Securities Industry Software
4725 Independence Street
Wheat Ridge, CO 80033-2937
Phone: 303/590-6006
Fax: 303/590-6420
http://sis.broadridge.com/sisnet

System Advisory

Advisory No.:	#a07-036	#a07036ng
Date:	May 25, 2007	
Attention:	All Clients	
RE:	Protecting Information and Assets	

Account security is a growing issue within the technological arena, and our industry is at a particular risk due to the financial nature of our business. Stolen passwords, compromised accounts, and identity theft are a concern for everyone, costing more money, time, and resources each year. The best way to prevent these costly and potentially devastating attacks is to be educated about the best practices for safeguarding personal information. Following is some information to read and share with associates and clients about some everyday threats to personal and account information. Taking a few small steps to keep information and systems safe from would-be attackers can protect a lifetime of hard-earned assets.

How do attackers try to gain information?

Some of the most common forms of attacks are from logger programs and cross-site scripting (XSS) attacks. Attackers place logger programs on computers to "log" information as it is entered. For example, logger programs may record keystrokes, such as account numbers, user names, and passwords, and then transmit them back to the attackers for their own use. Logger programs are more common on public computers, such as Internet cafes and airports, as attackers download these programs onto the computers in hopes of gaining users' personal information. Logger programs may also be downloaded inadvertently as part of a web page or attachment as part of an XSS attack. With XSS, attackers use scripts within a page or an e-mail to download malicious programs directly into browsers or computers without the user realizing that they are downloading anything. These programs may redirect the user to fraudulent pages that will record information, read account and password information stored in the browser's "cookie" files, or even give someone else control of the computer with all of the user's rights and privileges.

What are the risks?

With the growing dependence on technology, attackers have become more resourceful and can capture nearly any piece of personal information entered or stored on computers, given the opportunity. A user name or account number entered on a website, a password to an online trading account that the browser "remembers," even a Social Security number entered as part of an application can all be captured, recorded, and stolen by attackers. This can result in fraudulent charges to accounts, liquidation of hard-earned assets, and identity theft. An increasingly common fraud practice in the securities industry is to steal a user's online account information and sell off all the assets in their account. The proceeds from these sales are then used to buy large quantities of penny stocks that the attacker already owns, artificially inflating the price just long enough that the attacker can sell off their stocks at a substantial profit. Often, this happens within a matter of hours. By the time the problem is noticed, the assets have been liquidated.

How can this be prevented?

Prevention is key. Many security breaches start out as one small security mistake. To help keep information and identity safe, urge clients and associates to follow these rules:

- Install anti-virus and anti-spyware on computers and keep them updated; these can catch many problems on computers early on that might otherwise go unnoticed.
- Avoid using public computers to log in to financial sites; public computers are easy targets for attackers to try to log information.
- Do not follow links from e-mails, as the text of the link and the location that it actually points to may not necessarily match; enter links manually to go to the correct site.
- Verify web site addresses before entering information; it is easy for attackers to make a web site look legitimate to steal information, but the web site address will tell the truth.
- Choose passwords with a combination of upper and lower case letters, numbers, and special characters that are not part of the dictionary; different types of characters and an unusual combination of characters make it more difficult for attackers to crack passwords.
- Change passwords every 30 days; changing passwords frequently lowers the risk of having it stolen.
- Do not download attachments from e-mails unless it is expected, even if it is from someone known; many viruses appear to be sent from people who are in the user’s e-mail address book.
- Be suspicious of e-mail, web sites, and public computers; if something doesn’t seem right, it’s probably not.

These steps can help to keep information and assets safe. A few minutes of caution can save a great deal of time, trouble, and money for your clients and your firm.

Please contact Client Services if you have any questions.

Phil Goldsberry / Manager Client Services