Guia para pais de proteção infantil na Internet

INTRODUÇÃO

As crianças são o maior tesouro que temos, são o nosso futuro. Por isso, é necessário guiá-las no decorrer da vida. Essa responsabilidade, no mundo de hoje, representa um verdadeiro desafio para os pais. Com os computadores e dispositivos eletrônicos ficando cada vez mais modernos e com a linguagem que evolui cada vez mais rápido, os pais de hoje sofrem a pressão de ter uma tarefa dupla: educar-se para poder educar. Este guia oferece a possibilidade de conhecer quais aspectos deverá tomar em conta para poder assegurar aos seus filhos uma experiência sadia e segura na Internet, com tudo o que o ciberespaço oferece de útil.

QUEM DEVE FALAR COM AS CRIANÇAS?

Você.

No decorrer de sua infância, a criança irá conhecer pessoas que terão um papel muito importante em sua vida, como por exemplo: familiares, amigos, professores. Porém, nenhuma dessas pessoas irá substituir a figura dos pais, que são a maior referência para seus filhos.

QUANDO VOCÊ DEVE FALAR?

Agora.

À medida que a criança cresce, vai apresentando diferentes problemas. A educação deve estar presente desde o início, já que isso irá ajudar a facilitar a compreensão das medidas de segurança. A partir do momento em que ela começa a manifestar interesse pelo computador e pela web, é possível levar o aprendizado sobre segurança em geral à segurança na Internet. O meio muda, contudo, as ameaças continuam sendo as mesmas.

OS PAIS EDUCAM OS FILHOS E APRENDEM COM ELES

Os pais costumam sentir que os filhos "sabem mais de computador" que eles próprios. Enquanto as crianças atuais costumam ser nativos digitais que nasceram junto a um computador, os pais incorporaram este hábito já na vida adulta.

No entanto, isso não significa que os filhos deva ter o controle do computador na família. O costume no uso da Internet não é o mesmo que ter o conhecimento profundo das implicações das tarefas realizadas, e nesse campo estão as crianças.

Não é necessário que os pais saibam mais que os filhos sobre o que está disponível na rede. Por outro lado, o adulto deve manter o controle, e, ao encontrar algo desconhecido, esse é o momento de se juntar ao seu filho e informar-se a respeito, gerando um ambiente de colaboração familiar, com paciência e compreensão.

O QUE FAZER PARA CADA IDADE?

A seguir, compartilhamos um conjunto básico de regras que fortalecem as atividades das crianças online, de acordo com a faixa etária.

Até os 10 anos:

A *"Acompanhe-os em suas primeiras experiências na web"*

Assegure que você esteja presente em seus primeiros passos. Os primeiros contatos da criança com a Internet são uma boa oportunidade para sentar-se com eles e guia-los através dessa nova aventura.

B *"Defina condições para o uso da Internet"*

Em primeiro caso, devem se estabelecer as regras para a utilização de Internet no lugar. Supervisar a quantidade de horas e fixar horários permitidos são boas práticas para esta medida.

C *"Seja um bom exemplo"*

As crianças geralmente tomam o exemplo dos pais em seu comportamento, seja na Internet ou não. Se os demais membros da família mantém uma conduta positiva, ela será transmitida automaticamente aos filhos.

De 11 a 14 anos:

A *"Utilize ferramentas de Controle dos Pais"*

Aproveite que a tecnologia existe e use-a a seu favor. As ferramentas de controle dos pais permitem bloquear sites que contenham material potencialmente ofensivo. Em alguns casos, é possível impedir o acesso a determinada categoria de páginas.

B *"Ensine a não compartilhar informações que possa identifica-los"*

É importante esclarecer aos seus filhos que, no mundo virtual, nem todas as pessoas são amigas e que algumas podem lhes fazer mal. Por isso, é necessário não compartilhar informações como: Endereço, telefone, locais que frequentam ou onde estudam, etc. Por sua vez, a criança deveria estar devidamente autorizada por seus pais, antes de compartilhar fotos familiares na Internet.

C *"Mantenha o diálogo aberto"*

Estimule a comunicação com seus filhos sobre o que eles veem na Internet. Procure colocar o computador em um lugar comum da casa onde possa estar sob sua supervisão e não no quarto deles.

