Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

June 25, 2013

CYBER CRIMINALS CONTINUE TO USE SPEAR-PHISHING ATTACKS TO COMPROMISE COMPUTER NETWORKS

The FBI has seen an increase in criminals who use spear-phishing attacks to target multiple industry sectors. These attacks allow criminals to access private computer networks. They exploit that access to create fake identities, steal intellectual property, and compromise financial credentials to steal money from victims' accounts.

In spear-phishing attacks, cyber criminals target victims because of their involvement in an industry or organization they wish to compromise. Often, the e-mails contain accurate information about victims obtained via a previous intrusion, or from data posted on social networking sites, blogs, or other websites. This information adds a veneer of legitimacy to the message, increasing the chances the victims will open the e-mail and respond as directed.

Recent attacks have convinced victims that software or credentials they use to access specific websites needs to be updated. The e-mail contains a link for completing the update. If victims click the link, they are taken to a fraudulent website through which malicious software (malware) harvests details such as the victim's usernames and passwords, bank account details, credit card numbers, and other personal information. The criminals can also gain access to private networks and cause disruptions, or steal intellectual property and trade secrets.

To avoid becoming a victim, keep in mind that online businesses, including banks and merchants, typically will not ask for personal information, such as usernames and passwords, via e-mail. When in doubt either call the company directly or open your computer's Internet browser and type the known website's address. Don't use the telephone number contained in the e-mail, which is likely to be fraudulent as well.

In general, avoid following links sent in e-mails, especially when the sender is someone you do not know, or appears to be from a business advising that your account information needs updated.

Keep your computer's anti-virus software and firewalls updated. Many of the latest browsers have a built-in phishing filter that should be enabled for additional protection.

If you believe you may have fallen victim to a spear-phishing attack, file a complaint with the FBI's Internet Crime Complaint Center, https://www.ic3.gov/