

SECURITY ALERT

January 27, 2010

To: Our Valued Legal Industry Customers
From: Tammie Blancett, SpiritBank Director of Security

IMPORTANT! FBI warning for Spear Phishing emails targeting Law Firms

Recently a warning was posted on the FBI website informing us of an old type of attack (Phishing) being used to target two specific industries – Law and Public Relations firms.

The FBI has assessed with high confidence hackers are executing this ‘spear fishing’ attack with extreme accuracy. The hackers are using this specific technique in hopes delivery a malware program to be installed on the law firm’s computer so valuable non-public information can be stolen. Most often the target information they are looking for is the banking accounts, passwords and ID needed to do online banking. Once they have this information, it only takes minutes to transfer money from the victim’s accounts.

The email is a social engineering email designed to bypass the technological network defenses. The hacker is trying to exploit the ability of the end user to launch the malware from the internal network. The cyber criminal wants the individual to load the software (unknowingly) usually by clicking a URL link in the email or attaching a file to the email. The body of the email is meant to entice the recipient to open the attachment to click on the link. When one of these actions occurs, the malicious code is triggered to be installed. A number of intrusion detection technologies are unable to stop these attacks because the subject lines are written such that they appear to be appropriate for the legal industry. This file does not necessarily have to be a file with the extension of ‘.exe’. The other file formats can be ‘.zip’, or ‘.jpeg’. The body of the email is also written to appear to be relevant to the legal field enticing the recipient to act on the request. Please note: just by opening the message will not be enough to cause the infection. The link or the attachment must be clicked upon to infect the system.

The best course of action is not to click on any links in any email. Always type the URL addresses yourself. If you feel you have been infected, it is recommended to act immediately – stop using the machine and get it checked. Definitely, do not use the machine to do any online business. To see this posting and others, you can go to the FBI Cyber investigations website.

The FBI Cyber investigations website is:
www.fbi.gov/cyberinvest/escams.htm

We at SpiritBank want to do everything we can to prevent you from becoming a victim of information theft. If you have any information, questions or concerns, please contact me at 918-295-7497 or by email: tblancett@spiritbank.com.

Regards,

Tammie Blancett, Director of Security
SpiritBank