Universidade Federal de Minas Gerais

UNI003 - Oficina Online de Leitura e Produção de Textos
A Metodologia do Risco: Texto Livre

Artigo – Segurança da Informação

Helio Bertolini Junior

Patricia Almerinda de Moraes Xavier

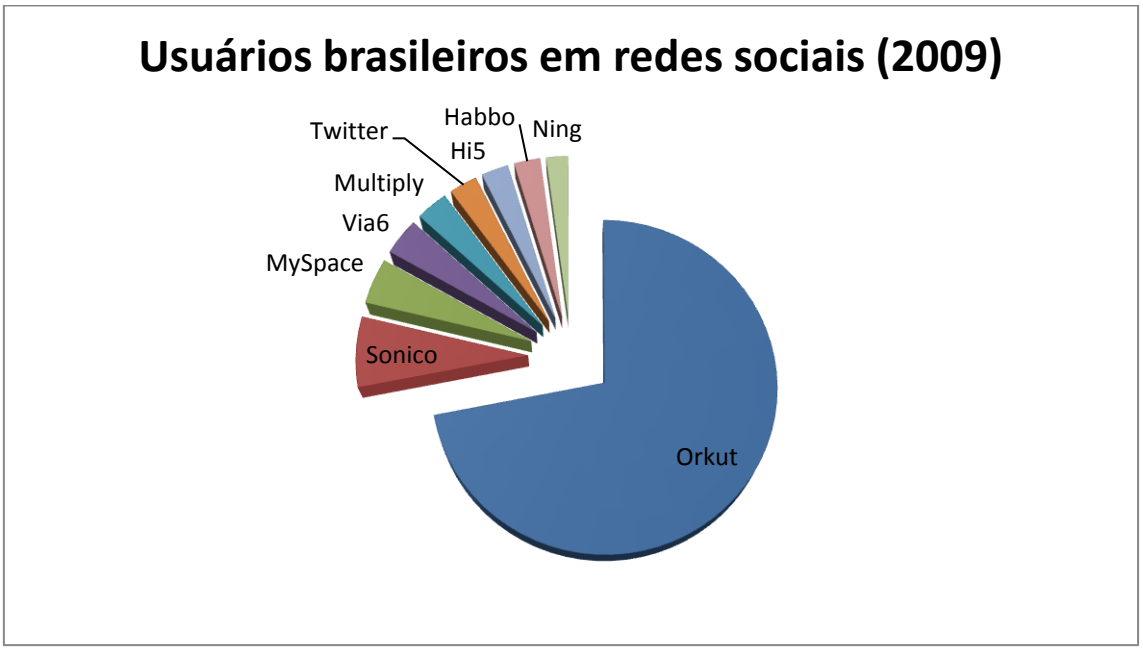
Carolina dos Santos Arantes Alves

Isaias Jose Ramos de Oliveira

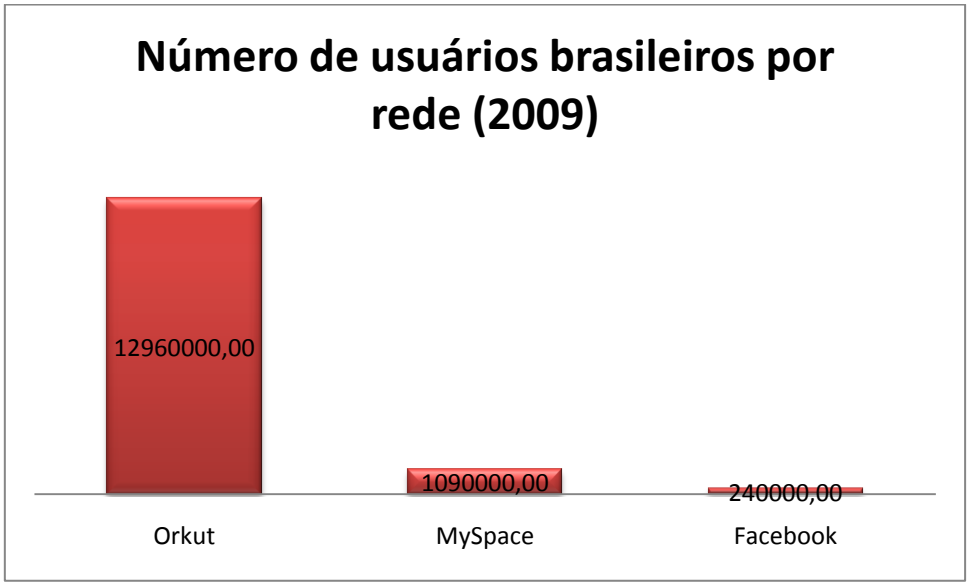
Marcela Castro Cardoso de Carvalho

Isa Paula Barbosa da Penha

As redes sociais não param de crescer no mundo inteiro e já são responsáveis por 62% do tráfego na web. Esse número é realmente grande e mostra que estamos gastando nosso tempo praticamente todo nos relacionando. Todas as grandes redes sociais estão em mais de um tipo de dispositivo físico ou móvel.



Para nos comunicar estamos conectados ou procurando conexão o tempo todo. Isso se tornou muito claro com a explosão do celular, recorde de vendas no Brasil, mas não é o único caso. São smartphones, netbooks, notebooks e agora os Ipads. Para nosso e-mail, uma página na internet, um vídeo no YouTube, estamos cada vez mais tempo on-line. Todas as operadoras oferecem planos e aparelhos para você usar para acessar suas redes sociais.



Uma pergunta, infelizmente pouco comum, mas muito importante acaba surgindo: com tantos dados pessoais trafegando, quem cuida da segurança da minha informação?

As maiores redes sociais sofrem diariamente com problemas de segurança. O mais recente foi o Facebook que encontrou uma falha em seus aplicativos que passavam informações pessoais para empresas. Já o Orkut foi invadido e contaminou 189 mil. As pessoas infectadas enviaram recados automaticamente para seus amigos e acabaram encadeando uma contaminação. Ainda recentemente o Facebook foi invadido e circula pela internet uma lista com todos os usuários, fotos, informações pessoais, URL e amigos. Já o Twitter não ficou de fora e também foi invadido, proliferando links maliciosos. A rede social integrada ao Gmail, o Buzz, já nasceu com uma incrível falha de segurança, que tornava sua lista de contatos pública.

