MANAGING YOUR MONEY

Protecting Against The Latest Cyber Crime: Web-Based Extortion

(NAPSA)—There are ways to protect yourself from Internet crimes, including identity theft and one of the faster-growing threats: extortion.

Becoming a victim of identity theft remains the No. 1 concern of adults in the U.S., with total identity fraud losses reaching $1.1 billion last year, according to the National Crime Prevention Council and Federal Trade Commission, respectively.

Dollar losses for cyber extortion could be even higher, as this crime is often unreported because victims simply pay to avoid embarrassment.

While cyber extortionists tend to target wealthy individuals, people of varying demographics can also become victims. Extortionists can exploit the activities of any family member, threatening humiliation to blackmail their targets.

"With the increasing popularity of sites like MySpace and YouTube, opportunities for exposure continue to multiply. If family members use the Internet for socializing or personal blogs, information such as names, addresses and phone numbers should be deleted. Video-sharing sites can offer an inside look into a home or issues some would rather keep private. Criminals seek this information for extortion," says James Kane, president of Hub International Personal Insurance, a North American insurance broker offering coverage and risk management services.

While cyber extortion may be an emerging concern among the more commonly known online scams, experts say people need to work harder to protect themselves from identity theft.

Victims can take up to 16 months to fully recover from identity theft.

Kane explains, "Many of the 'soft' costs associated with ID theft can't be recovered. That's why, in

Regularly updating protective software can help keep identity thieves and Web-based extortionists at bay.

addition to coverage, people should consult risk advisors to create a cyber security protection plan."

Protecting Yourself

Key suggestions for protecting your identity include:

• **Regularly update computer software**: New viruses and spyware pop up daily; therefore, anti-virus software should be kept up-to-date.

• **Purchase a shredder that cuts paper into confetti**: Thieves often use discarded information to collect victims' personal data.

• **Eliminate unwanted credit solicitations**: Visit www.optout prescreen.com to stop receiving prescreened applications.

• **Reduce access to your personal data**: Never provide personal data to telemarketers or in response to e-mails.

• **Monitor financial records**: Review financial statements each month and investigate anything suspicious.

• **Review Social Security benefits**: Request a statement at www.ssa.gov and alert the Social Security Administration of any irregularities.

For more information, visit www.ncpc.org or www.hubinterna tional.com.