

REDES SOCIAIS E SEGURANÇA DA INFORMAÇÃO

Em um mundo no qual a informação é um bem extremamente valioso, ganha pontos neste universo aquele que “tuíta”¹ mais rápido, compartilha o quanto antes as fotos no Facebook², dissemina conteúdo de maior relevância nos blogs, divulga primeiro as melhores informações tidas como “furo de reportagem” e avisa instantaneamente os amigos onde está e o que está fazendo.

Esta convergência das mídias faz com que permaneçamos cada vez mais tempo conectados, interagindo com nossos amigos e contatos profissionais em tempo real através da Internet.

Como toda tecnologia, também há os prós e contras dessa “socialização digital”. Dentre as vantagens, podemos citar: amigos a um clique de distância; migração dos meios analógicos para os digitais; interação do mundo “real” com o mundo “virtual”; maior compartilhamento de conhecimento; usuário passa a ser emissor de conteúdo, e não somente receptor; grande volume de informações divulgadas em maior velocidade; uso da rede como ferramenta para mobilização social; e rastreabilidade da informação (é possível conferirmos o autor de determinado conteúdo, em determinado dia e horário, e quais reflexos da publicação desse material).

Porém, há também os aspectos negativos desse comportamento: excesso de exposição no mundo virtual; *cyberbullying*³; limites entre privado e público passam a ser cada vez mais difusos; confusão entre vida pessoal e profissional; reputação negativa na Internet; reflexos negativos no âmbito profissional; entre outros.

¹ Neologismo de “tuitar”, relacionado ao microblog Twitter: publicar um comentário através do serviço de microblog.

² Rede social utilizada mundialmente – www.facebook.com.

³ O termo *cyberbullying* originou-se da expressão *bullying*, que é considerado “*todo ato de violência física ou psicológica, intencional e repetitivo, que ocorre sem motivação evidente, praticado por indivíduo ou grupo, contra uma ou mais pessoas, com o objetivo de intimidá-la ou agredi-la, causando dor e angústia à vítima, em uma relação de desequilíbrio entre as partes envolvidas.*” (Projeto de Lei nº 5369/09, de autoria do Deputado Vieira da Cunha. Conforme art. 1º deste projeto de lei, seu objetivo é instituir o Programa de Combate ao Bullying em todo o território nacional, vinculado ao Ministério da Educação). O *cyberbullying* é, portanto, o *bullying* praticado através dos meios eletrônicos: trata-se do uso da tecnologia da informação e comunicação (emails, celulares, SMS, fotos publicadas na Internet, sites difamatórios, publicação de mensagens ofensivas ou difamatórias em ambientes online, etc) como recurso para a prática de comportamentos hostis e reiterados contra um grupo ou um indivíduo.

Devido à alta interatividade e conectividade de seus usuários, as redes sociais vêm ganhando novos usuários a cada dia, e conseqüentemente, os problemas citados acima passam a ser cada vez mais comuns. Porém, o que nos chama a atenção é o fato destes reflexos negativos do mau uso dessas tecnologias originarem-se do comportamento de muitos profissionais que atuam justamente na área de Segurança da Informação.

Diariamente, deparamos com publicações no Twitter⁴ de usuários que ao informarem o que estão fazendo naquele momento, também dizem o local exato em que se encontram, com direito a mapa e outros detalhes. Isto pode ser interessante se você quiser ser encontrado mais rapidamente pelos amigos com quem combinou um passeio, porém, lembre-se de que aqueles rotulados como “*persona non grata*” também irão localizá-lo com a mesma facilidade. E se você diz que está em uma agência bancária, por exemplo, passa a aumentar consideravelmente o contingente de ameaças a sua integridade física.

O uso desmesurado de aplicativos que inserem a sua localização geográfica no momento da postagem de seus “tweets”⁵ é uma brecha de segurança, e mostra que você não se importa muito em ser localizado. O problema é ainda maior se você de fato é encontrado por quem não gostaria de ver, e também, se tais localizações contradizem com as informações que você forneceu anteriormente (exemplo: o funcionário que vai para um congresso pago pelo empregador, e “tuíta” a localização do bar em que se encontra, no mesmo horário do evento corporativo).

Sobre encontros desagradáveis motivados pelas redes sociais, recordo-me de um episódio ocorrido com um parente, que divulgou no Twitter, em um sábado à noite, que iria sair com os amigos. Uma de suas amigas publicou no microblog o nome do local onde se encontrariam. Resultado: minha parente acabou tendo a desagradável surpresa de encontrar com o ex-namorado, que acompanhava o perfil de sua amiga, e, portanto, sabia de seus passos. Uma discussão entre o ex e o atual namorado foi evitada pelos colegas que conseguiram conter os ânimos do rapaz, que agora, deixado no passado, tinha fortes características de um “*stalker*”⁶.