De 15 a 18 anos:

A ***"Ninguém deve conhecer suas senhas"***

As senhas são como as chaves de casa. Não devem existir cópias nas mãos de estranhos. Nunca se deve fornecer uma senha a um suposto funcionário, seja pela Internet ou pessoalmente, visto que isso nunca deve ser solicitado por nenhum provedor de Internet, serviço de e-mail ou qualquer outra organização.

B ***"Informar sobre abusos imediatamente"***

O cyber bullying é a manifestação dos abusos pessoais através da Internet. Seus efeitos, assim como os abusos fora da web, ferem a criança psicologicamente de forma recorrente e repetitiva. Por isso, deve-se orientar a criança para informar seus pais imediatamente, no caso de ocorrer algo desse tipo.

C ***"As transações financeiras on-line são para os adultos"***

Comprar pela Internet não deve representar um problema, quando feito de forma prudente. O envio de informações pessoais financeiras deve ser realizado sob a supervisão dos pais até que os filhos compreendam as medidas a serem tomadas.

EDUCAR SOBRE SEGURANÇA ONLINE - EM CASA OU NA ESCOLA?

Os pais devem estar permanentemente informados se as escolas desenvolvem algum plano de capacitação para as crianças com relação à segurança na Internet. No que for possível, participar e apoiar esse tipo de atividade escolar, já que os docentes podem ter um papel elevado na vida das crianças e podem aproveitar esse "papel-modelo" que representam para transmitir sugestões sobre o comportamento na rede. Os pais, contudo, continuam sendo a maior referência dos filhos. A educação deve vir, em primeiro lugar, de casa, e posteriormente da escola.

O QUE É O CONTROLE DOS PAIS?

São programas de computador específicos, para poder administrar o conteúdo que se pode ver na Internet. Desta forma, é possível bloquear, para os usuários menores de idade certos conteúdos na rede, ou a quantidade de horas que se pode acessar o sistema. Soluções de segurança antivírus e configurações nos navegadores, entre outros, também dão aos pais uma maneira de poder controlar o que os filhos podem ver na Internet.

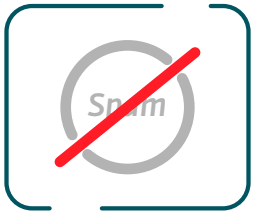
O QUE SÃO AS REDES SOCIAIS?

Uma rede social é uma estrutura social que relaciona pessoas. Pertencer a uma rede social na Internet é parte fundamental das premissas de comunicação modernas. Nessas redes o objetivo é a troca de mensagens e informações com os outros integrantes. Mesmo sendo uma ferramenta muito positiva de comunicação, seu uso deve ser acompanhado e monitorado.

QUAIS AS PRINCIPAIS AMEAÇAS?

Malware

É o acrônimo em inglês de software malicioso (malicious software). O objetivo desse tipo de aplicação é prejudicar o computador. Na maioria dos casos, a infecção ocorre por "erros" realizados pelos usuários, ao serem enganados pelos criminosos. Existem muitas ferramentas (antivírus, antispyware) e boas práticas, que reduzem o risco de infecção diante de todas as variantes de códigos maliciosos: vírus, worms, cavalos de tróia, spyware, etc. A diferença



Spam

O spam é o famoso "lixo eletrônico". São aquelas mensagens que não foram solicitadas pelo usuário e que chegam na caixa de entrada de e-mail. Normalmente, esse tipo de mensagem contém propagandas – muitas vezes enganosas – que convidam o usuário a acessar páginas com ofertas "milagrosas", cujo conteúdo é potencialmente nocivo para o usuário.

Scam

O scam é um golpe executado através da Internet. É realizado de diversas formas, como, por exemplo, através de mensagens não solicitadas (spam), assim como também através de técnicas de Engenharia Social. Esse último exemplo tenta convencer o usuário sobre a prestação de serviço quando na realidade só querem acessar a informação confidencial. Um exemplo são as mensagens falsas solicitando sua senha e login de redes sociais.

Cyber Bullying

É uma conduta hostil que pode ser praticada com as crianças. A vítima desse tipo de hostilidade é submetida a ameaças e humilhações da parte de seus colegas na web, cujas intenções são atormentar a pessoa e leva-la a um estresse emocional. Essas práticas podem ser realizadas através da Internet, assim como também por telefones celulares e videogames. Nem sempre é realizada por adultos, sendo também frequente entre adolescentes.

