FUNDAÇÃO OSORIO
Revista Científica

INTERNET, VILÃ OU MOCINHA? UMA NAVEGAÇÃO PELA GRANDE REDE

INTERNET, VILLA OR GIRL? A NAVIGATION BY THE GREAT NETWORK

Mário Eduardo Coutinho de Oliveira
Mestrando em Educação, Universidade Estácio de Sá, Rio de Janeiro, RJ, Brasil.
E-mail:professor.mario.eduardo@gmail.com.

Resumo

Desde o surgimento da primeira rede de computadores a ARPANET (*Advanced Research Projects Agency*), criada pelo Departamento de Defesas dos Estados Unidos, no ano de 1962, que a ideia de se ter a possibilidade de comunicação entre computadores vem se aprimorando. Este artigo se propõe a mostrar a necessidade de se saber como utilizar a Internet para pesquisas, redes sociais, entretenimentos sem correr risco de cair em "*ghost sites*" (sites fantasmas), de ter os seus dados capturados por pessoas desconhecidas. De um modo geral, mostrar os perigos que se escondem na Internet quando uma criança, adolescente ou adulto a utilizam. Mostrar que existem áreas obscuras na Internet, tais como a "*Deep Web*" e a "*Dark Net*" onde se pode encontrar muita coisa ruim. E alertar aos pais e responsáveis sobre como deve ser a utilização de computadores por crianças e adolescentes.

Abstract

Since the advent of the first computer network, the Advanced Research Projects Agency (ARPANET), created by the United States Department of Defense in 1962, has been improving the idea of having communication between computers. This article aims to show the need to know how to use the Internet for research, social networking, entertainment without risk of falling into ghost sites, to have your data captured by unknown people. Generally, show the dangers lurking on the Internet when a child, teenager or adult uses it. Show that there are obscure areas on the Internet, such as Deep Web and Dark Net where you can find a lot of bad stuff. And warn parents and guardians about how computers should be used by children and adolescents.

Resumen

Desde la aparición de la primera red informática, la Agencia de Proyectos de Investigación Avanzada (ARPANET), creada por el Departamento de Defensa de los Estados Unidos en 1962, ha estado mejorando la idea de tener comunicación entre computadoras. Este artículo tiene como objetivo mostrar la necesidad de saber cómo usar Internet para investigación, redes sociales, entretenimiento sin riesgo de caer en sitios fantasmas, para que sus datos sean capturados por personas desconocidas. En general, muestre los peligros que acechan en Internet cuando un niño, adolescente o adulto lo usa. Demuestre que hay áreas oscuras en Internet, como Deep Web y Dark Net, donde puede encontrar muchas cosas malas. Y advierta a los padres y tutores sobre cómo las computadoras deben ser utilizadas por niños y adolescentes.

A INTERNET

Nos dias atuais quase tudo está disponível na Internet. Quem nunca pagou um boleto bancário usando a "agência bancária" existente na grande rede de computadores? Quem nunca fez uma compra, assistiu a um vídeo, conversou com alguém, verificou as câmeras instaladas para segurança de sua casa, agendou uma consulta médica, verificou o andamento escolar do filho, e tantos outros serviços bem ali em cima da mesa ou no seu bolso? É, mas a algum tempo atrás isso não era possível. Este mundo de informações disponíveis todo o tempo e quase que instantaneamente começou a ser idealizada no final da década de 60, mais precisamente em 29 de outubro de 1969, quando aconteceu a primeira conexão entre computadores, a chamada ARPANET (*Advanced Research Projects Agency* - ARPA - Agência de Projetos de Pesquisa Avançada e o termo NET – *Network* – trabalho em rede). A ARPA era uma agência do Departamento de defesa dos Estados Unidos. A ARPANET foi a primeira rede de computadores de uso geral, conectou computadores em sites de pesquisa apoiados pelo governo, principalmente universidades nos Estados Unidos, e logo se tornou uma peça crítica de infraestrutura para a comunidade de pesquisa em ciência da computação nos Estados Unidos (KAHN; DENNIS, 2019).

No ano de 1970 surgiram redes de grande alcance, como por exemplo, a rede via satélite por pacotes que conectou os Estados Unidos a vários países da Europa e a regiões remotas do país. Para que essas conexões de longa distância fossem possíveis, foi projetado um novo conjunto de regras para regerem as transmissões de longa distância, os chamados protocolos, que neste caso, o que foi criado, recebeu o nome de TCP (protocolo de controle de transmissão), criado por Vinton Cerf, na Universidade de Stanford, na Califórnia. Este protocolo permitia diferentes tipos de máquinas na mesma rede. Este protocolo possuía um mecanismo de endereçamento global que permitia que os pacotes de dados fossem levados ao seu destino final através dos roteadores. Este mecanismo se chamava *Internet Protocol* (IP), formou o padrão TCP / IP. Com a formação deste padrão, surgiu a rede mundial de computadores, a Internet (*INTERnacional NETwork* – trabalho em rede internacional) que foi adotado pelo Departamento de Defesa dos EUA em 1980. Nos anos 80, a "arquitetura aberta" da abordagem TCP / IP foi adotada e endossada por muitos outros pesquisadores e, eventualmente, por tecnólogos e empresários de todo o mundo. Outros órgãos do governo norte-americano estavam envolvidos com redes, um dos mais importantes foi a NSF (*National Science Foundation* – Fundação Nacional de Ciências) trabalhou que toda a comunidade científica e acadêmica possuísse acesso ao TCP / IP, tornando-o padrão em todas as redes de pesquisa apoiadas pelo governo federal. Entre 1985 e 1986, a NSF financiou os cinco primeiros centros de supercomputação - na Universidade de Princeton, na Universidade de Pittsburgh, na Universidade da Califórnia, em San Diego, na Universidade de Illinois e na Universidade de Cornell. Ela também financiou a operação e o desenvolvimento da NSFNET, que era uma rede nacional de "backbone" (Espinha dorsal de uma rede. Estrutura de nível mais alto em uma rede composta por várias sub-redes. O *backbone* é composto por linhas de conexão de alta velocidade, que se conectam as linhas de menor velocidade formada por ligações de alta velocidade (FONSECA, 2001)).

