

SCAM ALERT #6

Beware when accessing “free services” on the Web

Offers of “free services”, such as Internet acceleration or e-mail virus scanning, are becoming more and more commonplace. While these offers might sound enticing, some providers have “privacy policies” that are very vague, allowing them to harvest and share your confidential information.

How can it happen?

Organizations ask unwitting end users to configure their browsers a certain way. When this is done, all Web traffic, including highly sensitive encrypted information, can be decrypted, harvested by the company making the “free” offer, and then sent on to its intended destination. This means that information you intended for only one recipient may actually be shared with unnamed third parties.

Many of these organizations rely on the fact that some Internet users either don’t understand the ramifications of accepting their free-offer terms, or that they will carelessly click through acceptance terms without reading the fine print of the privacy policy.

Be aware that companies using technology to intercept encrypted communications have full access to your personal information and publicly state that they share users’ information with third parties.

How can I stay safe?

Protect yourself by carefully reading all terms and conditions, as well as an organization’s privacy policy before accepting the offers. Companies should clearly state their practices, and some, like SEFCU, protect your information by only sharing it with subsidiaries or vendors which help provide member services.

SEFCU is committed to helping members protect themselves against fraud. This is the sixth in a series of SCAM ALERTS to educate members about deceptive activities that could harm members’ financial security. While we cannot advise members of every scam, we hope the series will advance awareness of privacy and security issues.

©SEFCU, January 2005