⁴ Serviço de microblogs, que permite publicação de mensagens rápidas, contendo até 140 caracteres – www.twitter.com.

⁵ Mensagens publicadas no serviço de microblogs Twitter.

⁶ Indivíduo que “persegue” constantemente sua vítima (atualmente pela Internet), mostrando-se onipresente em sua vida, dando demonstrações de que exerce certo controle sobre esta.

Vemos que há perigos bem reais do uso inconsciente deste tipo de aplicativo das redes sociais: riscos de ser furtado, excesso de exposição, reflexos negativos na vida corporativa e complicações na vida pessoal.

Uma pesquisa reproduzida pelo jornal “O Estado de São Paulo”, realizada pela empresa internacional TNS, relata que os internautas já estão passando mais tempo online nas redes sociais do que lendo e respondendo e-mails (gastam em média 3,1 horas semanais em redes sociais, contra 2,2 horas semanais com e-mails)⁷.

O fato de passarem muito tempo online, e sendo a maior parte deste em redes sociais, leva os usuários a serem muito comunicativos na Internet. E o hábito de falar demais no meio virtual pode gerar alguns incidentes bem reais, com publicação de comentários e conteúdos indevidos, publicação de fotos e vídeos constrangedores, etc.

Como exemplos dessa conduta, podemos citar alguns episódios: 1) ex-diretor de renomada empresa na área de hospedagem de sites, durante um jogo de futebol publicou mensagens de baixo calão, contra o time patrocinado pela própria instituição. Tal fato gerou graves problemas com a imagem da empresa, causando um incidente institucional. A empresa tentou minimizar os danos, publicando nota à imprensa, porém, acabou afastando o funcionário. 2) uma jornalista brasileira, ao escrever artigo em jornal de grande circulação, emitindo sua opinião sobre questões de tema eleitoral, acabou gerando tanta repercussão nas redes sociais, que foi demitida pelo próprio jornal. 3) jogadores brasileiros, que após uma partida, transmitiram vídeo através do Twitter, em que tratavam os torcedores do próprio time de modo ofensivo. A conduta imatura gerou problemas com a diretoria do clube, que teve de se posicionar diante da crise instalada.

Tais atitudes são vistas diariamente, praticadas não somente por jovens e adolescentes, mas também por profissionais adultos, que não imaginam a repercussão que podem causar, e os problemas que poderão gerar, abalando sua vida pessoal e profissional.

Nessa questão, chamamos a atenção dos profissionais da área de Segurança da Informação (SI) e executivos do segmento de Tecnologia da Informação (TI), que por estarem muito familiarizados à esse tipo de tecnologia, encaram tais ferramentas de modo natural e acabam publicando conteúdo que não condiz com suas posições profissionais.

⁷ <http://blogs.estadao.com.br/link/brasileiros-tem-2ª-media-de-amigos-online/>. Acesso em 12/10/2010, 20h55min.

Talvez, alguns imaginem que por dominarem as questões de segurança, nunca serão vítimas desses incidentes. A mídia mostra que a maioria destes profissionais de liderança tende a se mostrar desatenta para questões de segurança e convictos de estarem protegidos⁸.

Nós, que lidamos com SI, precisamos ser ainda mais alertas. Se somos responsáveis por mantermos a confidencialidade das informações de uma empresa, também devemos ter esse comportamento em nossa vida pessoal.

É importante sempre lembrarmos que:

- ✓ As ameaças não escolhem lado;
- ✓ Os golpes virtuais não conferem os crachás antes de se configurarem;
- ✓ Os criminosos virtuais também são reais, e estão de olho em pessoas com posições de liderança nas empresas, e também naquelas que demonstram maior *status* social e financeiro;
- ✓ A sua lista de amigos nas redes sociais pode incluir também seus colegas de trabalho, seu chefe e seus clientes. Portanto, cautela com o que diz por aí.

Somos responsáveis por mantermos a confidencialidade, integridade e disponibilidade das informações em nossas empresas.

Em nossa vida particular, também devemos ter o mesmo cuidado, porém, as informações não devem estar totalmente disponíveis.

(Abaixo, segue tabela contendo as principais dicas de Segurança da Informação nas redes sociais).