No ano de 1990, a ARPANET foi dividida em MILNET, com fins militares e em NSFNET, para pesquisadores, sendo a ARPANET formalmente encerrada. A NSFNET expandiu a rede de forma a englobar também empresas. Nasce então a Internet, compreendendo 1.500 sub-redes (nós) e 250.000 hosts - Computador principal

em um ambiente de processamento distribuído. Computador central que controla uma rede. Na Internet é qualquer computador ligado à rede, não necessariamente um servidor (Fonseca 2001). A partir da transformação da ARPANET em Internet, a rede entra, de fato, na vida das pessoas comuns. Em 1991 surgiu uma ferramenta capaz de ajudar na busca de informações espalhadas pela rede, baseada em menus, o *gopher* - Sistema distribuído para busca e recuperação de documentos, que combina recursos de navegação através de coleções de documentos e bases de dados indexadas, por meio de menus hierárquicos. O protocolo de comunicação e o software seguem o modelo cliente-servidor, permitindo que usuários em sistemas heterogêneos naveguem, pesquisem e recuperem documentos armazenados em diferentes sistemas, de maneira simples e intuitiva. (FONSECA, 2001). O *gopher* logo foi suplantado pela WWW - Navegação hipermídia. É Baseada em hipertextos ou hiperlinks, integrando diversos serviços Internet que oferecem acesso, através de hiperlinks, a recursos multimídia da Internet. Responsável pela popularização da rede pode ser acessada através de interfaces gráficas de uso intuitivo (*browsers* - navegador), como o *Netscape* ou *Internet Explorer* ou o *Google Chrome*. Possibilita uma navegação mais fácil pela Internet de forma muito mais interativa e intuitiva (Internet, 1996; Internet, 1996a).

A ligação com a rede chegou ao Brasil no ano de 1988 por intermédio da FAPESP (Fundação de Amparo à Pesquisa em São Paulo) e no estado do Rio de Janeiro na Universidade Federal do Rio de Janeiro (Folha, 1999). Em 1989, visando estruturar e manter o *backbone*, devido demanda pelo acesso à Internet de modo acadêmico, o Ministério da Ciência e Tecnologia cria a Rede Nacional de Pesquisa (RNP) com o objetivo de integrar esforços estaduais de redes e que viabilizasse a chegada dos serviços ao interior (capilaridade) com a qualidade e eficiência necessárias para o provimento de serviços Internet educacionais. Nesse momento o acesso à Internet no Brasil existia somente nas universidades. (RNP, 1996; RNP, 1996a)

A Internet de hoje é uma Internet de alta velocidade, onde se encontra de tudo que se possa imaginar. A grande "*vide*" do momento são as redes sociais ou "redes de relações sociais" (VERMELHO; MACHADO; BERTONCELLO, 2015, p. 865), que nada mais são do que uma imensa rede de pessoas interconectadas, interligadas através da Internet. A Internet também é utilizada para enviar mensagens através de e-Mail, realizar compras através das páginas de comercio eletrônico (*e-commerce*), assistir vídeos, filmes, palestras, cursos *online*, realizar um curso de formação acadêmica, os chamados EAD (Ensino A Distância) e, quem sabe, no próximo ano já te4nhamos até formação *stricto senso* (mestrado) no formato EAD, realizar conferências, fazer pesquisas acadêmicas ou não acadêmicas.

PERIGOS DA INTERNET

A internet e as redes sociais criaram um espaço infinito para a livre circulação de ideias e opiniões. A reboque, nesse território são instalados tribunais instantâneos que elevam ou enterram as reputações de celebridades e gente comum sem a menor piedade. Nesse meio é possível ter acesso aos mais brilhantes pensadores e conhecer gente bacana para, no clique seguinte, entrar na mira do pior dos criminosos ou ser vítima do mais insuspeito mau-caráter. Há notícias falsas, mentiras políticas, campanhas de ódio, constrangimentos públicos, agressões verbais, preconceitos, assédios, exposições de intimidade e até tentativa de homicídio usando os canais para aproximação com a vítima (VARGAS, 2019).

