E10 International Implications of Phishing Schemes: High-Tech Identity Theft

John D. Saba, Jr., JD, Office of the Attorney General of Texas, 3005 University Avenue, Austin, TX 78705; and Paul L. Singer, JD*, Office of the Attorney General of Texas, 300 West 15th Street, Austin, TX 78701*

After attending this presentation, attendees will understand the concept of a phishing scheme, the illusiveness of conducting the scam, and the limitations in battling the crime both for law enforcement and electronic forensic investigators.

This presentation will impact the forensic community and/or humanity by discussing how the scams are created and executed. Furthermore, this presentation will identify the electronic data needed to resolve the identity of the perpetrator. Finally, this presentation will discuss the ideal collaborative environment necessary for battling these crimes.

The basic phishing scheme has evolved due to the prevalence of malicious software on the Internet. Traditionally, phishing schemes were not so involved. The perpetrator would post a fake web site mimicking an actual web site (e.g., a large well-known financial institution), send phishing e-mail messages out to consumers, and then, more-times-than-not, store and collect personally identifiable information on the actual phishing web site, either to collect and use him or sell on the "e-black market." Under more advanced phishing schemes, the end result is reached with greater ease and near-complete anonymity due to the prevalence of electronic "proxies" and malicious software available on the net.

A typical modern-day phishing scheme will be presented, a) noting how one creates and executes the scheme, b) identifying how one approaches solving the phishing scheme, and c) discussing the practical barriers of battling the phishing scheme.

Phishing Scams, Identity Theft, Cyber Crime

 ** Presenting Author*