLICA

COMUNICAR EM SEGURANÇA

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

A Internet e os equipamentos tecnológicos 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.

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 contrafogo 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.

PHISHING E SPAM

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 será encaminhado, deverá 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.

Não deverá responder a e-mails desconhecidos.

Não 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.

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 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 REENCAMINHAR ESTES EMAILS

PARA OUTRAS PESSOAS

NÃO DAR DADOS PESSOAIS

NÃO CARREGAR EM LINKS
QUE ESTEJAM
NO EMAIL

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.*

O aspeto 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 direto 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 atividades 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 direto com familiares, amigos e colegas de escola.

Mais informações sobre este serviço do Mail do SAPO em

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

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.

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

Não instalar programas "*free*"
Não fazer *downloads* de programas e *softwares* não oficiais

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

Ter *passwords* seguras e fortes - Não utilizar nomes, moradas, só números, o nome do clube de futebol, etc

A COMUNICAÇÃO ATRAVÉS DA INTERNET

As crianças/jovens usam a tecnologia para se conhecerem e veem estes os blogues, redes sociais, e-mails como ”privados” e sem controlo dos pais.

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

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.

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

DADOS PESSOAIS

Não colocar fotografias que revelem a escola, morada, locais de férias ou atividades de lazer ou familiares.

Não partilhar informação pessoal como telefone, telemóvel, moradas, nome de escola, passatempos.

Não aceitar pedidos de amizade de pessoas que não conhecem.

Pedir autorização aos pais para colocar fotografias e dados de outras pessoas.

Criar grupos para partilhar fotografias

Ter passwords fortes que tenham letras, números, maiúsculas, minúsculas e símbolos especiais

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.

A Internet é pública, pelo que mesmo tendo perfis privados, existem informações e fotografias que não devem ser publicados na Internet.

Procure que nas fotos colocadas na Internet não exista uma identificação do local de onde são/estão 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 a criança/jovem é localizada.

Tenha também atenção às webcams dos equipamentos – tablets, pcs portáteis.

Tape as câmaras dos equipamentos para que não sejam acedidas remotamente por outras pessoas.

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

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 a criação de perfis falsos.

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?

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.

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.

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.

Deve transmitir à criança é que não deverá responder ao agressor, porque na maioria dos casos, os agressores querem ter uma reação.

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?"***

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.

CYBERBULLYING

É importante que não minimize situações de agressão ou as conversas dos filhos, pensando que "são coisas de miúdos" e que passa com 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.

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.

Mais informações em:

SITE | http://www.fundacao.telecom.pt/

Internet Segura | http://www.internetsegura.pt/

PSP | https://www.psp.pt/Pages/homePage.aspx

Linha Internet Segura
800 219 090