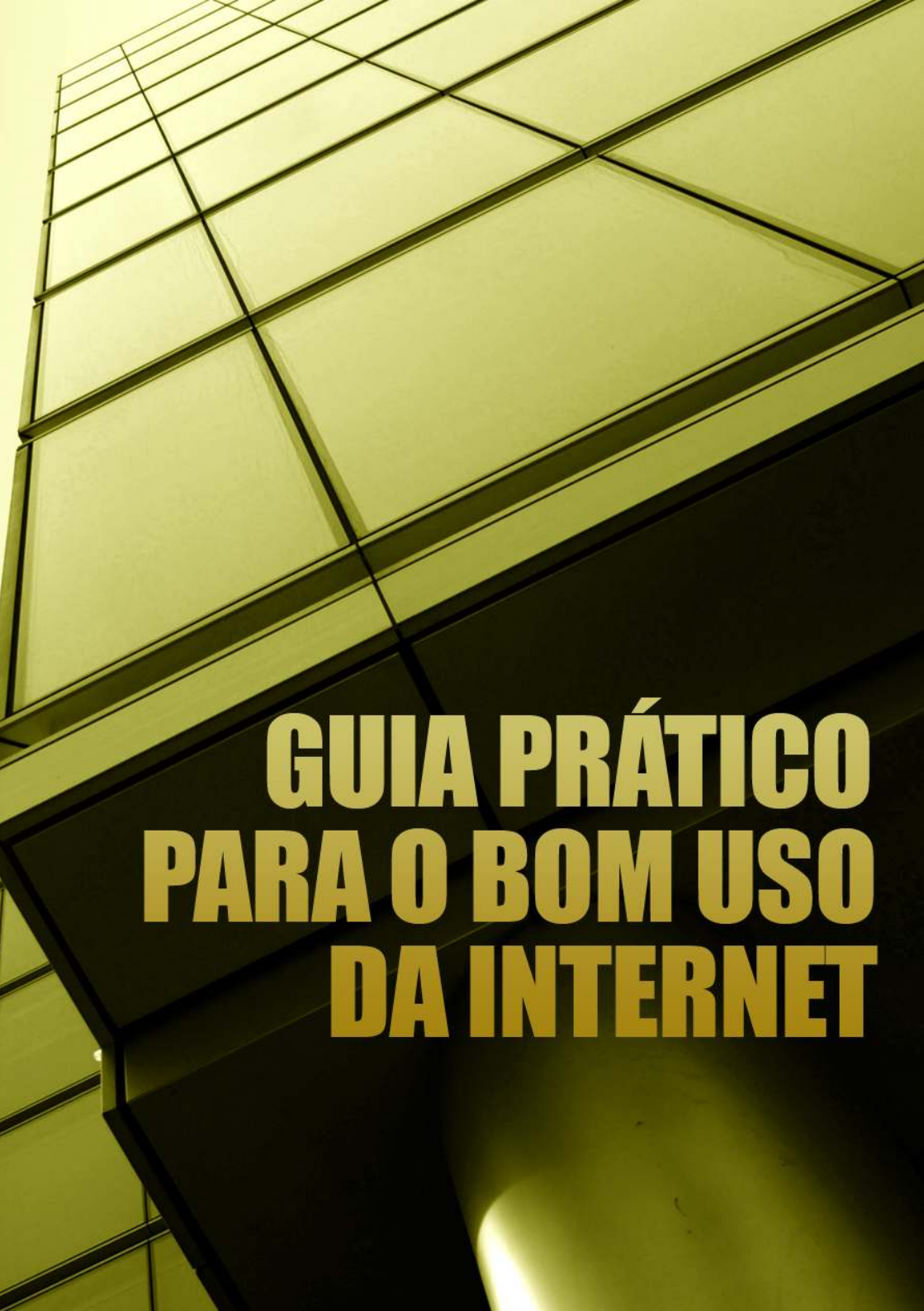

GUIA PRÁTICO PARA O BOM USO DA INTERNET

MARIANI, SANTOS & ADVOGADOS ASSOCIADOS
Rua Desembargador Motta, 3588 | Mercês | Curitiba | Paraná
Fone [41] 3335-5577 | Fax 3335-2665

www.marianiesantos.com.br

© MARIANI, SANTOS & Advogados Associados. Todos os direitos reservados.

SUMÁRIO

APRESENTAÇÃO

A internet e as novas tecnologias revolucionaram a forma como as pessoas se comunicam e se relacionam, buscam informações e são informadas sobre seus interesses. Atualmente, isto se aplica principalmente aos jovens e crianças, que têm estas ferramentas como parte fundamental do seu dia-a-dia, seja para estudo ou para lazer.

Isso significa facilidade de acesso a um manancial de recursos que são indispensáveis a sua educação e desenvolvimento, como também pode significar toda uma série de novos riscos, perigos e ameaças que poderão não ser do conhecimento de famílias, escolas e comunidades. Assim, se usadas de forma irresponsável e não segura, as novas tecnologias de informação e comunicação podem gerar além de benefícios muitos problemas.

O **GUIA PRÁTICO PARA O BOM USO DA INTERNET** tem foco pedagógico e o objetivo principal é ensinar os jovens a lidar com a tecnologia de forma simples e segura, levando ao seu conhecimento, bem como de pais e professores, quais são as implicações jurídicas advindas do mau uso da internet, as formas de ataque ao computador e dicas de prevenção.

Vale ressaltar que apenas as ferramentas tecnológicas não são suficientes para garantir a segurança em tecnologia da informação. Portanto, deve haver um acompanhamento dos pais e educadores para ensinar nossos jovens a se protegerem dos riscos da internet.

É papel de pais e educadores atuarem conjuntamente nesta "luta diária" para orientar nossos jovens a usar de forma

responsável e consciente a internet. Assim, o **GUIA PRÁTICO PARA O BOM USO DA INTERNET** não tem a pretensão de esgotar o assunto, mas servir como manual básico para pais e educadores nesta árdua tarefa educacional.

Antonio Carlos Mariani

Guilherme G.R.P. dos Santos

Helio Augusto Camargo de Abreu

1. Segurança da Informação

Segurança é o ato ou efeito de se ver livre de perigo ou de risco.

1.1. Propriedades de Segurança da Informação

A Segurança de Informação é garantida pela preservação de aspectos essenciais

- Confidencialidade: o principio da confiabilidade é respeitado quando apenas as pessoas explicitamente autorizadas podem ter acesso a informação;

- Integridade: o princípio da integridade é respeitado quando a informação acessada esta completa, sem alterações e, portanto, confiável;

- Disponibilidade: o princípio da disponibilidade é respeitado quando a informação está acessível, por pessoas autorizadas, sempre que necessário.

Destacam-se ainda outros princípios:

- Vulnerabilidade: pode causar, intencionalmente ou não, a quebra de um ou mais dos três princípios da Segurança da Informação;

- Ameaça: é um agente externo que aproveitando-se das vulnerabilidades presentes no hardware e software, poderá quebrar a confidencialidade, integridade e a disponibilidade da informação;

- Probabilidade: é a chance de uma falha de segurança ocorrer levando-se em conta o grau de vulnerabilidades presentes no hardware e software e

o grau de ameaças que possam explorar estas vulnerabilidades;

· Impacto: o impacto de um incidente são as potenciais consequencias que poderão ser causadas ao usuário, hardware e software.

1.2. A importância do cuidado com a Segurança no uso do computador

· Prevenir o furto de senhas e números de cartão de créditos;

· Bloquear a utilização da conta de acesso a internet por terceiros não autorizados;

· Impedir que os dados pessoais, ou até comerciais dos usuários sejam alterados, furtados, apagados ou visualizados.

1.3. Senhas

Deve-se ter todo o cuidado na elaboração das senhas de acesso comumentemente utilizadas na Internet. Portanto, não devem ser utilizados na sua elaboração nomes, sobrenomes, números de documentos, placas de carro, números de telefone e nenhuma data que possa ser relacionada ao usuário, como por exemplo, datas de aniversário.

Assim, para dificultar que terceiros através de softwares específicos tentem descobrir a senhas, é interessante que o usuário crie uma senha bem "embaralhada", pois mais difícil será descobri-la e cuide para memorizá-la e não anotar no celular ou papel que outras pessoas tenham fácil acesso.

Uma sugestão é tentar misturar letras maiúsculas, minúsculas, números e sinais de pontuação.

Atenção!!!

