80 – Outubro 2006

Perigos do Orkut que você pode evitar.

As redes eletrônicas de relacionamento, a exemplo do Orkut da Google, vêm crescendo em escala geométrica. Muitos acreditam que o motivo de tanto sucesso esteja ligado à necessidade do ser humano de estar em contato com seus semelhantes, mesmo que ainda ligados por uma interface virtual. Outros apostam no simples interesse pela vida alheia, no voyeurismo ou ainda na sensação de estar mais acessível e visível em um mundo onde é cada vez mais escasso o tempo para os amigos e a família. Existem ainda aqueles que usam o ambiente para reencontrar velhos amigos e estabelecer grupos de interesse que facilitem a troca de dicas e experiências.

Qualquer que seja a razão para fazer parte desta comunidade, é preciso conhecer também os perigos associados ao novo ambiente e conhecendo-os, definir seu perfil de risco e adotar tática e mecanismos de defesa para evitar armadilhas.

Premissas de análise

- Em geral essas redes de relacionamento são serviços eletrônicos hospedados em local comumente desconhecido, acessível em qualquer parte do mundo através da Internet e com permissão para livre consulta ao perfil dos usuários.
- Não existe qualquer processo de identificação do usuário a partir de documentos legalmente reconhecidos no momento da criação de um novo perfil ou uma nova comunidade de interesse.
- Não existe qualquer mecanismo eletrônico de proteção de propriedade das fotografias que são compartilhadas no ambiente.
- O único meio usado pelas redes para proteger a identidade do usuário é através da autenticação por senha simples e não há qualquer política de formação e renovação de senha por tempo de uso.

Perigos de primeiro nível

- O perigo mais óbvio é ter sua senha descoberta, seja por tentativa ou por grampo de teclado e trojan, permitindo o acesso irrestrito aos ambientes de edição de perfil, comunidades e mensagens.

- O perigo mais imperceptível é o fato de estar reduzindo sua própria privacidade e criando trilhas de auditoria em sua própria vida, onde fatos e fotos contam sua história na linha do tempo a qualquer um que se interesse por ela.

- O perigo mais destrutivo está no fato de disponibilizar indiscriminadamente detalhes demais sobre sua vida e a de sua família, potencializando todo tipo de golpe,

que pode começar por uma simples ameaça, passando por chantagem, o roubo de identidade, a fraude financeira, calúnia e até mesmo maximizar a tentativa de seqüestro.

Com os perigos de primeiro nível, só a criatividade, coragem e a motivação inerente ditarão os limites dos perigos de segundo nível. Desta forma, o usuário estará sujeito a inúmeras armadinhas e riscos que até então desconhecia:

- **Responsabilidade Legal:** se um desconhecido obtiver acesso à sua senha e seu perfil, poderá agir em seu nome, enviando mensagens, criando comunidades e assim, podendo cometer crimes de apologia às drogas, à pedofilia ou ainda crime de racismo e muitos outros.
- **Roubo de Identidade:** sem a existência de processos fortes de identificação e autenticação de novos usuários quando da criação de novos perfis e comunidades, nada impede que alguém crie um novo perfil copiando e utilizando suas fotos, seu nome, seus dados pessoais e detalhes de sua vida acessíveis através do perfil verdadeiro.
- **Crime Contra a Honra:** ainda de posse de acesso à edição de seu perfil, o fraudador pode se inserir em comunidades que indiquem distúrbios de comportamento, opções sexuais, gostos duvidosos e assim, associar você a interesses que influenciem no julgamento que seus amigos fazem de você e de sua honra.
- **Chantagem:** expondo detalhes demais de sua vida e de sua família, você pode estar potencializando os goles de chantagem, seqüestro falso ou qualquer outro em que conhecer o nome de seus familiares ou simplesmente onde passou suas últimas férias, poderá fazê-lo acreditar na veracidade do golpe e assim, ser alvo fácil.
- **Fraude Financeira:** em função do conceito primário da rede de herança de confiança entre amigos, onde o amigo de um grande amigo seu passa a ter, supostamente, a sua confiança, você poderá ser levado a acreditar cegamente nele, sem, no entanto se lembrar de que não existe nenhum critério sério de avaliação e aceitação de amigos na rede. Desta forma, pedidos falsos de ajuda financeira, caridade ou qualquer outro passam a ter grandes índices de aceitação.
- **Phishing:** a rede de relacionamentos pode até nem ser o ambiente de um golpe, mas sim uma fonte de informações valiosas para viabilizar outros golpes como o phising via email. Um email de phishing com um link falso mencionando dados e fatos pessoais será sem dúvida muito mais eficaz ao persuadi-lo.

