

Digital Insight – Security Bulletin, December 16, 2004  
Addendum – Bulletin text, with notes and research

FROM DIGITAL INSIGHT:

Internet Banking, as provided by Digital Insight, is secure. However, there are things that people can do, either at home or at their place of business, to make their own computers insecure. Users need to safeguard their own computers. This means that they need up-to-date anti-virus software, firewalls, properly patched software (Windows, browsers, etc) and they need to properly safeguard their login information. In some cases, users can install software on their computer that subverts all these safeguards, thus putting their personal information in jeopardy. Users need to exercise caution before loading software from the Internet on their computer. Before doing so, they should understand what it does, who sponsors it and the privacy policy of the sponsoring organization. People need to read reports from the using community on the Internet that the software is safe and works as advertised."

SECURITY BULLETIN TEXT, RELEASED DECEMBER 16, 2004:

Digital Insight - Security Bulletin  
December 16, 2004

There are organizations on the Internet that offer 'free services' such as Internet acceleration or email virus scanning. Some of those organizations have 'privacy policies' that are so loosely defined as to allow them to harvest and share information that is universally considered to be personal and highly sensitive by Internet users. Such organizations ask unwitting end users to configure their browsers to cause all web traffic, including highly sensitive encrypted secure traffic to be decrypted, pass through that organization's servers to be harvested and then continue on to its intended destination. Hence, information that is thought by the end user to be inaccessible to everyone except the intended recipient is collected, and according to liberal privacy policies, may be shared by the intermediaries with unnamed third parties. We believe such organizations may rely upon the fact that many inexperienced Internet users don't understand the ramifications of such a situation (referred to in information security circles as a 'man-in-the-middle' exploits), or that they will carelessly click through acceptance terms without reading the fine print of the privacy policy. In our opinion, this dangerous situation is made worse by the fact that end users' efforts to uninstall such software on their computers has been designed so that it will often fail, leaving what amounts to a back door by the organization to usurp what are supposed to be private communications in the future.

Consider MarketScore, (formerly known as NetSetter) which we believe follows this sort of business model. MarketScore installs its own trusted root certificates, so that it can intercept secure (SSL) connections made by the end user machine.

The privacy policy of MarketScore states:

...Marketscore monitors all of your Internet behavior, including both the normal web browsing you perform, and also the activity you may have through secure sessions, such as when filling a shopping basket or filling out an application form that may contain personal financial and health information...

... We monitor the Internet connections of our users so we can not only accurately and anonymously model the browsing habits of Internet users, but also their shopping, registration, and other interactions as well...

... In addition to the monitoring of your Internet behavior, we may also combine the information that you provide us with information such as credit or prescription information that we obtain from third parties such as consumer preference reporting companies, credit reporting agencies, and prescription benefits managers....

... There are some limited cases in which we share personally identifiable information with third parties. Specifically, we provide personally identifiable information to third parties for the purpose of conducting the secure and confidential matches discussed more fully above....

It is important that Internet Banking users be made aware that those Internet companies that use technologies to intercept encrypted communications have full access to end users' personal information and have publicly stated that they can share users' information with third parties.