- Certifique-se de não estar sendo observado ao digitar a senha;

- Não forneça sua senha em hipótese alguma para estranhos;

- Havendo a necessidade de realizar operações na internet que precise utilizar as senhas, fuja de computadores de *Lan Houses, cybercafés, stands de eventos, etc.*

- Averiguar se seu provedor de acesso a internet possui sistema de criptografia.

1.4. Dicas de segurança em sua residência:

- **Sempre sair do programa pela opção sair/logout;**

- **Crie uma lista com regras da casa para o uso da Internet com seus filhos adolescentes. Você deve incluir os tipos de sites que estão fora dos limites, o número de horas que podem passar na Internet e orientações sobre comunicação online, incluindo comunicação em salas de bate-papo.**

- **Mantenha os computadores conectados à Internet em áreas comuns da casa, não nos quartos dos adolescentes.**

- **Converse com seus filhos sobre seus amigos virtuais e suas atividades online, da mesma forma que conversa sobre suas outras atividades. Converse com seus filhos sobre a sua lista de contatos em programas de mensagens instantâneas e instrua-os a não falar com**

estranhos.

- Saiba sempre quais são as salas de bate-papo ou grupos de discussão que seus filhos estão visitando e com quem estão conversando online. Incentive-os a usar salas de bate-papo monitoradas e insista para que permaneçam em áreas de bate-papo públicas.

- Ensine-os a nunca fornecer informações pessoais sem a sua permissão ao usar email, salas de bate-papo ou mensagens instantâneas, preencher formulários de registro e perfis pessoais ou participar de competições online.

- Ensine-os a não baixar programas, música ou arquivos sem a sua permissão. Explique que se compartilharem arquivos ou copiarem texto, imagens e trabalhos artísticos da Web, eles podem estar violando leis de direitos autorais e que isso pode ser ilegal.

- Incentive-os a lhe contar se algo ou alguém online fizer com que se sintam desconfortáveis ou ameaçados. Mantenha a calma e lembre-os de que não estão fazendo nada de errado se quiserem lhe mostrar algo. (É importante deixar claro que eles não irão perder o direito de usar o computador.).

- Converse com seus filhos sobre conteúdo adulto e pornografia online e oriente-os a sites positivos sobre saúde e sexualidade.

- Ajude a protegê-los contra spam. Instrua-os a não fornecer seu endereço de email online, não responder a mensagens de lixo eletrônico e a usar filtros de email.

- Esteja atento aos sites da Web que seus filhos

freqüentam. Verifique se não estão visitando sites com conteúdo ofensivo ou publicando informações pessoais ou fotos de si mesmos online.

- Ensine-os a ter um comportamento responsável e ético online. Eles não devem usar a Internet para espalhar fofocas, intimidações ou ameaças aos outros.

- Deixe claro que devem sempre consultar você antes de realizar qualquer transação financeira online, inclusive encomendar, comprar ou vender itens online.

- Converse com eles sobre os jogos de azar online e seus riscos potenciais. Lembre-os de que os jogos de azar online são ilegais para eles.

- Pesquise sobre ferramentas de filtragem da Internet (como o Controle de Menores do MSN Premium, em inglês), que devem ser usadas como um complemento à supervisão paterna, não uma substituição.

- Permita que seus filhos usem apenas salas de bate-papo monitoradas em sites infantis reconhecidos.

- Para que seu filho não participe de atividades online sem o seu conhecimento, dê a eles uma conta de usuário (em inglês) limitada.

- Incentive-os a lhe contar se algo ou alguém online fizer com que se sintam desconfortáveis ou ameaçados. Mantenha a calma e lembre-os de que não estão fazendo nada de errado se quiserem lhe mostrar algo. Elogie o seu comportamento e incentive-os a procurá-lo novamente se a mesma

coisa acontecer de novo. Leia mais sobre como lidar com os predadores online e os intimidadores virtuais.

- Insista em ter acesso às contas de email e de mensagens instantâneas para ter certeza de que não estão falando com estranhos.

- Incentive seus filhos a compartilhar suas experiências na Internet com você. Divirta-se na Internet junto aos seus filhos.

- Se seus filhos visitam salas de bate-papo, usam programas de mensagens instantâneas, videogames online ou outras atividades na Internet que exijam um nome de logon como identificação, ajude-os a escolher um nome que não revele nenhuma informação pessoal sobre eles.

- Insista para que nunca informem seu endereço residencial, número de telefone ou outras informações pessoais, como onde estudam ou onde gostam de brincar.

- Ensine a seus filhos que a diferença entre certo e errado na Internet é a mesma que na vida real.

- Insista para que respeitem a propriedade de outros online. Explique que fazer cópias ilegais do trabalho de outras pessoas, como música, videogames e outros programas, é roubo.

- Diga a eles que não devem nunca encontrar amigos virtuais pessoalmente. Explique que os amigos virtuais podem não ser quem eles afirmam ser.

- **Ensine a eles que nem tudo o que lêem ou vêem online é verdade. Encoraje-os a perguntar a você se não tiverem certeza.**

2. Dos meios de comunicação na internet

2.1. E-mail

Serviço de envio e recebimento de mensagens eletrônicas através da internet. Importante destacar que o e-mail pode sofrer violação de privacidade, pois até chegar ao verdadeiro destinatário, as mensagens eletrônicas são passíveis de prévia leitura e até adulteração. Tais atitudes constituem crime, previsto no código penal no art. 151, *in verbis*:

"Devassar indevidamente o conteúdo de correspondência fechada, dirigida a outrem."

Ferem, também, o art. 5º, inciso XII, da Constituição Federal:

"É inviolável o sigilo da correspondência e das comunicações telegráficas, de dados e das comunicações telefônicas, (...)"

Atenção!!!

- Atualmente circulam na internet muitas informações falsas e golpes que são encaminhadas

nas mensagens;

- Criminosos podem se aproximar para prejudicar, difamar e roubar;

- Crianças podem receber conteúdos impróprios e até serem aliciadas;

- Método mais utilizado para espalhar vírus;

- Atenção àquelas propostas boas demais ou produtos milagrosos, geralmente são fraudes;

- Os protocolos POP3 e SMTP não são criptografados. Se uma pessoa conseguir acessar a rede na qual o servidor esteja executando o serviço POP3, ela poderá ler os emails dos usuários;

- Ao sair do programa click em sair/logout;

- Você pode configurar sua conta para bloquear contatos indesejados;

- Troque sua senha periodicamente;

- Não aceite nem abra e-mail de desconhecidos! Simplesmente apague sem ler;

- Procure sempre saber a origem da informação e se o responsável é de confiança ou conhecido;

- Atenção com cartões virtuais. Não abra quando o nome do arquivo tiver "**.exe**" no final;

- Não mostre nas mensagens seu endereço, número pessoal, informações de seus familiares e outros detalhes;

- Mantenha sempre atualizado o anti-vírus e use

anti-spam;

· Jamais acredite em pedidos de pagamento, correção de senhas ou pedido de qualquer dado pessoal por e-mail. Comunique-se por telefone com a instituição que supostamente enviou o e-mail e confira do que se trata.

2.2. Chat – Salas de Bate Papo

É um serviço oferecido na Internet onde o usuário pode conversar com várias pessoas ao mesmo tempo, é um correio eletrônico on-line, ao vivo, em que você lê ao mesmo tempo a mensagem enviada e sua resposta. É um bate-papo de várias pessoas numa sala virtual. A pergunta e resposta são enviadas, simultaneamente, a todos os participantes da sala. São conhecidas como Salas de Bate Papo e são divididas por temas, idade ou preferências.

Atenção!!!

· Cuidado com os estranhos, pois as salas são abertas ao público em geral;

· Por vezes os freqüentadores inventam falsos perfis e mentem para tentar ganhar confiança e prestígio;

· Em muitas salas as conversas são impróprias para crianças que podem entrar sem serem identificadas;

· Nas salas de chat/bate papo os freqüentadores costumam utilizar apelidos, o que pode facilitar a ação de criminosos, pois dificultam a identificação;

· Ao sair do programa click em sair/logout e nunca forneça dados pessoais;

- Sempre mantenha seus pais informados de suas ações na internet. Portanto jamais vá ao encontro de pessoas que você acabou de conhecer no chat ou que não conheça pessoalmente sem a concordância dos seus pais;

- Caso uma pessoa insista a conhecer você pessoalmente chame um adulto imediatamente;

- Tempo de conversa não garante a confiança nem a verdade das informações, tome cuidado;

- Caso receba mensagens ou imagens agressivas que tentem forçar uma conversa, bloqueie o usuário, denuncie e peça ajuda;

2.3. Comunicadores instantâneos

São programas instalados no seu computador, no qual você adiciona endereços de pessoas que utilizam o mesmo software, para enviar e receber mensagens instantâneas, em tempo real, através de texto, voz e/ou vídeo.