A Internet é uma grande rede com milhões de computadores interligados, com um número incalculáveis de informações disponíveis com um simples clicar do mouse,

armazenadas e disponíveis em milhões de páginas eletrônica. Com toda essa quantidade de computadores, página eletrônica, informações, seria impossível que não houvesse pelo menos um perigo, por menor que fosse. Claro que não, a Internet é um local virtual onde existem vários problemas e perigos para aqueles que não sabem identificá-los. São alguns deles:

1) **Vírus**

Em informática, um vírus de computador é um software malicioso que é desenvolvido por programadores geralmente inescrupulosos. Tal como um vírus biológico, o programa infecta o sistema, faz cópias de si e tenta se espalhar para outros computadores e dispositivos de informática. A maioria das contaminações ocorre por ação do usuário. Um exemplo muito comum se dá por meio do download de arquivos infectados que são recebidos em anexos de e-mails. A contaminação também pode ocorrer de outras formas: acessando *sites* de procedência duvidosa ou ainda por meio de arquivos infectados em *pendrives*, CDs, DVDs ou qualquer outro tipo dispositivo de armazenamento de dados. Outra maneira de ter um dispositivo contaminado, seria por meio de um Sistema Operacional desatualizado, sem as devidas correções de segurança que visam barrar o acesso indevido destes softwares maliciosos que tentam entrar nas máquinas via Internet (UOL, 2013).

Existem vários tipos de vírus, alguns assim que alojados na máquina, agem instantaneamente. Outros procuram por informações específicas e ainda há outros que permanecem ocultos em determinadas horas ou até mesmo por dias. Estes, geralmente, entram em execução em horas ou datas específicas.

Cada tipo de vírus tem uma execução diferente. Existem vírus que simplesmente escondem os arquivos, outros apagam arquivos do local infectado, tem ainda os que abrem para um acesso externo os arquivos contidos no seu computador, permitindo que o invasor externo acesse, leia, altere, apague os dados contidos nos arquivos ou ainda, apague ou copie o arquivo.

Como se prevenir?

Para se prevenir dos vírus é sempre recomendado fazer o uso de um bom antivírus em seu computador, caso seja possível procure utilizar uma versão paga do antivírus, pois assim você conta com todos os seus recursos de proteção ao computador. Outro bom hábito é evitar *sites* de pornografia, baixar programas que são pagos mas, com um programa chamado de *crack* que inibe a necessidade de chave de ativação do programa. (SECNET, 2019).

2) **Spams**

Spam é um termo de origem inglesa cujo significado designa uma mensagem eletrônica recebida, mas não solicitada pelo usuário. O conteúdo de um spam é normalmente uma mensagem publicitária que tem o objetivo de divulgar os serviços ou produtos de alguma empresa a uma grande massa de usuários de e-mail. A prática de envio em massa desse tipo de mensagem é denominada de *Spamming*, e o autor desse envio é denominado *spammer*. As características principais do *spamming* são o envio da mensagem para milhares de pessoas ao mesmo tempo e a ausência de autorização do destinatário para utilização do seu endereço eletrônico (UOL, 2013).

Além das corriqueiras mensagens para fins comerciais, existem vários outros tipos de spam que invadem as caixas de mensagens dos usuários. Por exemplo, aquelas mensagens maliciosas que tentam induzir o usuário 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 usuário a reencaminhar para os seus contatos, têm geralmente o objetivo de expandir a base de dados de *e-Mail* do *spammer*. Em muitos casos, os usuários não têm o cuidado de ocultar os endereços de *e-Mail* quando reencaminham este tipo de mensagem.

Como se prevenir?

O spam afeta praticamente todos os usuários de *e-mail* e possivelmente você já se deparou com vários, então o recomendado neste caso é que você não abra *e-mails* dos qual você não tenha solicitado, nunca responda um *e-mail* spam e não clique em nenhum *link* ou anexo que foi enviado através do mesmo. No caso das informações falsas sobre conta bancária ou contas pendentes, sempre que receber um *e-mail* desse tipo procure verificar o remetente, e conferir juntamente ao site do mesmo ou por telefone se é um e-mail válido (SECNET, 2019).

3) **Pessoas mal intencionadas**

A internet tem a vantagem - ou desvantagem - de poder preservar a identidade de seus usuários. Muitas pessoas adquirem outras personalidades para conseguirem persuadir os internautas. As intenções são as mais variadas, desde *crackers* tentando roubar informações pessoais até pedófilos tentando marcar encontros (UOL, 2013).

Como se prevenir?

Para evitar este perigo basta não se comunicar com estranhos. Tanto nas redes sociais como por *e-mail*, apenas converse com quem tenha contato, com quem conheça (SECNET, 2019).

4) **Exposição a conteúdos inapropriados**

Refere-se ao acesso ou exposição de crianças e adolescentes, intencionalmente ou acidentalmente, a conteúdos violentos, de natureza sexual ou que gerem ódio, sendo prejudicial ao seu desenvolvimento (MENDOZA, 2018). Esse Tipo de conteúdo é muito fácil de achar na Internet e está disponível para qualquer usuário. Alguns, quando se acessa, apresentam uma tela perguntando se quem está acessando é maior de 18 anos e explica o tipo de conteúdo da página, mas, mesmo não tendo 18 ou mais anos de idade e clicar no botão “SIM”, o acesso será permitido. Existem ferramentas que impedem que determinado conteúdo seja acessado por um computador.

Como se prevenir?

Para que crianças e adolescentes não acessem esse tipo de conteúdo, basta instalar um programa onde o usuário adulto pode definir o que não será acessado pelo computador (SECNET, 2019). Alguns exemplos de programas que fazem este trabalho: *Crawler Parental Control*; The Web Blocker; Kid Mode for Chrome, entre outros.

