SPYWARE

The Internet has become a popular method for both conducting business and managing finances through online banking relationships. While most financial institutions and some individuals have taken steps to protect their computers, many firewall and anti-virus software packages do not protect computers from one of the latest threats, "spyware" – a form of software that collects personal and confidential information about a person or organization without their proper knowledge or informed consent, and reports it to a third party.

Spyware Infection

Spyware is usually installed without a user's knowledge or permission. However, users may intentionally install spyware without understanding the full ramifications of their actions. A user may be required to accept an End User Licensing Agreement (EULA), which often does not clearly inform the user about the extent or manner in which information is collected. In such cases, the software is installed without the user's "informed consent."

Spyware can be installed through the following methods:

- Downloaded with other Internet downloads in a practice called "bundling." In many cases, all the licensing agreements may be included in one pop-up window that, unless read carefully, may leave the user unaware of "bundled" spyware.
- Directly downloaded by users who were persuaded that the technology offers a benefit. Some spyware claims to offer increased productivity, virus scanning capabilities or other benefits.
- Installed through an Internet browsing technique called "drive-by downloads." In this technique, spyware is installed when a user simply visits a Web site. The user may be prompted to accept the download believing it is necessary in order to view the Web page. Another method is to prompt the user to install the program through pop-up windows that remain open, or download the software regardless of the action taken by the user.
- Automatically downloaded when users open or view unsolicited e-mail messages.

Behaviors Associated With Spyware

- Spyware can be difficult to detect and remove because it:
- Does not always appear as a running program in the Window's Task Manager; therefore, the user may be unaware that his or her computer is infected.
- May not include a removal option in the Windows "Add/Remove Programs" function. When such an option is present, the removal process may not eliminate all components, or it may redirect the user to an Internet site to complete the removal. This often results in new or additional infection rather than removal. In addition, some spyware includes a feature to reinstall itself when any portion is deleted.
- May cause a further infestation by installing other spyware programs onto users' computers.

FDIC Recommendations to Customers

- The FDIC recommends the following that customers can take to prevent spyware from being downloaded on their computers.
- Customers can prevent and detect spyware by:
- Installing and periodically updating anti-spyware, virus protection and firewall software.
- Adjusting browser settings to prompt the user whenever a Web site tries to install a new program or Active-X control.
- Carefully reading all End User Licensing Agreements and avoiding downloading software when licensing agreements are difficult to understand.
- Maintaining patches to operating systems and browsers.
- Not opening e-mail from untrustworthy sources.