As conversas podem ser feitas entre duas ou mais pessoas num ambiente privado, diferentemente dos Chats que geralmente tem ambientes abertos para todas as pessoas conectadas. Exemplos de programas gratuitos: MSN, ICQ, Yahoo Messenger, Google Talk.

Atenção!!!

- Suas fotos podem ser alteradas através de softwares de editoração de imagens para prejudicar você;

- Pessoas mal intencionadas se passam por " amigos virtuais" e mentem para seduzir, intimidar e

ofender outros internautas.

- Mantenha o programa sempre atualizado para evitar vulnerabilidades;

- Comunique-se somente com quem você conheça, ignore os estranhos;

- Jamais aceite o convite de estranhos para utilizarem a *Webcam*, pois você poderá estar abrindo a porta da sua casa para um criminoso;

- Configure o programa para ocultar seu endereço de IP;

- Não utilize o sistema de entrada automática do programa no computador, principalmente se usar em *Lan House*, Infocentro, ou qualquer local de acesso público;

- Cuidado com o conteúdo dos arquivos que recebe, pois pode conter algo agressivo ou mesmo ilegal;

- Ao receber um arquivo ou mensagem que insulte você, peça ajuda para gravar no seu computador. Caso não seja possível chame um adulto para que seja feita uma ata notarial* e bloqueie o contato em sua lista.

***IMPORTANTE:** Ata notarial é o ato unilateral do notário ou tabelião, de natureza declaratória, visando o relato escrito de um determinado fato, que deve ser narrado como conteúdo desse documento, que servirá como prova para eventual ação judicial.

Em outras palavras, na "ata notarial" o tabelião relata, livremente, de acordo a sua percepção, o que vê, ouve, verifica e conclui, independentemente da interferência de

quem quer que seja.

Assim, na ocorrência de qualquer evento que venha a prejudicar-lhe na internet chame o notarial até sua casa ou leve o computador até o cartório imediatamente para que a imagem, arquivo, etc, não seja deletado pelas pessoas mau intencionadas.

2.4. Rede de relacionamentos

São sites que permitem criar uma página pessoal na Internet, encontrar amigos, participar e criar comunidades para compartilhar gostos e idéias. Possibilita atualizar e divulgar um espaço pessoal na Internet com textos, fotos e vídeos. Hoje é um dos espaços preferidos pelos Internautas de todas as idades para se encontrarem e se relacionarem pela Internet. Exemplos: *Orkut*, *MySpace*, *Hi*5, *Facebook*, etc.

2.4.1. Twitter

É a mais nova sensação entre os jovens, a qual merece destaque. Sendo considerado o sistema de telégrafo da WEB 2.0, o *Twitter* é definido como uma rede social e serviço de *micro-blogging* que permite aos seus usuários enviar e receber atualizações de outros utilizadores. Essas atualizações são conhecidas como *twetts* e podem ter o tamanho máximo de 140 caracteres. Para participar você precisa, como em qualquer outra rede social, fazer um cadastro.

A grande novidade do *Twitter* é o ritmo. O site do *Twitter* tem uma pergunta básica – "O que você está fazendo?" – e todo mundo responde, várias vezes ao dia: contam que estão almoçando, dizem que o ônibus quebrou, avisam ter visto uma celebridade. Como é possível postar do celular, os twitteiros (como são comumente chamados) não descansam na narração do trivial. É um fluxo contínuo de minudências que os americanos chamam de

"intimidade ambiental". A comunicação é rápida e contínua, uma pequena e organizada gritaria digital. Visto de fora parece histérico, mas para os envolvidos soa natural.

Atenção!!!

- Jamais divulgue informações de cunho pessoal, pois elas tornam-se públicas;

- No *Twitter* JAMAIS passe informações sobre sua localização, tais como, onde seu pai acabou de deixar você, que esta indo assistir um filme em tal cinema, que irá para a casa de tal colega, o que esta fazendo, etc. Cuidado com as informações lançadas no *Twitter.*

- Não divulgue imagens de passeios, com sua família, com detalhes que possam identificar o local onde você costuma ir, Viagens que fez ou pretende fazer, veículos da família, foto com fachada de residências, de lugares que freqüenta, como bares, restaurantes, etc;

- Não exponha os detalhes de sua vida, sua intimidade é preciosa e não deve ser aberta para qualquer um;

- Os "cadeados" e bloqueios de acesso podem ser "quebrados" por pessoas mal intencionadas;

- Podem ser usadas para reunir criminosos e agressores;

- Seus dados podem ser roubados e manipulados para ofender e mesmo chantagear.

2.5. Blogs e Fotologs

São espaços na internet que podem ser criados por

qualquer internauta para publicar suas idéias, fotos, preferências, desejos e expectativas. Nos Blogs e Fotoblogs podemos debater diversos temas, fazer comentários, enquetes, compartilhar links e todas informações que consideramos interessantes. Podem ser individuais ou coletivos e geralmente são gratuitos. Os Fotologs são mais dedicados a fotos.

Atenção!!!

- As informações podem usadas contra você por pessoas mal intencionadas;

- Jamais publique qualquer comentário de conteúdo violento, difamatório, desrespeitoso, etc;

- A qualquer momento você pode apagar seu Blog ou Fotolog, mas uma vez publicado tudo pode ser gravado por outros e voltar ao ar;

- **VOCÊ É LEGALMENTE RESPONSAVEL POR TUDO O QUE PUBLICA**.

2.6. Redes P2P - Compartilhamento de arquivos

Conhecida como P2P (do inglês, peer-to-peer = ponto-a-ponto), é uma rede descentralizada de computadores que podem trocar entre si informações como músicas, vídeos, textos e programas. Exemplo: Emule.

Além das redes P2P há os sites de compartilhamento de arquivos. Livros, filmes, fotos e músicas ficam disponíveis em páginas na Intenet para que os internautas possam assistir e em alguns casos gravar. Exemplo: YouTube- visualização de vídeos, RapidShare -compartilhamento de arquivos.

Atenção!!!

- Ao receber arquivos impróprios e agressivos sem querer;
- Você pode receber arquivos contendo nomes falsos, disfarçando arquivos ilegais;
- Deixar seu computador vulnerável, facilitando a invasão para roubo de dados;
- Facilita a distribuição de vírus.

3. Do mau uso das novas Tecnologias de Informação e Comunicação (TIC)

3.1. CiberCrime - Crime Digital

Práticas criminosas utilizando meios eletrônicos como a Internet para ações ilícitas como roubo, chantagem, difamação, calúnia e violações aos direitos humanos fundamentais. Tais crimes podem ser classificados levando em conta o papel do computador no ilícito, quando ele for: (a) o alvo: crime de invasão, contaminação por vírus, furto de informação, vandalismo, etc; (b) instrumento para o crime: crime de fraude em conta corrente e/ou cartões de crédito, transferência de valores, divulgação e exploração de pornografia, etc; (c) incidental para outro crime: crimes

contra honra, jogo ilegal, lavagem de dinheiro, fraudes contábeis, etc; (d) associado com o comutador: pirataria de software, falsificação de programas, comércio ilegal de equipamentos e programas, etc.

Denúncias:

- www.cert.br;

- www.denunciar.org.br;

- Delegacia especializada em crimes eletrônicos: Polícia Civil do Paraná, Rua José Loureiro, 540, centro, Curitiba, Paraná, fone: (041) 3883 - 8100, E - mail: cibercrimes@pc.pr.gov.br.

Atenção!!!

· Pode acarretar prejuízos de ordem moral e material a qualquer pessoa;

· A falsa sensação de anonimato e impunidade faz com que a ocorrência desses cibercrimes aconteça;

· É totalmente cabível a utilização da atual legislação penal nos casos de crimes cometidos pela internet;

· Oportuno destacar que existem projetos em trâmites no Senado para a redução da maioridade penal.

3.2. CiberBullying

É a prática realizada através da internet que busca humilhar e ridicularizar os alunos, pessoas desconhecidas e também professores perante a sociedade virtual.

Apesar de ser praticado de forma virtual, o *cyberbullying* tem preocupado pais e professores, pois através da internet os insultos se multiplicam rapidamente e ainda contribuem para contaminar outras pessoas que conhecem a vítima.

Os meios virtuais utilizados para disseminar difamações e calúnias são as comunidades, e-mails, torpedos, blogs e fotologs.