5) **Publicação de informações privadas**

Se nossa vida está cada vez mais online, cada vez mais nossas ações produzem dados pessoais. Se antes as informações pessoais ficavam em nossa memória e na dos nossos conhecidos, agora temos milhares de novas formas de produzir, registrar e compartilhar dados pessoais.

Nos ambientes digitais somos convidados a criar e compartilhar nossas informações, seja através de nome, apelido, preferências e opiniões nas redes sociais como *Facebook*, de nossas intimidades no *Whatsapp* e no Snapchat, ou de informações sobre nossa vida profissional no *LinkedIn*, passando pelas dezenas de sites nos quais nos cadastramos para fazer compras - músicas, livros, passagens, presentes, roupas, jogos, etc -, sem esquecer que outras pessoas, empresas e governos também produzem dados sobre nós com base em nossas amizades, compras, buscas e formas de participação na vida pública – dentro e fora da Internet.

Os dados pessoais na rede são a soma das incontáveis informações que compartilhamos, junto às produzidas pelas pessoas e instituições com as quais nos relacionamos. Não há como se relacionar sem compartilhar algum tipo de dado, e isso muito antes da Internet. Compartilhar é ótimo, e ao compartilhar podemos todos crescer e aprender. Conectar-se amplia as liberdades. Para conectar é preciso se expor. E isso significa abrir-se ao risco. A consciência sobre como conectar-se com segurança minimiza riscos e amplia a liberdade.

Precisamos fazer boas escolhas para utilizar as tecnologias com segurança e liberdade. Pensar em "O que? ", "Com quem? ", "Onde? ", "De que forma? ", "E por quanto tempo? " compartilhar nossos dados pessoais pode ajudar.

Há duas formas diferentes de nossas informações pessoais ficarem gravadas na internet: de maneira voluntária ou involuntária. Os dados voluntários são aqueles em que o usuário publica diretamente suas informações pessoais, como em acesso a e-mails; para comentários em vídeos, fotos; ou para cadastrar preferências, opiniões e informações em sites de todo tipo.

Os dados involuntários são um conjunto de dados e metadados pessoais que são gerados e armazenados pelos equipamentos e serviços que fazem a mediação com os ambientes digitais. Cookies, histórico de navegação e buscas, dados de acesso a arquivos e serviços, dados técnicos das máquinas fotográficas, senhas, *login*, *Hashs* de imagem estão entre esses dados.

As informações que cedemos aos serviços online são necessárias para muitos dos sites que navegamos por identificação de acesso, compras online, entre outros serviços digitais. A ferramenta de identificação é necessária para a navegação na internet. A solução para proteger-se é saber como ela funciona e conhecer os meios de utilizá-la com segurança.

O vazamento de dados pessoais está em segundo lugar nas denúncias na ONG Safernet (G1, 2018).

Como se prevenir?

Nunca preencha seus dados pessoais como números de documentos; locais de trabalho, moradia e escolas de filhos; agencia e conta bancária, números de telefone, seja fixo ou celular, tanto em cadastros de redes sociais, cadastros de *e-mail* ou qualquer site não confiável que venha a solicitar.

6) **Páginas falsas**

As páginas falsas são uma forma de fraude eletrônica que tem o objetivo de adquirir informações pessoais dos internautas que a acessarem. Elas também são chamadas de *phishing* e sempre tentam induzir seus visitantes a colocarem os dados. As favoritas a se tornarem falsas são as páginas de banco. Para se proteger, toda a vez que for usar seus dados pessoais tente usar a navegação *InPrivate* (dados de navegação como histórico, arquivos temporários da Internet e cookies não são salvos no computador) que os navegadores oferecem (UOL, 2013).

Como se prevenir?

Ao acessar uma página onde você precisa inserir seus dados procure sempre verificar se o site utiliza um Certificado SSL, assim você tem a garantia de que a troca de informações entre você e o servidor está protegida. Você pode ainda utilizar janelas anônimas do navegador todas as vezes que for inserir suas informações em uma página (SECNET, 2019).

7) **e-Mails maliciosos**

Há vários tipos de e-mail que possuem o objetivo de roubar informações pessoais dos internautas. Algumas vezes eles utilizam grandes empresas, como bancos, para poderem persuadir o receptor a entrar no link e fornecer seus dados. Promoções fabulosas também aparecem nas caixas de e-mail.

Como se prevenir?

Sempre que receber algo suspeito, investigue. Se tiver dúvidas, não acesse ou clique em qualquer link.

8) **Abuso sexual de crianças e adolescentes (Pedofília)**

Para se aproximar de uma criança, um pedófilo deve ter uma maneira de se comunicar com ela de forma privativa. Os criminosos utilizam redes sociais, chats e outros espaços que tenham popularidade entre crianças e adolescentes para esta modalidade de crime: o aliciamento online.

Ações deliberadamente realizadas com o objetivo de fazer amizade e estabelecer uma conexão emocional com a criança a fim de diminuir a inibição em preparação para a atividade sexual. Essa é a definição de aliciamento online. Os ambientes online podem ser acessados por qualquer pessoa de qualquer lugar do mundo. Isto combinado com sistemas VOIP (por exemplo, Skype) permitem conversas com voz, vídeo e comunicação baseada em texto, que possibilitam potencial e pleno acesso de comunicação com crianças e adolescentes com intenções criminosas.