Gisele Truzzi

Advogada especialista em Direito Digital e Direito Criminal.

www.truzzi.com.br

gisele@truzzi.com.br

⁸ *Quatro motivos que tornam os executivos alvos de golpes online*, publicado no portal IDGNow! em 12/10/2010. http://idgnow.uol.com.br/computacao_corporativa/2010/10/12/quatro-motivos-que-tornam-os-executivos-alvos-de-golpes-online/. Acesso em 12/10/2010, às 21h25min.

PRATIQUE A SEGURANÇA DA INFORMAÇÃO NAS REDES SOCIAIS

1	<p>Se você possui perfis em redes sociais, separe seus contatos em listas diversas, diferenciando os contatos pessoais dos contatos profissionais. Assim, você poderá criar álbuns de fotos acessíveis para um único grupo, evitando “queimar o filme” com seu chefe ou colegas de trabalho, ao publicar abertamente fotos do churrasco com os amigos no último final de semana, em que você exagerou na dosagem ética.</p>
2	<p>Mantenha seu perfil “clean” e organizado. A maioria das empresas, antes de efetuar uma contratação, pesquisa na Internet e em redes sociais, informações sobre os candidatos à vaga. Uma foto mais formal, poucos aplicativos adicionados, o mínimo de informações pessoais e dados curriculares verídicos em seu perfil transparecem maior seriedade e profissionalismo, ao contrário daquela antiga foto tirada na “balada” com o pessoal dos tempos da faculdade. Seu chefe ou futuro empregador também não precisa saber qual é seu apelido de infância, ou que você é viciado em jogar “Farmville”.</p>
3	<p>Uma imagem vale mais do que mil palavras. Cautela com o tipo de foto que publica e a quem liberará o acesso. Seus amigos podem estar interessados nos passeios e viagens que você faz, mas seus colegas de trabalho, nem tanto. Estes irão achar que você terá, eventualmente, um salário maior do que merece.</p>
4	<p>Tudo o que você publica poderá ser visto pelos seus colegas de trabalho, clientes, parceiros e chefe. Altere as configurações padrões de privacidade, para que sejam acessíveis as informações somente aos interessados. Assim, evitará que o vizinho do seu amigo fique sabendo de suas andanças, e aperfeiçoará a separação das suas listas de contatos pessoais e networking. Mesmo assim, tenha em mente que nada é 100% seguro. Portanto, não publique nada do qual poderá se arrepender futuramente.</p>
5	<p>Se beber, não tweet. Todos sabemos que o estado alterado de consciência produzido pelo álcool poderá gerar comportamentos fora de padrão à maioria das pessoas. Alguns se tornam depressivos, outros falam demais, etc. Portanto, ao exagerar na dose, não tweet. Na 2a. feira você poderá arrepender-se do que publicou nas redes sociais após a bebedeira de sábado.</p>
6	<p>Menos é mais. A maioria das pessoas não está interessada em saber se você está com dor de cabeça ou se vai dormir. Logo, publicações contínuas podem gerar uma espécie de spam irrelevante, irritando seus contatos. O mesmo vale para publicações sem conteúdo. Um dos grandes benefícios das redes sociais é o compartilhamento, portanto, se for publicar algo, procure disseminar conteúdo relevante, divulgar conhecimento. Você também pode utilizar essas ferramentas para divulgar seu trabalho, fazendo seu marketing pessoal. Mas não se torne um spammer de newsletter, não há amizade virtual que resista.</p>
7	<p>Mantenha a coerência das informações. Seu chefe não gostará de saber que no dia em que você faltou porque não estava bem de saúde, na realidade estava degustando uma porção generosa de camarões à beira-mar.</p>
8	<p>Seus amigos virtuais nem sempre são seus amigos reais. Certamente, nem a metade de seus amigos virtuais são seus amigos reais. Se já é difícil ter uma amizade verdadeira (real), o que dirá de uma amizade virtual... Logo, seu melhor amigo online não precisa (e não deve) ficar sabendo de todos os detalhes de sua vida pessoal. Evite publicar informações de sua rotina ou de sua família, dessa forma você se tornará um alvo facilmente identificável e rastreável para alguém com intenções criminosas.</p>
9	<p>Seus colegas de trabalho nem sempre estão na sua lista porque gostam de você. Tudo o que você publica nas redes sociais poderá ser utilizado contra você. E no seu trabalho também. Principalmente se você possuir algum colega que está de olho no que você diz na Web, somente para ter algo a entregar ao seu chefe e então, “puxar seu tapete”.</p>
10	<p>Lembre-se: você poderá estar a um tweet da demissão por justa causa. Ou do fim de um relacionamento, ou do término de uma reputação positiva, construída por anos.</p>

Autora: Dra. Gisele Truzzi. (Direitos autorais reservados).