Schools and Colleges seen as 'Soft Targets' for Cyber Criminals

Leaders of schools and institutions of higher education (IHE) have been paying much attention over the past several years to increasing the physical security and access control of their buildings and campuses. At the same time, however, reports suggest that educational leaders may have been neglecting the security of their computer systems/networks.

While threats posed by student hackers, such as changing grades or gaining personnel information continue to be of concern, there is an emerging and more insidious threat to school and IHE finances from outside gangs of cyber criminals.

Vigilance and education

In fall 2009 alone, educational institutions in Colorado, Illinois, Pennsylvania and Oklahoma had money stolen from their bank accounts – totaling tens of thousands of dollars in each instance.

Since then, other schools have fallen prey to cyber criminals' attempts to siphon money from their bank accounts. In January 2010, a small rural school in New York State was targeted for $3.8 million. In some of these instances, the stolen monies were recovered – but in most instances not completely, leaving a significant loss of critical funds needed for education and school operations.

This growing wave of cyber crime against schools and IHE across the United States has caught the eye of Federal and State law enforcement agencies, IT Security Professionals, School Administrators, Banking Industry Officials, and Insurance and Risk Management Professionals.

Experts agree it is nearly impossible to completely protect against cyber criminals attacking school or IHE computer systems and networks. Vigilance in maintaining firewalls, anti-virus software and security patches – along with educating staff and students about cyber security and cyber ethics – is key in managing the risk of hackers and other network intruders gaining access to banking and other sensitive information, and control over networks to carry out other crimes.

Critical information and best practices

A March 2010 **Cyber Security Advisory** issued by the United States Secret Service and Federal Bureau of Investigation, along with New York State law enforcement and various Financial Services Information Sharing and Analysis Centers (ISACs), contains critical information and best practices in managing the cyber crime

exposure for schools and IHE countrywide. It is highly recommended that you download and review the complete document at the following link:
http://www.cscic.state.ny.us/documents/Wire-transfer-fraud-recommendations-2010.pdf

Excerpts from the Cyber Security Advisory

- **Install a security software suite** from a reputable vendor that includes antivirus, anti-spyware, malware and adware detection. Keep the software up to date through an automatic update feature and configure it to routinely perform recurring, automated complete system scans.
- **Routinely install all new software and hardware patches** or use the automatic update feature when available. Ensure all your software, including your operating system and application software such as Microsoft Office, Adobe Flash, Apple QuickTime, Adobe Acrobat, etc., is updated, too – not just the computer's operating system.
- **Use a dedicated computer for all online transactions** and implement white listing methods to prevent the system from going to any site/address that does not have a documented business need.
- **Educate users on good cyber security practices** to include how to avoid having malware installed on a computer, along with new malware trends like the development of malvertizing, where malware is hidden in the code of a legitimate Web site.
- **Immediately report any suspicious activity** in your accounts. There is a limited recovery window and a rapid response may prevent additional losses.
- **Make sure the Web address of the banking site you use starts with "https://" instead of "http://".** The "s" indicates a secure transaction, using a different method of communication than standard Internet traffic.
- **Be suspicious of e-mails and text messages** purporting to be from your financial institution or a government agency. Financial institutions should not contact you via e-mail to request that you verify information.
- **Always lock your computer when you leave it unattended.** Set the computer to automatically lock after a set period of inactivity, e.g. 15 minutes.
- **Do not allow** your computer or web browser to save your login names or passwords.
- **Use a strong password** – at least 10 characters, combining upper and lower case letters, numbers and symbols.
- **Properly log out of all financial institution Web sites** and close the browser window. Simply closing the active window may not be enough.
- **Do not open e-mails from un-trusted sources or suspicious e-mails from trusted sources.** Be aware that "Reading Pane" features, like those within Microsoft Outlook, automatically open the e-mails they display.
- **Check with your financial institution** about enabling "alerts" and other security measures that may be available. Some financial institutions offer additional security measures, **but they are only available upon request.**

Meet with your financial institution representative to review the availability of fraud prevention services such as **ACH Debit Blocks, ACH Debit Filters, Positive Pay, Positive Pay with Payee Verification, Teller Line Positive Pay Verification, Check Cashing Limits, Reverse Positive Pay**, and **Post No Checks**. These services may not be available in every bank so it's important to inquire! *Many of these services may be free or of little cost to the school or IHE compared to the potential loss of dollars should cyber criminals gain access to your school or IHE bank accounts*.

Some final – yet important – recommendations:

- Review your bank account balances daily and reconcile accounts regularly.
- Meet with your insurance agent to discuss the exposure, availability of and appropriate limits needed for crime coverage, computer fraud and funds transfer.

