

102 – Agosto de 2008

Iphone 3G: uma granada no bolso?

COBIT que nada! Diferente do planejado, vamos mudar os rumos e falar este mês sobre a ‘sensação’ mundial. O novo telefone celular da Apple, o Iphone 3G lançado dia 11 de Julho.

Sem perder tempo com revisões ou detalhamentos sobre os novos recursos, que muitos já têm feito de forma competente mundo a fora, vamos falar sobre segurança e os riscos potenciais do novo dispositivo. O Iphone 3G chega quebrando alguns paradigmas, não necessariamente quando analisamos suas qualidades de forma isolada, mas sim por reunir um pacote de recursos que sobrepõe algumas limitações de seus antecessores.

Sob a ótica da segurança, ele também se destaca, mas desta vez por potencialmente adicionar mais risco ao bolso dos usuários. Estou me referindo aos riscos de furto, risco de vazamento de dados e especialmente risco de quebra de privacidade. Vamos iniciar uma análise *topdown* organizada por tópicos, começando pelas características comuns aos demais telefones móveis, até chegarmos aos fatores que acrescentam risco.

- Por ser um aparelho móvel, portátil, e ainda mais leve, fino e com maior autonomia de bateria, será transportado mais facilmente, sem que limitações de espaço incomodem, o que o fará estar com seu usuário em um número maior de lugares por mais tempo, aumentando sua exposição.
- Por possuir um sistema fácil de usar, uma interface agradável, mais espaço de armazenamento e ainda mais recursos de integração com outras aplicações, mais usuários o desejarão e se sentirão aptos a utilizá-lo plenamente, o que significa que mais dados pessoais serão armazenados e transportados nele, aumentando os riscos.
- Por ser 3G, oferece um substancial aumento de velocidade de conexão, o que se traduz em maior velocidade para acessar páginas Internet e receber e enviar arquivos, fazendo com que, em um acesso não autorizado, se consiga copiar mais informações em um menor espaço de tempo.
- Por vir habilitado a suportar tecnologias diferentes de conexão sem fio, como Wireless, Bluetooth e a própria rede de telefonia celular, existe o risco real de ter um dispositivo desconhecido e não autorizado, realizando acessos ao seu aparelho e, portanto, aos dados armazenados nele.
- Para delírio dos usuários, com toda razão, o aparelho não funciona mais como uma ilha de difícil acesso. Ele vem amparado pela Apple Store que promete disponibilizar uma infinidade de aplicações próprias e também desenvolvidas por terceiros. É sem dúvida um grande atrativo e uma ótima solução para permitir ao usuário extrair o máximo do aparelho, mas na teoria a Apple perde controle sobre os programas e códigos que residem no aparelho, abrindo uma potencial brecha para códigos maliciosos, programas espíões, aplicativos defeituosos e toda sorte de arquivos que uma cabeça hacker é capaz de inventar.

- Sua alta popularidade, ao mesmo tempo em que garante mercado promissor para viabilizar mais investimentos da própria Apple e de terceiros, atrai naturalmente a atenção dos codificadores de vírus ou de programas mal intencionados, fazendo com que os usuários tenham que conviver, de agora em diante, com potenciais perdas de dados, resets inesperados ou, na melhor das hipóteses, com a rotina de atualizar seu *mobile* antivírus regularmente.
- O pequeno notável ainda vem com inteligência geo-referenciada, ou GPS. Utiliza a tecnologia de triangulação baseada no sinal das antenas de telefonia celular para localizá-lo no mapa e traçar seu caminho, o que faz maravilhas pelos usuários, sem sombra de dúvida, mas também potencializa a quebra de privacidade. Isso porque, de uma forma ou de outra, esses dados estão armazenados no aparelho e com todo seu potencial de conectividade, permite que estranhos obtenham acesso não autorizado e possam saber por onde você andou. Até que alguma mente criativa viabilize também o monitoramento em tempo real!
- Como se não bastasse, os problemas potenciais que o novo dispositivo oferece transcendem a esfera digital e pode afetar sua integridade física também. Por se tratar de um equipamento altamente desejado no mundo todo, seja por seu design, por seu estilo, pelo alto valor pago no mercado negro ou simplesmente pelo status que ele oferece, o usuário poderá estar em perigo se for visto ao telefone em cidades perigosas. E não é preciso se esforçar muito para imaginar o que os ladrões serão capazes de fazer por ele, dado o que já fazem com seus irmãos GSM mais humildes.