Além de discriminar as pessoas, os autores são incapazes de se identificar.

Contudo, é importante dizer que mesmo anônimos, os responsáveis pela calúnia sempre são descobertos.

Atenção!!!

- Os agressores não se identificam;
- Como tudo na rede se multiplica, os ataques podem se prolongar por anos;
- Não de continuidade, não repasse mensagens que agridam outras pessoas, ao repassar você também está agredindo e também poderá ser responsabilizado;
- Tenha sempre em mente: ***"Não faça aos outros, aquilo que não gostaria que fizessem com você."***

3.3. Sexting

Fenômeno de fotografar ou filmar a si próprio em momentos de intimidade e transmitir as imagens por celular nasceu nos Estados Unidos, onde é chamado de "*sexting*" – neologismo que une *sex* (sexo) e *texting* (a troca de mensagem de texto pelo telefone). Em pouco tempo, a mania se espalhou como vírus. Não se trata de

cenas baixadas da internet, mas gravadas por colegas e distribuídas por tecnologias a que todo celular hoje em dia tem acesso, como o *Bluetooth*.

Uma pesquisa publicada em dezembro de 2008, comprova que, nos EUA, o *sexting* é mais comum do que imaginam os pais. Segundo o estudo, um em cada cinco jovens americanos com idade entre 13 e 19 anos já enviou pelo celular algum tipo de foto ou vídeo de si mesmo nu ou seminu. Para chegar ao resultado, a organização não governamental *National Campaign to Prevent Teen and Unplanned Pregnancy* (Campanha Nacional para Prevenção dos Jovens e Gravidez Não Planejada) ouviu 1.280 adolescentes americanos entre 13 e 26 anos. Entre os jovens de 20 a 26 anos, o fenômeno é ainda mais comum: um terço dos entrevistados declarou já ter praticado o *sexting.*

Todavia, o desfecho pode ser devastador. Em julho de 2008, uma adolescente americana se suicidou depois de um escândalo de *sexting*. Jessica Logan, então com 18 anos, queria presentear o namorado. Fotografou-se sem roupa e enviou pelo celular as imagens para o garoto. Quando o relacionamento de dois meses terminou, o jovem não hesitou em compartilhar as imagens da ex-namorada, uma líder de torcida loira, extrovertida e atraente, com os amigos de seu colégio, na cidade de Cincinnati. Em pouco tempo, a foto de Jessica percorreu sete colégios. A garota não aguentou as provocações. Chamada de "piranha" e "vagabunda", entrou em depressão e começou a faltar às aulas. Até que pôs um fim em sua vida.

Uma ONG de prevenção à gravidez nos EUA diz como evitar embaraços on-line:

PARA OS ADOLESCENTES

· Saiba que as mensagens e fotos que você postou

na internet podem ser passadas adiante;

- Nunca repasse fotos ou vídeos com conteúdo sexual. Resista à pressão de amigos curiosos que desejam ver as imagens ou vídeos eróticos que chegaram até você;

- Se você é uma garota, não ceda aos pedidos dos meninos para escrever conteúdo erótico ou mostrar partes do corpo pela *webcam* ou por fotos;

- Leve em consideração a reação de quem receberá sua mensagem ou foto. Um comentário com conteúdo sexual parece engraçado para quem escreve, mas pode soar ofensivo para outros;

- Lembre-se de que nenhum conteúdo que circula pelo celular ou pela internet é realmente anônimo. Fotos, mensagens e informações como e-mail e telefone podem cair na mão de estranhos que querem bisbilhotar sua vida

PARA OS PAIS

- Converse com seu filho para saber o que ele faz na internet. Os jovens devem entender que imagens enviadas pela internet ou pelo celular não são anônimas;

- Zele pelo bom comportamento on-line de seu filho. É impossível apagar os vestígios de uma foto ou vídeo que circularam pela rede;

- Conheça as amizades virtuais de seu filho. É tão importante quanto conhecer os amigos de verdade. Os adolescentes costumam tratar como "amigo" qualquer um de sua lista de contatos;

- Avalie a necessidade de restringir o tempo que

seu filho passa no celular ou computador. Evite que o jovem passe a madrugada navegando;

· Saiba o que seu filho está postando publicamente. Visitar o perfil dele no *Orkut* ou *Facebook* não é bisbilhotice.

3.4. Para Aliciamento ou Chantagem On-Line

Você ou algum conhecido seu recebe ou recebeu mensagens no celular, emails, recados no Blog ou no site de relacionamento com convites para encontro, imagens de sexo ou conteúdos impróprios para sua idade? Isto pode ser uma tentativa de aliciamento. Infelizmente na Internet também há pessoas mal intencionadas que buscam vítimas para abusar e até mesmo seqüestrar. Tome sempre muito cuidado para aproveitar a Internet sem correr este risco.

Atenção!!!

· Fingem-se amigos virtuais, são muito "amáveis" nas primeiras conversas de Chat e Comunicador Instanâneo (MSN...);

· Passam-se por crianças e aparentam conhecer o mundo infantil;

· Alguns se apresentam como adultos e enviam cenas de sexo com desenhos para estimular fantasias impróprias;

· Ficam elogiando demais para ganhar confiança e pedir informações como nome de escola, endereço, celular e fotos;

· Pedem cada vez mais fotos e depois solicitam conversas com Webcam;

- Podem manipular fotos e colocar o rosto em cenas de sexo;

- Ameaçam divulgar na Internet as fotos manipuladas para humilhar diante de amigos e familiares em sites, Email e Blogs;

- Ameaçam saber o endereço para agredir presencialmente em casa ou na escola;

- Nos piores casos pode terminar em seqüestro para abusar sexualmente das vítimas.

3.5. Predadores online: o que você pode fazer para minimizar o risco

Quando as crianças usam ferramentas de comunicação pela Internet, como salas de bate-papo, email e mensagens instantâneas, correm o risco de entrar em contato com predadores online.

O anonimato da Internet significa que a confiança e a intimidade podem evoluir rapidamente online.

Os predadores se aproveitam desse anonimato para criar relacionamentos online com jovens inexperientes.

Você pode ajudar a proteger seus filhos se estiver a par dos riscos relacionados à comunicação online e se estiver envolvido nas atividades de seus filhos na Internet.

Como os predadores online operam?

Os predadores estabelecem contato com crianças por meio de conversas em salas de bate-papo, mensagens instantâneas, email ou grupos de discussão. Muitos adolescentes usam fóruns de apoio online para lidar com seus problemas. Os predadores costumam procurar

vítimas vulneráveis nessas áreas online.

Os predadores online tentam seduzir gradualmente seus alvos oferecendo-lhes atenção, afeto, ternura e até mesmo presentes, e geralmente dedicam uma considerável quantidade de tempo, dinheiro e energia a esse esforço.

Eles estão informados sobre as músicas e passatempos do interesse dos jovens. Eles se mostram interessados nos problemas das crianças e demonstram empatia. A fim de tentar quebrar as inibições dos jovens, eles vão gradualmente introduzindo conteúdo sexual na conversa ou mostrando material sexualmente explícito.

Alguns predadores trabalham mais rápido que outros e já começam com conversas sexuais.

Esta abordagem mais direta pode incluir assédio, ou o predador pode perseguir a vítima. Os predadores também podem avaliar as crianças que conhecem online para futuro contato pessoal.

Que tipo de jovem corre maior risco?

Os adolescentes mais jovens são o grupo etário mais vulnerável e correm um alto risco com os predadores online.

Os adolescentes mais jovens tendem a explorar sua sexualidade, afastar-se do controle dos pais e procurar novos relacionamentos fora da família. Com o pretexto do anonimato, eles tendem a arriscar-se mais online, mesmo quando não compreendem bem as possíveis implicações.

Os jovens mais vulneráveis aos predadores online costumam ser:

- novatos nas atividades online e pouco familiarizados com a *netiqueta*;

- usuários agressivos de computador;

- o tipo que gosta de experimentar atividades novas e arriscadas na vida;

- carentes de atenção e afeto;

- rebeldes;

- solitários;

- curiosos;

- confusos com relação à sua identidade sexual;

- facilmente enganado por adultos;

- atraídos por grupos sociais diferentes do mundo de seus pais.

Os jovens sentem que estão a par dos perigos dos predadores, mas na realidade, são ingênuos quanto aos relacionamentos online.

Como os pais podem minimizar o risco de uma criança se tornar uma vítima?

- Converse com seus filhos sobre predadores sexuais e perigos potenciais online.