Muitas vezes, as crianças sentem que estão a salvo, mas não sabem com quem estão falando. Os aliciadores podem ser hábeis para obter o máximo de informações sobre a localização, interesses e até mesmo conhecimento e experiências sexuais de crianças e adolescentes. As habilidades incluem persuadir a vítima a não buscar proteção dos pais ou outros responsáveis.

A SaferNet Brasil recebe denúncias de páginas de abuso sexual infantil que estejam disponíveis publicamente. Para suspeitas de crime de aliciamento sexual infantil, o canal de ajuda pode orientar vítimas a reportar às autoridades competentes: Conselho tutelar, Ministério Público e Polícia Federal. A Safernet possibilita formas mais seguras e eficazes para preservar o denunciante ou a vítima.

Mais de 24 milhões de crianças e adolescentes têm acesso à internet no Brasil e 77% deles assistem a vídeos online, segundo dados do Comitê Gestor da Internet no Brasil (G1, 2018).

Muitas das vezes este perigo ocorre através de redes sociais. A criança ou o adolescente aceita uma nova “amizade” após ler o perfil do abusador ou recebe um convite para incluí-lo como amigo. Começa a trocar mensagens, o abusador conquista a sua “vítima” com assuntos do seu interesse, até que chega o memento que se marca um encontro físico, e é neste momento que o abuso ocorre.

Como se prevenir?

Os pais e responsáveis devem orientar as crianças e os adolescente para esse tipo de “amizade”. Os computadores, *e-mails* e as redes sociais de crianças e adolescentes devem ser visitados pelos pais e responsáveis periodicamente, ver as conversas que estão acontecendo, os arquivos que se encontram no computador, a relação de amigos. Existem programas que gravam toda a qualquer troca de mensagem feita através, por exemplo, das redes sociais. As conversas podem ser apagadas das redes sociais, o computador pode ser desligado que, mesmo assim, as conversas ficam gravadas e o usuário não tem ciência disso. Alguns exemplos: Online Guardian – monitora atividades

online (páginas acessadas); Social Monitor – monitora atividades do Facebook, entre outros.

9) **Materiais de abuso sexual de crianças e adolescentes gerados digitalmente**

São filmes longos, vídeos curtos de produção artificial, através da mídia digital, de todo tipo de material que represente crianças e adolescentes que participam de atividades sexuais e/ou de maneira sexualizada, para fazer com que os fatos pareçam reais.

10) ***Grooming***

O termo refere-se às estratégias que um adulto realiza para ganhar a confiança de uma criança ou adolescente, através da Internet, com o propósito de abusar ou explorar sexualmente. O *grooming* sempre é realizado por um adulto. Existem dois tipos de *grooming*: o primeiro é quando não há fase anterior de relacionamento e geração de confiança, mas o assediador consegue obter fotos ou vídeos sexuais da criança para extorquir. A segunda é quando há uma fase anterior em que o assediador procura gerar confiança, fazendo com que a criança ou adolescente entregue material sexual a fim de torná-lo alvo de chantagens. O assediador geralmente finge ser uma criança, consegue manipular através dos gostos e preferências da vítima e usa o tempo para fortalecer o vínculo (MENDOZA, 2018).

Como se prevenir?

- Fale com seu filho sobre o que ele geralmente fez na Internet, que páginas visitou, se falou com alguém em *chats* e quais assuntos.
- Explique a ele os riscos que existem no mundo virtual para que ele tenha sempre cuidado.
- Alerte para qualquer *spam* ou *e-mails* indesejados. Ele não tem que abrir emails ou arquivos de pessoas que não conheça porque existem programas que podem roubar suas senhas.
- Nunca deve revelar nenhum dado pessoal na Internet
- Deve sempre utilizar os controles de privacidade das redes sociais.
- O computador deve estar em algum lugar onde possa estar sempre à vista de outros membros da família, ainda mais se tiver webcam.
- Verifique de vez em quando o histórico de navegação para conhecer que páginas foram visitadas.
- Insista que ele não tem que enviar fotos, vídeos, nem ativar a webcam a pessoas que ele não conhece.
- Verifique sua lista de amigos nas redes sociais e comprove que ele não adicionou pessoas desconhecidas.

Além de seguir estes conselhos, é muito importante utilizar um bom software com filtro de conteúdo e controle dos pais avançado como o que oferecido pela Vivo Portal de Segurança, chamado Vivo Filhos Online.

11) ***Cyberbullying* / Assédio virtual**

São ofensas e intimidações postadas nas redes sociais – este tipo de perigo na Internet está em primeiro lugar entre as denúncias recebidas pela ONG Safernet no ano passado. Comentários e postagens que demonstrem racismo, homofobia, intolerância religiosa e xenofobia são os mais comuns nesse tipo de *bullying*. “Ainda tem gente que não leva em consideração que quando está online precisa considerar todas as regras de convivência e cidadania, respeito ao outro, respeito às leis. Todas as leis valem também na internet”, afirma Rodrigo Nejm, diretor da Safernet (G1, 2018).

12) ***Happy slapping***

É uma forma de *cyberbullying* que ocorre quando uma ou várias pessoas agridem um indivíduo enquanto o incidente é gravado para ser transmitido nas redes sociais (MENDOZA, 2018).