Mas o maior problema de segurança das redes sociais está na verdade lendo esse texto. O maior foco de invasão de privacidade é o usuário. Seja por senha mal formulada (fraca) ou por informar coisas demais ao traçar o perfil ou até mesmo por adicionar ou aceitar qualquer "amizade" nessas redes, o usuário final, o mais prejudicado, é na verdade o grande difusor de práticas que o expõe mais diretamente aos riscos.

Tentando alertar o usuário existem várias iniciativas. Uma delas foi feita pela RNP (Rede Nacional de Ensino e Pesquisa), a primeira rede de acesso à internet no Brasil, disponibilizando uma cartilha de Recomendações Gerais aos usuários (disponível em http://www.rnp.br/_arquivo/disi2009/rnp-disi-2009-cartilha.pdf) que trata desde a forma correta de criar sua senha até o que se deve ponderar ao criar um perfil no Orkut, Twitter e Facebook, com imagens e dicas. Já a Google anunciou nessa semana que disponibilizará $8,5 milhões em atitudes que visem educar as pessoas na criação e manutenção de seus perfis Buzz.

É realmente preocupante a quantidades de dados pessoais que trafegam hoje na internet. No Twitter, por exemplo, você pode postar onde está nesse momento. Já pensou a gama de possibilidades (positivas e negativas) para uma informação dessas? Você sabe quem lê seus "twitts"? Protegeu seu perfil do Orkut? Tem senha forte? Preparamos então uma série de dicas para quem se alarmou:

- Ao entrar em uma nova rede social, informe o mínimo possível
- Use pelo menos 8 caracteres em suas senhas, incluindo caracteres especiais (%*&$#@^~]}_-)
- Não utilize a mesma senha em mais de um serviço! "Mas como vou lembrar as senhas?" Utilize um gerenciador de senhas (como o KeePass - http://keepass.info/).
- Troque suas senhas se utilizar as redes sociais em redes abertas como aeroportos, lan houses ou mesmo no computador de outra pessoa
- Utilize a saída segura "logout" dos serviços, assim você não deixa brecha para próximo "espertinho".

- Serviços como o TinyUrl e o Migre.me devem ser evitados.

Então fique atento!