- Crianças pequenas não devem usar as salas de bate-papo, visto que os perigos são grandes demais. À medida que as crianças crescem, podem começar a participar de salas de bate-papo que sejam bem monitoradas e especiais para crianças. Incentive até mesmo os adolescentes a usarem salas de bate-papo

monitoradas.

- Se seus filhos participam de salas de bate-papo, informe-se sobre as salas que visitam e as pessoas com que conversam. Monitore as áreas de bate-papo você mesmo para ver que tipo de conversa acontece.

- Instrua seus filhos a nunca sair da área pública da sala de bate-papo. Muitas salas de bate-papo oferecem áreas privadas onde os usuários podem bater papo uns com os outros com privacidade, sem que os monitores do bate-papo possam ler essas conversas. Elas são chamadas de áreas de "sussurro".

- Mantenha o computador com conexão com a Internet em uma área comum de sua casa e não no quarto de seu filho. É muito mais difícil para um predador estabelecer um relacionamento com uma criança se a tela do computador estiver facilmente visível. Mesmo quando o computador está em uma área comum de sua casa, esteja presente enquanto eles estiverem online.

- Crianças pequenas devem compartilhar um endereço de email da família em vez de ter sua própria conta. À medida que crescem, você pode pedir ao seu provedor para configurar um endereço de email separado, mas as mensagens de seus filhos ainda devem residir na sua conta.

- Se todas as precauções falharem e seus filhos vierem a encontrar um predador online, não os culpe. A responsabilidade é sempre do criminoso. Tome medidas decisivas para que seu filho pare imediatamente de ter contato com essa pessoa.

Como seus filhos podem reduzir o risco de se tornarem vítimas?

Há várias precauções que as crianças podem tomar como, por exemplo:

- Nunca baixar imagens de uma fonte desconhecida. Elas podem ser sexualmente explícitas.

- Usar filtros de email.

- Contar para um adulto imediatamente se alguma coisa online fizer a criança se sentir desconfortável ou amedrontada.

- Escolher um nome de tela que não indique o sexo do usuário nem contenha palavras com conotação sexual ou revelem informações pessoais.

- Nunca revelar informações pessoais sobre si mesmos (inclusive idade e sexo) ou informações sobre sua família para ninguém online, e nunca preencher perfis pessoais online.

- Interromper qualquer comunicação por email, conversa por mensagens instantâneas ou bate-papos se alguém começar a fazer perguntas muito pessoais ou com conotação sexual.

- Colocar as regras da família sobre o comportamento online perto do computador para lembrar seus filhos de proteger sua privacidade na Internet.

Como saber se uma criança é alvo de predadores?

É possível que seus filhos sejam alvo de um predador online se:

- A criança ou adolescente passar muito tempo online. A maioria das crianças que são vítimas de predadores online, passam muito tempo online, especialmente em salas de bate-papo, e podem fechar a porta de seu quarto para manter suas atividades em segredo quando vão trabalhar no computador.

- Você encontrar pornografia no computador da família. Os predadores freqüentemente usam pornografia para intimidar sexualmente as crianças. Os predadores podem fornecer sites da Web, fotos e mensagens de email de conteúdo sexual para iniciar conversas de caráter sexual com suas vítimas potenciais. Os predadores podem usar fotos de pornografia infantil a fim de convencer uma criança de que é normal os adultos terem relações sexuais com crianças. Lembre-se de que seus filhos podem ocultar arquivos pornográficos em discos, especialmente se outros membros da família usarem o computador.

- Seu filho ou adolescente receber telefonemas de pessoas que você não conhece, ou fizer chamadas (às vezes interurbanas) para números que você não reconhece. Depois de estabelecer contato com seu filho online, alguns predadores online podem tentar entrar em contato com os jovens para tentar convencê-los a ter relações sexuais por telefone ou para tentar marcar um encontro pessoal no mundo real. Se as crianças hesitarem em fornecer o número de telefone de sua casa, os criminosos sexuais podem oferecer seus telefones. Alguns têm até números gratuitos, para que suas vítimas potenciais possam ligar para eles sem o conhecimento dos pais. Outros dirão às crianças para ligar a cobrar. Dessa forma, com o serviço de identificação de chamada, os predadores poderão determinar facilmente o número do telefone da criança. Não permita que seus filhos

encontrem pessoalmente um estranho que conheceram online sem a sua supervisão.

- Seu filho ou adolescente receber cartas, presentes ou pacotes de alguém que você não conheça. É comum aos criminosos enviar cartas, fotografias e presentes às vítimas potenciais. Os criminosos sexuais online podem até enviar passagens aéreas para incitar uma criança ou adolescente a encontrá-los pessoalmente.

- Seu filho ou adolescente se afastar da família e dos amigos, desligar o monitor do computador rapidamente ou mudar de tela quando um adulto entrar no quarto. Os predadores online esforçam-se muito por criar diferenças e distanciamento entre as crianças e suas famílias e geralmente fazem com que pequenos problemas familiares pareçam maiores. As crianças vítimas de abuso sexual apresentam tendência ao isolamento e à depressão.

- Seu filho estiver usando a conta online de outra pessoa. Mesmo as crianças que não têm acesso à Internet em casa podem ter contato com um criminoso ao usar a Internet na casa de um amigo ou em algum outro local público como, por exemplo, na biblioteca. Algumas vezes os predadores fornecem uma conta de computador a suas vítimas para poderem se comunicar.

O que você pode fazer se seu filho for alvo de predadores?

- Se seu filho receber fotos sexualmente explícitas de um correspondente online, ou se for aliciado sexualmente por meio de email, mensagens instantâneas ou algum serviço online, entre em contato com o departamento de polícia local. Guarde qualquer documentação, inclusive endereços de

email, endereços de sites da Web e registros em log de bate-papos para fornecer à polícia.

- Verifique se há arquivos pornográficos ou qualquer forma de comunicação sexual em seu computador – estes costumam ser sinais de que há algo errado.

- Monitore o acesso de seus filhos a todos os meios de comunicação eletrônica ao vivo, como salas de bate-papo, mensagens instantâneas e email. Os predadores online geralmente encontram suas vítimas potenciais em salas de bate-papo e continuam a se comunicar com elas por meio de email ou mensagens instantâneas.

4. Modalidades de invasão de privacidade pela Internet

4.1. Hackers e *crackers*

São termos distintos e que geram muita confusão, pois os *crackers* usam uma engenharia inversa, com o intuito de danificar quaisquer tipos de componentes eletrônicos, enquanto *hackers* agem a favor do bem, com ética. Inclusive muitas empresas contratam *hackers* para descobrir vulnerabilidades em seus sistemas, fechando qualquer porta que possa estar aberta para intrusos. A única semelhança entre eles é que são verdadeiros conhecedores de informática; contudo, enquanto os *hackers* usam sua inteligência para o bem, os *crackers* a

usam para o mal.

4.2. Cookies

*S*ão informações gravadas no *browser* acerca de sites visitados pelo usuário. Quando se clica o mouse, ativa-se *cookies* que vão deixando rastros e pegadas que informam hábitos de compra, hobbies, áreas de interesse, idade dos filhos, endereço, doenças e demais dados pessoais.

Os *cookies* promovem um monitoramento não autorizado, ferindo a privacidade e intimidade do usuário, na medida em que consistem em coletas de dados não autorizadas.

Estas informações podem ser usadas para:

- reconhecimento automático pela pagina na qual os dados de identificação do usuário - como login e senha - servem para acessá-la;

- armazenar informações sobre os hábitos dos usuários;

- capturar dados referentes a ideologia, religião, crença, saúde, origem racial, orientação e vida sexual do cidadão, que em mãos errados podem causar sérios prejuízos;

- conhecer as preferências das pessoas que navegam na internet.

Depois de classificas, essas informações poder ser vendidas aos comerciantes que as utilizam em mala direta ofertando produtos e serviços compatíveis com os hábitos dos usuários.

Assim, estas preferências podem ser compartilhadas

entre diversos *sites* da internet, afetando a privacidade do usuário e a sua vulnerabilidade, haja vista que os *cookies* contem diversas informações sobre o usuário que podem ser utilizados por pessoas mal intencionadas. Desta forma, é prudente que seja desabilitado no seu computador o recebimento de *cookies*, salvo para *sites* de sua confiança.

4.3. Engenharia Social

Conjunto de técnicas utilizadas por invasores para convencer os usuários a instalar programas maliciosos e divulgar informações confidenciais.