13) ***Sexting***

Sexting é um exemplo de uso da Internet para expressão da sexualidade na adolescência. É um fenômeno no qual os adolescentes e jovens usam redes sociais, aplicativos e dispositivos móveis para produzir e compartilhar imagens sensuais, de nudez e sexo. Envolve também mensagens de texto eróticas com convites e insinuações sexuais para namorado(a), pretendentes e/ou amigos(as). A palavra *sexting* já indica um gap entre o discurso adulto e a experiência dos jovens. Quando se pergunta aos adolescentes sobre *sexting*, nem sempre eles conhecem ou usam essa palavra. É a junção da palavra *sex* (sexo) + *texting* (torpedo), tem origem inglesa e surgiu quando a Internet nem era 3G e as pessoas enviavam mensagens de texto por SMS (*Short Message Service*) de caráter erótico e sexual, hoje as mensagem são fotos e vídeos por MMS (*Multimedia Messagem Service*) (SAFERNET, 2019).

Este tipo de perigo está em terceiro lugar em denuncias feitas a ONG Safernet (G1, 2018).

Como se prevenir?

- Não partilhe fotografias íntimas. Muito menos com estranhos, mesmo que insistam para que o faça;
- Não envie conteúdos privados para atrair a atenção da pessoa de quem gosta. Se não for recíproco, essa pessoa pode acabar por divulgar as suas mensagens só por divertimento;
- Não use o *sexting* como forma de pregar partidas ou de fazer piada. Este é um assunto sério, que pode trazer muitos problemas;
- Não publique fotos íntimas nas redes sociais. Há sempre alguém disposto a usá-las contra si.

O que fazer se estes conteúdos forem tornados públicos?

- Não comente as imagens ou vídeos publicados nas redes sociais. Evitará, assim, atrair ainda mais atenção.
- É possível minimizar as consequências negativas publicando conteúdos positivos nas redes sociais. A melhor forma de fazer frente a esta situação é ignorar todos os comentários que tenham a ver com o incidente;
- Independentemente da plataforma onde publicaram estes conteúdos íntimos, recomendamos que alerte o administrador do espaço para informa-lo que essas imagens ou vídeos foram publicados sem o seu consentimento. Neste caso, a plataforma é obrigada a eliminá-los;
- Se estas recomendações não forem suficientes, o melhor é contratar um advogado e informar-se acerca da legislação em matéria de proteção de dados pessoais e distribuição de pornografia infantil;
- Denunciar o delito aos organismos pertinentes, nomeadamente à Polícia Judiciária e Polícia de Segurança Pública (PSP), pelo *site* da SAFERNET através do endereço http://www.safernet.org.br/site/denunciar ou pelo disque 100.

14) **Sextorsão**

É a chantagem realizada a crianças ou adolescentes por meio de mensagens intimidadoras que ameaçam propagar imagens sexuais ou vídeos gerados pelas próprias vítimas. A intenção da pessoa que realiza uma o extorsão é a de continuar com a exploração sexual e/ou ter relações sexuais com a vítima (MENDOZA, 2018).

Como se prevenir?

Não realizar o *sexting*.

15) ***Cyberstalking***

A expressão *cyberstalking* é oriunda da palavra em inglês *stalk* que significa perseguir. Semanticamente, consiste no uso de ferramentas tecnológicas com o objetivo de perseguir ou assediar uma pessoa. É a versão virtual do termo *stalking*, conceituado como o comportamento de perseguição e/ou ameaças repetitivas contra uma pessoa e que podem ser manifestados por meio de ações como: seguir a vítima em seu trajeto, aparecer repentinamente em sua casa ou local de trabalho, realizar ligações telefônicas inconvenientes e até mesmo invadir a residência da vítima. Pode incluir também alegação de falsas acusações, monitoramento, ameaças, roubo de identidade, dano a dados ou equipamentos, solicitação de sexo a menores de idade ou aquisição de informações para uso prejudicial

Como se prevenir?

- Faça boas escolhas online. Evite divulgar dados como endereço, local de trabalho/estudo ou telefone em redes sociais, sempre configurando o perfil para que apenas pessoas próximas tenham acesso as suas informações.
- Tenha cuidado com quem se relaciona e com quem conversa online, nunca podemos ter certeza de quem está do outro lado da tela.
- Caso esteja sendo vítima de *stalking*, grave todas as possíveis provas, particularmente aquelas que são explicitamente abusivas ou ameaçadoras, pois estas podem servir de evidências para ser registrado um boletim de ocorrência por meio das autoridades.
- Não interaja com a pessoa que perseguir ou assediar, pois isso pode reforçar o comportamento dela para continuar tendo alguma forma de contato com você.
- Bloqueie o contato do *stalker* em suas redes sociais e denuncie no próprio serviço.

16) ***Fake News***

Não é de hoje que mentiras são divulgadas como verdades, mas foi com o advento das redes sociais que esse tipo de publicação se popularizou. A imprensa internacional começou a usar com mais frequência o termo *fake News* durante a eleição de 2016 nos Estados Unidos, na qual *Donald Trump* tornou-se presidente. *Fake News* é um termo em inglês e é usado para referir-se a falsas informações divulgadas, principalmente, em redes sociais.

Um exemplo do dano que pode causar uma *Fake News* foi o que aconteceu com Fabiane Maria de Jesus, morta por linchamento em 2014 no Guarujá, em São Paulo. Ela foi confundida com uma sequestradora que agiria na cidade e que teve o retrato divulgado no *Facebook*. Dias depois, foi descoberto que nem sequer a suspeita era ligada ao caso (VARGAS, 2019).