Você pode estar se perguntando agora se comprar o Iphone 3G é mesmo uma boa escolha. Eu diria que a resposta esta com você. Como tudo na vida, você precisa fazer escolhas baseadas nos riscos associados. Da mesma forma, você precisa avaliar as ameaças, os impactos que um furto de informação, uma quebra de privacidade ou até mesmo a perda do aparelho pode gerar. Se o impacto resultante da análise for inaceitável, você pode ainda tomar ações de mitigação, ou melhor, ações que reduzam os riscos até que você se sinta confortável para tomá-lo.

Algumas medidas genéricas que você pode adotar para viabilizar sua decisão de adquiri-lo:

1. Procure conhecer as funções de acesso ao aparelho protegidas por senha. Habilite-as e procure usar senhas únicas e mais complexas evitando sua fácil descoberta.
2. Se suspeitar que sua senha de acesso tenha sido descoberta, troque-a imediatamente.
3. Desative os dispositivos de conectividade que não são usados com regularidade, ligando-os apenas quando necessário, e mesmo assim, certificando-se de combinar eletronicamente senhas com o outro dispositivo para que a conexão seja autenticada.
4. Seja rigoroso ao selecionar os dados que irá armazenar e transportar em seu Iphone. Não é pelo fato de ter espaço de sobra que você terá de levar cópias de documentos privados, senhas de todos os seus cartões de crédito ou ainda contratos e outros documentos importantes. Se mesmo assim for necessário, procure um aplicativo que proteja seus dados armazenados com criptografia.
5. Mesmo que seu plano de acesso seja generoso, não deixe o aparelho conectado à Internet a esmo. Assim como em seu computador, quanto mais tempo conectado, mais exposto você e seus dados estarão. Vale também para o Iphone a mesma regra

usada nos computadores de só baixar aplicativos de fontes confiáveis, a começar pelos programas do *underground* que prometem desbloquear ilegalmente o seu Iphone. Cuidado, além de perigoso, é crime!

6. Com relação aos aplicativos distribuídos pela própria App Store, mesmo que de terceiros, não há muito a fazer, pois ainda não se sabe em detalhes como será a política de aprovação e validação de aplicativos.
7. Quanto ao recurso de GPS e o potencial risco de quebra de privacidade, infelizmente não estou qualificado a falar dos detalhes já que não obtive informações sobre as formas de armazenamento desses dados. Em todo caso, se houver a possibilidade de apagar regularmente o histórico do aplicativo como se faz com os browsers Internet, faça-o.
8. Sobre segurança física, adquira um *handset*, ou melhor, um daqueles pontos de ouvido que se conectam ao seu telefone via Bluetooth. Assim você poderá manter o aparelho escondido de olhares suspeitos e ainda assim falar com tranquilidade sem revelar o conteúdo do seu bolso.

A propósito, estou à espera do meu Iphone 3G, produto que também desejo e que, para o meu perfil de risco, é seguro o suficiente.

Iphone 3G, aproveite com moderação.

Marcos Sêmola é Global IT GRC Manager da Shell International Limited Gas & Power na Holanda, CISM, BS7799 Lead Auditor, PCI Qualified Security Assessor; Membro fundador do Institute of Information Security Professionals of London. MBA em Tecnologia Aplicada, Professor da FGV com especialização em Negociação e Estratégia pela London School, Bacharel em Ciências da Computação, autor de livros sobre gestão da segurança da informação, governança e inteligência competitiva. É ainda fotógrafo Getty Images com trabalhos publicados no Brasil, Estados Unidos, Inglaterra e Holanda www.s4photo.co.uk Visite www.semola.com.br ou contate marcos@semola.com.br

Nota: Este artigo expressa exclusivamente a opinião pessoal do autor, não representando necessariamente a opinião da empresa citada.