Grooming

Trata-se da persuasão de um adulto a uma criança, com a finalidade de obter uma conexão emocional e gerar um ambiente de confiança para obter relações sexuais. Muitas vezes os adultos se fazem passar por crianças de sua idade e tentam ganhar confiança para, em seguida, marcar encontros pessoais.

Sexting

Provém do acrônimo formado pelas palavras em inglês Sex e Texting. Inicialmente, e como indica seu nome, se tratava do envio de mensagens com conteúdos eróticos. Posteriormente, devido ao avanço tecnológico, essa modalidade evoluiu para a troca de imagens e vídeos convertendo-se em uma prática habitual entre adolescentes e crianças.

Roubo de informação

Toda informação que viaja pela web, sem medidas de precaução necessárias, corre o risco de ser interceptada por um terceiro. Igualmente, existem também ataques com essa finalidade. A informação procurada normalmente indica os dados pessoais. Um passo em falso nesse tipo de incidente pode expor o menor de idade ao roubo de dinheiro da família ou de identidade.

4 SUGESTÕES FINAIS

Utilize ferramentas de controle dos pais

Essas podem ser aproveitadas tanto nos navegadores, assim como também nos programas de antivírus. É possível utilizar essa versão no ESET Smart Security. Existe esse tipo de ferramentas para consoles também, como Nintendo Wii e Xbox 360.

Não envie informação confidencial pela Internet. Suas informações jamais serão solicitadas por e-mail ou por chat. Os bancos não solicitam os dados de sua conta, muito menos seu PIN. É importante, por sua vez, não ceder essa informação aos seus filhos.

Os bancos não solicitam os dados de sua conta, muito menos seu PIN. É importante

Não responder, nem eliminar mensagens de bullying

Caso seus filhos recebam mensagens de cyber bullying, é necessário instruí-los a não tomar represálias a respeito. Normalmente, o intimidador busca este tipo de reação das crianças para poder continuar fomentando seu desejo de machucar. Esse tipo de situação deve ser apaziguada pelos pais, e, em caso de se repetir, notificar as autoridades correspondentes. Para isso, as mensagens recebidas não devem ser eliminadas, visto que constituem evidência do ato.

Nem tudo o que se vê na rede é verdade

Os filhos devem ser conscientes de que nem toda informação que se distribui na rede provém de uma fonte confiável. Atualmente, é muito fácil obter na Internet um espaço para publicar opiniões. Por fim, deve-se ser muito cuidadoso na hora de recorrer a esses conteúdos.

Comunicação aberta

A comunicação com seus filhos desempenha um papel-chave em sua segurança. O resultado é muito mais produtivo ao incentivá-los a comentar seus medos e inquietações, ao invés de reprimi-los. Mantendo um bom clima e o diálogo aberto, tanto na Internet como na vida real, podem chegar a ser chave de sucesso para lidar com seu bem-

5 BOAS PRÁTICAS PARA OS PAIS

1. ***Crie uma conta de usuário para seu filho:***
   É a única forma de controlar suas atividades na Internet. O usuário administrativo de um sistema deve ser sempre um adulto.

2. ***Mantenha atualizado seu antivírus e sua ferramenta de controle dos pais***

3. ***Monitore o histórico de navegação.***
   Se ele tiver sido apagado, é um bom motivo para ter uma conversa.

4. ***Controle a webcam, e tenha certeza que ela está desconectada enquanto não se deve utilizar.***

5. ***Revise as configurações de redes sociais da criança***
   Um mural de Facebook compartilhado publicamente, sem limitações, pode ser um risco para a integridade do jovem.

CONCLUSÃO

Negar o acesso à tecnologia não é uma solução possível. Ela é parte do dia-a-dia das crianças, e são cada vez mais importantes para o seu crescimento. Portanto, os pais devem acompanhar o uso que os filhos fazem delas e participar da interação do filho com os computadores. Além disso, vale destacar que muitos desses riscos também podem afetar os adultos, já que muitas das precauções aqui descritas devem ser realizadas sempre e em todas as idades.

A segurança dos filhos é responsabilidade de todos, e seguir os conselhos oferecidos neste guia irá ajudar os adultos a proteger melhor a informação, os sistemas, e a própria integridade dos menores de idade.