17) **Uso em excesso da tecnologia**

Ver o uso excessivo como uma patologia tem sido uma discussão entre os profissionais de psiquiatria e psicologia. A corrente que defende o comportamento como patologia associa o excesso de uso da Internet a tratamentos para transtorno

compulsivo e dependência. Mas é preciso problematizar essa visão psicopatológica, pois quando há algum sofrimento ou transtorno, o uso excessivo pode ser consequência e não causa. Ou seja, um transtorno de ansiedade, depressão ou uma inibição podem estar associados ou contribuindo para o uso patológico da Internet e deve ser tratado integralmente nas disfunções que provoca.

Além disso, se cada vez há mais mobilidade para a tecnologia e os dispositivos estão incorporados em nossas vidas, permitindo que fiquemos sempre online, como identificar que o uso está exagerado? Para identificar o uso excessivo é importante considerar não apenas o tempo de uso da Internet, mas especialmente a qualidade desse uso.

Criança e adolescente não conseguem sair da internet e resistem a atividades que incluem hábitos diários, como tomar banho e se alimentar. Além disso, o uso excessivo se caracteriza por ser uma atividade repetitiva e muito pouco criativa. Ou seja, não é só o tempo de uso, mas o modo como ele navega na rede e o impacto na vida do usuário como um todo. O uso excessivo não é um transtorno em si, ele pode ser uma forma de revelar outros problemas ou sofrimentos.

Como agir para evitar o uso excessivo, principalmente da Internet

- Proibir o uso não educa, nem previne. Diálogo e negociação são palavras-chave para estabelecer regras e limites;
- Estipule horários para que o uso não atrapalhe outras atividades;
- Lembre-se que quanto menor for a criança, menor deve ser o tempo de uso. Um desenvolvimento saudável é aquele rico de oportunidades de aprendizagem e lazer, diversifique as oportunidades que oferece ao seu filho;
- Incentive a busca de soluções criativas dos próprios adolescentes e jovens, envolvê-los no problema.
- Lembre-se: Internet não é babá eletrônica! Os pais precisam acompanhar a navegação dos filhos, especialmente nos primeiros anos.

AS REDES SOCIAIS E OS SEUS PERIGOS

Quando falamos em rede social, o que vem à mente em primeiro lugar são sites como *Facebook*, *Twitter* e *LinkedIn* ou aplicativos como Snapchat e Instagram, típicos da atualidade. Mas a ideia, no entanto, é bem mais antiga: na sociologia, por exemplo, o conceito de rede social é utilizado para analisar interações entre indivíduos, grupos, organizações ou até sociedades inteiras desde o final do século XIX.

Na internet, as redes sociais têm suscitado discussões como a da falta de privacidade, mas também servido como meio de convocação para manifestações públicas em protestos. Essas plataformas criaram, também, uma nova forma de relacionamento entre empresas e clientes, abrindo caminhos tanto para interação quanto para o anúncio de produtos ou serviços.

Foi na década de 1990, com a internet disponível, que a ideia de rede social migrou também para o mundo virtual. Criado em 1997, o site SixDegrees.com é creditado por muitos como a primeira rede social moderna, pois já permitia que usuários tivessem um perfil e adicionassem outros participantes, em um formato parecido com o que conhecemos hoje.

O site pioneiro, que em seu auge chegou a ter 3,5 milhões de membros, foi encerrado em 2001, mas já não era o único. No início do milênio, começaram a brotar páginas voltadas à interação entre usuários: *Friendster*, *MySpace*, Orkut e hi5 são alguns exemplos de sites ilustres no período. Muitas das redes sociais mais populares em atividade no momento também surgiram nessa época, como *LinkedIn* e *Facebook*.

Até recentemente, pouca gente imaginava que as redes sociais teriam um impacto tão grande quanto possuem hoje. Mas o desejo de se conectar com outras pessoas de qualquer lugar do mundo tem feito com que pessoas e organizações estejam cada vez mais imersas nas redes sociais.

Mas, as redes sociais têm o seu lado obscuro. Ela tem sido utilizada por pessoas inescrupulosas, por aliciadores, por pedófilos, entre outros para realizarem vários crimes. Segundo Vargas (2019) 70% dos ataques às pessoas que utilizam as redes sociais, são mulheres.

A "vida virtual" e os crimes da vida real

No Brasil ainda são poucos os crimes virtuais que são tipificados, mas, alguns crimes da vida real também são crimes e passiveis de punição no mundo virtual tais como:

- Homofobia é uma violação contra os Direitos Humanos que consiste na intolerância, discriminação, ofensa ou qualquer manifestação de repúdio à homossexualidade e à homoafetividade. A homossexualidade não pode ser considerada doença nem distúrbio mental, pois significa a livre orientação de indivíduos saudáveis, responsáveis e consciente dos seus direitos enquanto cidadãos.
- Racismo é crime e qualquer tipo de preconceito baseado na ideia da existência de superioridade de raça, manifestações de ódio, aversão e discriminação que difundem segregação, coação, agressão, intimidação, difamação ou exposição de pessoa ou grupo está qualificada por Lei, passível de punição como violação dos Direitos Humanos. A discriminação refere-se ao ato de fazer uma distinção. É importante diferenciar raça de etnia. A raça de uma pessoa é expressa pelas características visíveis, ou seja, físicas, tais como tonalidade de pele, formação do crânio e do rosto, e tipo de cabelo. Na etnia, além das características físicas, são considerados outros aspectos como cultura, nacionalidade, afiliação tribal, religião, língua e tradições, que entram em outras classificações quando alvo de discriminação, mas são tratados igualmente perante a Lei, ou seja, como crime.
- Neonazismo é crime também para quem propaga a ideologia na web. Consiste na intolerância com base na ideologia nazista de superioridade e pureza de determinada raça com recursos de agressão, humilhação e discriminação. No caso específico do neonazismo, está incluído quem fabrica, comercializa, distribui ou veicula símbolos, emblemas, ornamentos, distintivos ou propaganda com símbolos (como a cruz suástica) e defesa do pensamento nazista.
- Ameaçar alguém, por palavra, escrito ou gesto, ou qualquer outro meio simbólico, de causar-lhe mal injusto e grave.
- Caluniar alguém, imputando-lhe falsamente fato definido como crime.
- Difamar alguém, imputando-lhe fato ofensivo à sua reputação.
- Injuriar alguém, ofendendo-lhe a dignidade ou o decoro.
- Falsa Identidade é atribuir-se ou atribuir a terceiro falsa identidade para obter vantagem, em proveito próprio ou alheio, ou para causar dano a outrem:

CONCLUSÕES

Não há dúvidas quanto ao grande benefício que foi a criação do computador e, posteriormente, a criação da Internet. Muito ajuda nas tarefas que realizamos, mas, devemos pensar que sempre existe algum que os utilizam para realizarem crimes, maldades com outros usuários. Não sou contra a sua utilização, mas, sou mais a favor

da sua utilização com conhecimento, com cautela, sabendo dos perigos que rondam esse ambiente.

AGRADECIMENTOS

Agradeço a minha querida esposa Leila Gomes por sua paciência neste período em que me encontro atarefado e assim negligenciando a atenção devida a ela. Agradeço também a minha orientadora a Professora Doutora Sônia Regina Mendes dos Santos, pelo sua dedicação e empenho em me orientar no que escrevo e como escrevo para que vire, um dia, a minha dissertação de mestrado.

REFERÊNCIAS

FOLHA. Caderno de Informática: Especial Internet 30 anos. **Folha de São Paulo**, São Paulo, 20 out. 1999.

FONSECA, Guilherme de Souza. **A trajetória de um provedor de acesso a internet: o caso da Interaccess no período de 1995 a 2001.** Florianópolis, SC, 2001. Disponível em: https://repositorio.ufsc.br/xmlui/bitstream/handle/123456789/79523/185359.pdf?sequence=1&isAllowed=y. Acesso em: 03/11/2019.

G1. **Internet pode oferecer riscos para crianças e adolescentes**. 2018. Disponível em: https://g1.globo.com/profissao-reporter/noticia/2018/11/29/internet-pode-oferecer-riscos-para-criancas-e-adolescentes.ghtml. Acesso em: 6/11/2019

INTERNET World. Rio de Janeiro, Mantelmedia, v. 2, n. 15, 1996.

_____ . Rio de Janeiro, Mantelmedia, n. 5, 1996ª.

KAHN, Robert; DENNIS, Michael Aaron. Internet. **Britannica Academic 250 anniversary**, 2019. Disponível em: https://academic-eb-britannica.ez204.periodicos.capes.gov.br/levels/collegiate/article/Internet/1458. Acesso em: 28/10/2019.

KOVACS, Michelle H; FARIAS, Salomão A. Dimensões de Riscos Percebidos nas Compras Pela Internet; **REA-eletrônica**, v. 3, n. 2, Art. 12, 2004.

RNP. **Guia do Empreendedor Internet/Brasil** - Versão 1.0. Abril, 1996. 47 p.

_____. **Guia do Usuário Internet/Brasil** - Versão 2.0. Abril, 1996a. 72 p.

SECNET. Perigos da internet. **Quais são e como se prevenir**. 2019. Disponível em: https://www.secnet.com.br/blog/perigos-da-internet. Acesso em: 06/11/2019

VERMELHO, Sônia Cristina; MACHADO, Ana Paula; BERTONCELLO, Velho Valdecir. Sobre o conceito de redes sociais e seus pesquisadores. **Educ. Pesqui.**, São Paulo, v. 41, n. 4, p. 863-881, out./dez. 2015.

UOL, **5 grandes perigos da Internet**, 2013. Disponível em: https://seguranca.uol.com.br/antivirus/dicas/curiosidades/5-grandes-perigos-da-internet.html#rmcl. Acesso em: 06/11/2019.

MENDOZ, Miguel Angel. **Os 10 principais riscos na Internet para crianças e adolescentes**, Welivesecutity, 2018. Disponível em:

https://www.welivesecurity.com/br/2018/05/21/principais-riscos-na-internet-para-criancas-e-adolescentes/. Acesso em: 06/11/2019.

SAFERNET. https://new.safernet.org.br/, 2019. Acessado em: 06/11/2019.

VARGAS, André. Os perigos das redes sociais. **Revista Isto É**, edição 2601, 2019. Disponível em: https://istoe.com.br/os-perigos-das-redes-sociais/.Acesso em: 05/11/2019