Medidas preventivas

Diante de tantas possibilidades de golpe e armadilhas, algumas medidas podem ser tomadas para reduzir as chances de se tornar alvo fácil e assim, balancear as funcionalidades do serviço com a sua privacidade e risco.

1. Evite utilizar senhas óbvias ou fáceis demais e sempre a substitua com regularidade ou sempre que desconfiar de sua confidencialidade.
2. Evite disponibilizar informações muito pessoais, que em geral, só sua família ou pessoas muito próximas deveriam ou poderiam saber.
3. Evite disponibilizar telefones de contato e endereços físicos, a não ser que exista um interesse comercial no uso do serviço.
4. Evite disponibilizar fotografias que exponham detalhes de sua residência ou trabalho, ou ainda, fotografias que permitam dupla interpretação.
5. Evite disponibilizar fotografias que exponham outras pessoas de seu convívio, especialmente familiares, a menos que previamente autorizadas.
6. Evite autorizar pessoas desconhecidas, mesmo que lhe pareçam familiar ou lhe tenham enviado uma mensagem de solicitação. Lembre-se do conceito de herança de confiança, isso poderá representar uma ameaça aos seus amigos.
7. Evite criar e entrar em comunidades de gosto duvidoso ou simplesmente com título e descrição que são sejam inteiramente alinhadas ao seu perfil. Você pode ser mal interpretado.
8. Evite utilizar fotografias em seu perfil que simbolizem algo muito diferente do que você realmente é. Desta forma, evitará atrair pessoas mal intencionadas ou compatíveis com o simbolismo equivocado transmitido pela imagem.
9. Habilite o recurso de identificação do visitante. É uma boa forma de conhecer o perfil de quem tem se interessado em conhecer você e assim, lhe permitirá identificar possíveis equívocos na definição do seu perfil e na escolha das fotografias.
10. Não clique em links enviados através da rede de relacionamentos, pois além de não haver qualquer razão aparente para se usar este recurso, esses têm sido alvos de ataques de phising.
11. Nunca confie inteiramente no que é escrito e disponibilizado na rede de relacionamentos. A fragilidade dos processos de identificação não garante a autenticidade dos usuários e a integridade das mensagens.
12. Não haja como se a Internet e o próprio ambiente da rede de relacionamentos fossem um playground onde tudo é brincadeira. Assim, tome cuidado ao criar e entrar em comunidades que ferem direitos, que tenham qualquer associação ao crime ou representem gostos duvidosos. De alguma forma, sua escolha reflete uma vontade e um pensamento e você poderá, mesmo que inconscientemente, ser confundido.
13. Como parâmetro de decisão, evite disponibilizar qualquer informação que você não teria coragem de contar ao sorveteiro que lhe vendeu o picolé de chocolate no último domingo de sol. Isso porque até ele poderá ser também usuário da rede de relacionamentos.

A lista acima revela recomendações, o que não impede que algumas sejam ignoradas se o usuário encontrar motivos reais após avaliar o risco inerente e os benefícios de cada atitude negligenciada.

Apesar de estarmos falando de um ambiente virtual e moderno demais para a realidade das décadas passadas, me parece que a velha máxima: “diga-me com quem andas e te direi quem és.”, continua valendo. Por isso, cuide bem do seu perfil, escolha bem seus amigos e comunidades e seja feliz também no mundo dos bytes.

Marcos Sêmola *é Diretor de Operações de Security & Information Risk da Atos Origin em Londres, Consultor Sênior em Gestão de Segurança da Informação, certificado CISM, BS7799 Lead Auditor, Membro da ISACA, ISSA, CSI e fundador do IISP – Institute of Information Security Professionals of London. Professor da FGV, Pós Graduado em Negociação e Estratégia pela London School, MBA em Tecnologia Aplicada, Pós Graduado em Marketing e Estratégia de Negócios, Bacharel em Ciência da Computação, autor de livros sobre gestão da segurança da informação e inteligência competitiva. Premiado SecMaster® em 2003 e 2004, tornando-se membro da comissão em 2005. Visite www.semola.com.br ou contate marcos@semola.com.br*