Citamos o exemplo de quando você recebe uma mensagem *e-mail,* onde o remetente é o gerente ou alguém do departamento de suporte do seu banco. Na mensagem ele diz que o serviço de *Internet Banking* esta apresentando algum problema e qual problema pode ser corrigido se você executar o aplicativo que esta anexado a mensagem. A execução deste aplicativo apresenta uma tela muito parecida aquela que você utiliza para ter acesso a conta bancária, aguardando que você digite sua a senha. Na verdade, este aplicativo esta preparado para furtar sua senha de acesso a conta bancária e envia-la para o atacante.

4.4. Phishing

Também conhecido como *phishing scam* ou *phishing/scam*, foi um termo originalmente criado para descrever o tipo de fraude que se dá através do envio de mensagem não solicitada, que se passa por comunicação de uma instituição conhecida, como um banco, empresa ou *site* popular, e que procura induzir o acesso a páginas fraudulentas (falsificadas), projetadas para furtar dados pessoais e financeiros de usuários.

A palavra *phishing* (de "*fishing*") vem de uma analogia

criada pelos fraudadores, onde "iscas" (*e-mails*) são usadas para "pescar" senhas e dados financeiros de usuários da Internet.

Atualmente, este termo vêm sendo utilizado também para se referir aos seguintes casos:

- mensagem que procura induzir o usuário à instalação de códigos maliciosos, projetados para furtar dados pessoais e financeiros;

- mensagem que, no próprio conteúdo, apresenta formulários para o preenchimento e envio de dados pessoais e financeiros de usuários.

A subseções a seguir apresentam cinco situações envolvendo *phishing*, que vêm sendo utilizadas por fraudadores na Internet. Observe que existem variantes para as situações apresentadas.

Além disso, novas formas de *phishing* podem surgir, portanto é muito importante que você se mantenha informado sobre os tipos de *phishing* que vêm sendo utilizados pelos fraudadores, através dos veículos de comunicação, como jornais, revistas e *sites* especializados.

Também é muito importante que você, ao identificar um caso de fraude via Internet, notifique a instituição envolvida, para que ela possa tomar as providências cabíveis

Como identificar

Seguem algumas dicas para identificar este tipo de mensagem fraudulenta:

- leia atentamente a mensagem. Normalmente, ela conterá diversos erros gramaticais e de ortografia;

- os fraudadores utilizam técnicas para ofuscar o real link para o arquivo malicioso, apresentando o que parece ser um link relacionado à instituição mencionada na mensagem. Ao passar o cursor do *mouse* sobre o *link*, será possível ver o real endereço do arquivo malicioso na barra de *status* do programa leitor de *e-mails*, ou *browser*, caso esteja atualizado e não possua vulnerabilidades. Normalmente, este *link* será diferente do apresentado na mensagem;

- qualquer extensão pode ser utilizada nos nomes dos arquivos maliciosos, mas fique particularmente atento aos arquivos com extensões ".exe", ".zip" e ".scr", pois estas são as mais utilizadas. Outras extensões freqüentemente utilizadas por fraudadores são ".com", ".rar" e ".dll";

- fique atento às mensagens que solicitam a instalação/execução de qualquer tipo de arquivo/programa;

- acesse a página da instituição que supostamente enviou a mensagem, seguindo os cuidados apresentados na seção 2.3, e procure por informações relacionadas com a mensagem que você recebeu. Em muitos casos, você vai observar que não é política da instituição enviar e-mails para usuários da Internet, de forma indiscriminada, principalmente contendo arquivos anexados.

Exemplo

- Páginas de comércio eletrônico ou *Internet Banking* falsificadas.

Você recebe uma mensagem por e-mail ou via serviço de troca instantânea de mensagens, em nome de um site de comércio eletrônico ou de uma instituição financeira, por

exemplo, um banco. Textos comuns neste tipo de mensagem envolvem o recadastramento ou confirmação dos dados do usuário, a participação em uma nova promoção, etc. A mensagem, então, tenta persuadí-lo a clicar em um link contido no texto, em uma imagem, ou em uma página de terceiros.

Risco

O *link* pode direcioná-lo para uma página *Web* falsificada, semelhante ao *site* que você realmente deseja acessar.

Nesta página serão solicitados dados pessoais e financeiros, como o número, data de expiração e código de segurança do seu cartão de crédito, ou os números da sua agência e conta bancária, senha do cartão do banco e senha de acesso ao *Internet Banking*.

Ao preencher os campos disponíveis na página falsificada e clicar no botão de confirmação (em muitos casos o botão apresentará o texto "Confirm", "OK", "Submit", etc), os dados serão enviados para os fraudadores.

A partir daí, os fraudadores poderão realizar diversas operações, incluindo a venda dos seus dados para terceiros, ou utilização dos seus dados financeiros para efetuar pagamentos, transferir valores para outras contas, etc.

4.5. Spywares

São instalados no computador através de um programa gratuito (freeware) ou um programa de uso limitado (shareware), o qual são oferecidos prometendo facilitar a vida dos internautas.

O resultado é o rastreamento das informações do

usuário, gerando ofertas de produtos futuras. Diferenciam dos *cookies* justamente pelo fato de serem instalados no computador através de programas.

4.6. Spam

Envio de mensagens de natureza anunciativa/propagandas de bens e serviços não solicitado.

4.7. Negação de Serviço (*Denial of Service*)

Atividade maliciosa em que o atacante utiliza um computador para tirar de operação um serviço ou computador conectado a internet para:

- Gerar uma grande sobrecarga no processamento de dados de um computador;
- Gerar um grande tráfego de dados para uma rede, ocupando toda a banda disponível;
- Tirar serviços importantes de um provedor do ar, impossibilitando o acesso dos usuários a sua caixa de correio no servidor de email ou servidor *Web.*

4.8. Código Malicioso (*Malware*)

Termo genérico que se refere a todos os tipos de programa que executam ações maliciosas em um computador.

Exemplos

- Vírus;
- Caválo de tróia ou *Trojans;*

- *Adware e Spyware;*
- *Backdoors;*
- *Keyloggers;*
- *Screenloggers;*
- *Worms;*
- *Bots;*
- *Botnets;*
- *Rootkits.*

4.8.1. Vírus

É um programa ou parte de um programa de computador, normalmente malicioso, que se propaga infectando, isto é, inserindo cópias de si mesmo e se tronando parte de outros programas e arquivos de um computador. O vírus depende da execução do programa ou arquivo hospedeiro para que possa tornar-se ativo e dar continuidade ao processo de infecção.

Modos para evitar a infecção do computador:

- Não abrir arquivos anexados aos e-mails com as seguintes extensões: ".exe", ".zip" e ".scr", pois estas são as mais utilizadas. Outras extensões freqüentemente utilizadas por fraudadores são ".com", ".rar" e ".dll";
- fique atento às mensagens que solicitam a instalação/execução de qualquer tipo de arquivo/programa;
- Se você desconhece o remetente ou se e-mail for

encaminhado por um amigo seu com cópia para várias pessoas ou não, mas que estranhamento pede para você abrir um arquivo em anexo, não abra pois poderá ser vírus;

· Não instale programas de procedência duvidosa ou desconhecida obtidas pela internet, de pen drives, CDs, DVDs, etc.

Por fim, importante destacar que o vírus também se propaga pelo celular através do *Bluetooth* ou MMS (*Multimedia Message* Service).

Todavia, o vírus de celular são diferentes dos tradicionais, pois normalmente não inserem cópias de si mesmos em outros arquivos armazenados no celular, mas podem ser projetados para sobrescrever arquivos de aplicativos ou do sistema operacional instalado no aparelho.

Assim, uma vez instalado, o vírus pode:

· destruir/sobrescrever arquivos, remover contatos da agenda, efetuar ligações telefônicas, drenar a carga da bateria, além de tentar se propagar para outros celulares.

Alguns antivírus gratuitos disponíveis na internet:

AVG Antivirus

A versão grátis do AVG vem com antivírus e antispyware em um único núcleo. Tem filtro de links de navegação, verificação de rootkit e ferramentas integradas ao sistema, como verificação de processos e conexões de rede. Roda em Windows 2000, XP e Vista.

Avira Anti Vir Personal

O antivírus alemão detecta e elimina pelo menos 50 mil vírus catalogados. Trojans, backdoors, hoaxes, worms e dialers também estão na mira do programa, que ainda é capaz de monitorar todas as ações do usuário. Roda em Windows 2000, XP e Vista.

Comodo Antivirus

Tem proteção em tempo real e atualizações diárias. Escaneia dispositivos removíveis (CDs, DVDs, drives externos, câmeras digitais e aplicativos USB) e arquivos comprimidos. Funciona em Windows 2000 e XP.

Avast Home Edition

Pacote da Avast vem com antispyware e antirrookit. Tem proteção a clientes de e-mail, detecção de invasão, proteção a programas P2P como Kazaa e BitTorrent, filtro e monitoramento de trânsito na Web, firewall embutido, filtro de grupos Usenet e boot time scanner. Para continuar funcionando depois dos 60 dias da instalação, é necessário registrar o produto. No entanto, o registro é gratuito. Possui atualização automática do banco de dados. Para Windows 95, 98, Millenium, NT, 2000, XP e Vista.

PC Tools Antivirus Free Edition

O programa traz proteção em tempo real e filtro de e-mail. Busca e elimina worms, spam e vírus difundidos pela Internet.

ThreatFire AntiVirus Free Edition

Do mesmo fabricante do PC Tools Antivirus, a ferramenta remove vírus, worms, trojans, spyware, keyloffers e erros de programação que possam prejudicar a segurança do

sistema. Segundo a PC Tools, o programa funciona por análise de comportamento, em vez de depender de um banco de dados com malwares previamente conhecidos e listados. Isso, em tese, permite ao ThreatFire identificar ameaças desconhecidas que passariam batidas por outros antivírus. Roda em Windows 2000, XP, 2003 e Vista.

BitDefender Free Edition

A versão grátis do BitDefender Antivirus Plus tem atualização automática e quarentena para arquivos suspeitos. Protege e-mails, downloads e discos de armazenamento. Compatível com Windows 98, NT, 2000, Millenium e XP.

A-Squared Free

O programa funciona como um antimalware, e não como uma suíte antivírus. Remove trojans, backdoors, keyloggers, rootkits, spywares, adwares, tracking cookies, worms, bots e dialers. O software grátis não tem detecção em tempo real, filtro Web nem atualização automática, ao contrário da versão paga.

Multi Virus Cleaner 2008

Traz uma lista de 6.000 vírus, worms, trojans e dialers conhecidos. Não dispensa a instalação de um antivírus completo no computador, pois não funciona em tempo real nem cria barreiras contra malwares; só realiza "caças" a softwares maliciosos quando o usuário faz o scan manual. Assim, ele funciona como uma ferramenta extra de detecção e limpeza.

ClamWin Portable

O antivírus opensource é portátil, ou seja, pode ser carregado em um pendrive. Agenda escaneamentos e

tem atualização automática do banco de dados, mas não oferece proteção em tempo real. Não são raras reclamações sobre a lentidão dos scans.

4.8.2. ***Trojans*** (cavalos-de-troia)

São programas executáveis, normalmente recebidos como cartão virtual, álbum de fotos, protetor de tela, jogo, etc, que transformam seu micro em um terminal de internet "aberto".

Estes programas eliminam as proteções que impedem a transferência de informações.

O cavalo de tróia ou *trojan* pode:

- Instalar keyloggers ou screenloggers;
- Furtar senhas e outras informações, como número do cartão de crédito;
- Inclusão de backdoors, para permitir que um atacante tenha total controle sobre o computador;
- Alteração ou destruição de arquivos;
- Formatar o disco rígido do computador;
- Permitir que o invasor acesse e copie todos os arquivos armazenados no computador, etc.

4.8.3. Adware e *Spyware*

Adware (*Advertising software*) é um tipo de software especificamente projetado para apresentar propagandas através do *browser* ou de algum outro programa instalado em um computador.

Spyware software que tem o objetivo de monitorar

atividades de um sistema e enviar as informações coletadas a terceiros. Alguns *Adwares* podem ser programados para assumir as características de *Spyware.*

Apesar de poderem ser utilizados de forma legítima, na grande maioria dos casos são usados de forma ilícita, pois são projetados para monitorar os hábitos dos usuários durante a navegação na internet, direcionando as propagandas que serão apresentadas, de forma dissimulada, não autorizada e maliciosa.

4.8.4. Backdoors

Programa que permite a um invasor retornar a um computador comprometido sem precisar recorrer aos métodos utilizados na realização da invasão e sem ser notado.

4.8.5. Keyloggers

Programa capaz de capturar e armazenar as teclas digitadas pelo usuário no teclado do computador. Normalmente, o *keyloggers* vem como parte de um programa *spyware* ou cavalo de tróia.

4.8.6. Screenloggers

Forma avançada de *keylogger*, capaz de armazenar a posição do cursor e a tela apresentada no monitor, nos momentos em que o *mouse* é clicado, ou armazenar a região que circunda a posição onde o *mouse* é clicado.

4.8.7. Worms

Programa capaz de se propagar automaticamente através da rede, enviando cópias de si mesmo de computador para computador.

Diferente do vírus, o *worm* não embute cópias de si mesmo em outros programas ou arquivos e não necessita ser explicitamente executado para se propagar. Sua propagação se dá através da exploração de vulnerabilidades existentes ou falhas na configuração dos softwares instalados em computadores.

A sua detecção é difícil. Embora existam antivírus que permitam detecta-los e até mesmo evitar que se propaguem, isto ás vezes nem sempre é possível.

4.8.8. Bots

De modo similar ao *worm*, o *bot* é um programa capaz de se propagar automaticamente, explorando vulnerabilidades existentes ou falhas na configuração de software instalados em um computador. Adicionalmente ao *worm*, dispõe de mecanismos de comunicação com o invasor, permitindo que o *bot* seja controlado remotamente.

Através do *bot*, o invasor pode:

- Desferir ataques na internet;
- Executar um ataque de negação de serviço;
- Furtar dados do computador;
- Enviar e-mail de phishing;
- Enviar spam.

4.8.9. Botnets

São redes formadas por computadores infectados com *bots.*

Um invasor que tenha o controle sobre uma *botnet* pode

utilizá-la para aumentar a potência de seus ataques, por exemplo, para enviar centenas de milhares de e-mail de *phishing* ou *spam*, desferir ataques de negação de serviço, etc.

4.8.10. Rootkits

Mecanismo utilizado para esconder e assegurar a presença do invasor do computador comprometido; assim ele terá acesso privilegiado ao computador previamente comprometido.

Um *rootkits* pode fornecer programas com as mais diversas funcionalidades. Dentre eles, podemos citar os seguintes softwares:

- Para ocultar atividades e informações deixadas pelo invasor;
- *Backdoors* para assegurar acesso futuro do invasor ao computador comprometido;
- Para remoção de evidencias em arquivos *logs*;
- *Sniffers* (dispositivo ou programa de computador utilizado para capturar e armazenar dados trafegando na internet, como senhas de usuários);
- *Scanners* (programa utilizado por invasores para mapear potenciais vulnerabilidades em outros computadores);
- Outros tipos de *malware*, com cavalos de tróia, *keyloggers*, ferramentas de ataque de negação de serviço, etc.

5. Da responsabilidade civil e criminal

Os pais são civilmente responsáveis pela reparação dos danos causados pelos filhos menores sob sua GUARDA, por lhes caber precipuamente os deveres de disciplina e vigilância, conforme dispõe o art. 932 do Código Civil:

"Art. 932 – São também responsáveis pela reparação civil:

I – os pais, pelos filhos menores que estiverem sob sua autoridade e em sua companhia;"

Desta forma, mais do que nunca os pais devem esta atentos aos seus filhos quando estiverem navegando na internet.

A internet não é um "território sem lei", pois quem se relaciona virtualmente responde por seus atos com base na Constituição Federal e nos Códigos Civil e Penal. Além disso, é equivocado pensar que é possível agir anonimamente, valendo-se de nomes falsos ou nicknames, acreditando estar acobertado pelo manto da impunidade, e praticar qualquer ato ilícito que jamais será descoberto. Através do endereço de IP - que é um número único que identifica um computador ou dispositivo ligado a uma rede que se comunica através do protocolo de redes TCP (Transmission Control Protocol) - é possível chegar até o computador que gerou determinado conteúdo e, por meio desse computador, descobrir a identidade do proprietário.

Vários são os crimes que já estão previstos nos dispositivos do atual Código Penal, que são aplicáveis no combate ao crime digital:

ATO	INFRAÇÃO	ARTIGO CP
Falar através dos recursos da internet disponíveis, que alguém deve se matar ou sugerir a forma de fazê-lo	Instigação ao suicídio	122
Falar através dos recursos da internet que alguém cometeu um crime que não aconteceu	Calúnia	138
Repassar para várias pessoas e-mail denegrindo a reputação de alguém	Difamação	139
Enviar e-mail falando mal das características físicas e/ou morais de alguém	Injúria	140
Enviar e-mail para alguém dizendo que vai pega-la	Ameaça	147
Enviar e-mail divulgando dados confidenciais para terceiros, fotos de momentos íntimos	Divulgação de segredo	153
Invadir computadores pessoais e se apropriar de dados e senhas bancárias para se apossar de valores	Furto	155
Enviar vírus que destrua dados ou aparelhos	Dano	163
Copiar um conteúdo e não mencionar a fonte	Violação de direito autoral	184
Criar comunidade on-line que fale mal das religiões	Escárnio por motivo de religião	208
Divulgar fotos em comunidade on-line com gestos obscenos	Ato obsceno	233
Criar comunidade on-line incentivando o roubo de determinado comércio	Incitação ao crime	286
Criar comunidade on-line para ensinar a realizar atos ilícitos	Apologia de crime	287
Criar comunidade on-line para enaltecer criminoso	Apologia a criminoso	287
Enviar e-mail com remetente falso ou mesmo criar cadastro com dados falsos em loja virtual	Falsa identidade	304
Ao receber um Spam, devolve-lo com vírus ou com mais Spam	Exercício arbitrário das próprias razões	345
Estabelecer ou explorar jogos de azar	Jogo de azar	Art. 50 LCP

OUTRAS LEIS		
Usar cópia de software sem a devida autorização ou licença.	Crimes contra os direitos autorais	Art. 12 da lei 9.609/98
Utilizar on-line logomarca de empresa, no todo ou em parte ou mesmo imitá-la de forma a induzir confusão.	Crime contra a propriedade industrial	Art. 189 da lei 9.279/96
Veicular imagens e ilustrações com cenas de sexo explícito ou erótica.	Crime de pedofilia	Art. 241 e seguintes da lei 8069/90 ECA
Incitar em um *chat* a discriminação de alguém em virtude da raça.	Crimes de discriminação ou preconceito de raça, cor, etnia, religião ou procedência nacional	Art. 20 da lei 7.716/89

6. Do anonimato

A Constituição da Republica Federativa do Brasil, promulgada no ano de 1988, veda em seu art. 5, inc IV o anonimato, *in verbis*:

"É livre a manifestação do pensamento, sendo vedado o anonimato."

O anonimato é uma das maiores entraves na internet, pois favorece a prática de ilícitos, de atividades antiéticas e até crimes. Por tais motivos, é imprescindível que a instituição de ensino promova a identificação individual e única de cada aluno quando o mesmo estiver fazendo uso de seus computadores para navegar nos ambientes virtuais.

Cabe a escola conferir uma Identidade Digital para o Aluno, pois na ocorrência de algum incidente, será possível verificar quem o praticou. Desse modo, a escola poderá aplicar medidas educativas visando a orientação do aluno, bem como para adverti-lo e, sendo o caso, praticar algum tipo de penalidade, como suspensão do uso do ambiente eletrônico por um período, ou em casos mais graves, até a expulsão.

Agindo desta forma, a instituição de ensino irá diminuir os riscos de uma possível demanda judicial em que se pede a responsabilidade civil por danos causados a terceiros, uma vez que tudo vai ficar registrado como tendo sido feito em seus computadores.

7. Dicas para proteger seu computador

7.1. No Windows

Você pode começar a proteger seu computador simplesmente configurando seu Windows, seguindo estes passos:

Menu Iniciar → Configurações → Painel de Controle → Central de Segurança

Assim, você poderá configurar o que segue:

7.1.1. Firewall

Um *firewall* é um software ou hardware que verifica informações oriundas da Internet ou de uma rede e bloqueia-as ou permite que elas passem pelo seu computador, dependendo das configurações do firewall.

Um *firewall* pode ajudar a impedir que *hackers* ou softwares mal-intencionados (como *worms*) obtenham acesso ao seu computador através de uma rede ou da Internet.

Um *firewall* também pode ajudar a impedir o computador de enviar software mal-intencionado para outros computadores.
O *Firewall* do Windows pode ajudar a proteger o computador. Por isso, mantenha sempre o *Firewall* do Windows ou outro em execução no computador.

7.1.2. Windows Defender

É importante executar software anti-*spyware* sempre que você estiver usando o computador. *Spyware* e outros softwares potencialmente indesejados podem tentar se instalar no seu computador toda vez que você se

conectar à Internet.

Eles também podem infectar o computador quando você instalar alguns programas usando CD, DVD ou outra mídia removível. Software mal-intencionado ou potencialmente indesejado também pode ser programado para ser executado em horários inesperados, e não apenas quando é instalado.

O *Windows Defender* oferece três formas de ajudar a impedir que spyware e outros softwares potencialmente indesejados infectem o computador:

Proteção em tempo real. O *Windows Defender* alerta quando *spyware* ou software potencialmente indesejado tenta se instalar ou ser executado no seu computador.

Ele também alerta caso os programas tentem alterar configurações importantes do Windows.

Comunidade *SpyNet*. A comunidade online do Microsoft *SpyNet* ajuda você a ver como outras pessoas respondem a software que ainda não tenha sido classificado com relação aos riscos.

Ver se outros membros da comunidade permitem a execução do software poderá ajudá-lo a decidir se deve ou não permitir no seu computador.

Por sua vez, se você participar, suas opções serão adicionadas às classificações da comunidade para ajudar outras pessoas a escolherem o que devem fazer.

Opções de verificação. Você pode usar o *Windows Defender* para verificar se há *spyware* e outros softwares potencialmente indesejados instalados em seu computador, agendar verificações regularmente e remover automaticamente qualquer software mal-intencionado que seja detectado durante a verificação.

Ao usar o *Windows Defender*, é importante manter as definições atualizadas. As definições são arquivos que atuam como uma enciclopédia de possíveis ameaças de software em constante crescimento.

O *Windows Defender* usa as definições para determinar se o que ele detectou é spyware ou software potencialmente indesejado e alertá-lo sobre possíveis riscos.

Para ajudar a manter as definições atualizadas, o *Windows Defender* trabalha com o Windows Update para instalar automaticamente novas definições à medida que elas são lançadas.

Também é possível definir o *Windows Defender* para conferir se há definições atualizadas antes da verificação.

7.1.3. Windows Update

Mantenha o *Windows Update* ativo em seu computador, pois através das atualizações pode-se evitar ou corrigir problemas, aumentar a segurança do computador ou melhorar seu desempenho.

7.2. Antivírus

Tenha instalado um antivírus (verificar item 4.8.1 antivírus gratuitos disponíveis na internet) em seu computador e mantenha-o sempre atualizado.

O Escritório

MARIANI, SANTOS & advogados associados

O escritório MARIANI, SANTOS & Advogados Associados, altamente especializado em Direito Digital e Informática, conta com profissionais com mais de 20 anos de experiência neste segmento do direito.

Oportuno destacar que o escritório nasceu da comunhão de ideais visando à prestação de serviços jurídicos de excelência, que ofereçam continuamente confiança, presteza e eficiência para satisfazer e atender aos anseios de nossos clientes.

Como diferenciais podemos citar a busca incessante de soluções jurídicas para atender as necessidades, desejos, expectativas e conveniências dos nossos clientes e a rápida e profunda imersão no estudo dos novos ramos do direito, com vistas a disponibilizar novas ferramentas em seu benefício.

O escritório MARIANI, SANTOS & Advogados Associados é um escritório inovador, altamente qualificado, que constrói sua política interna e planejamento estratégico tendo sempre em foco nosso bem maior: o cliente.

Para conhecer todas as nossas especialidades, acesse nossa página na internet: www.marianiesantos.com.br.

Por fim, colocamos-nos a inteira disposição para maiores esclarecimentos e dirimir eventuais dúvidas.

Fontes

PAESANI, Liliana Minardi, Direito da Informática – Comercialização e desenvolvimento internacional de software – 6. Ed. – São Paulo : Atlas, 2007

PINHEIRO, Patrícia Peck, Direito Digital – 2. Ed. – São Paulo: Saraiva, 2008

http://www.safernet.org.br/site/prevencao/

http://www.microsoft.com/brasil/athome/security/children/default.mspx

http://www.cartilha.cert.br/

APOIO

ASSESPRO
PARANÁ

design graffo solution
www.graffodesign.com

MARIANI, SANTOS & advogados associados

Rua Desembargador Motta, 3588 | Mercês | Curitiba | Paraná
Fone: (41) 3335-5577 | Fax: (41) 3335-2665 | CEP 80430-200

www.marianiesantos.com.br