Tips For Avoiding Social Networking Disasters

(NAPSA)—Small businesses need effective, low-cost marketing strategies, and tools like Facebook and Twitter deliver megahits for microbudgets. Yet while many business owners are being advised to engage customers via social media, not all are informed of the risks.

Social network sites are fertile waters for Internet pirates who troll for unsuspecting victims, hoping to steal data by planting malware in the form of computer viruses, worms, Trojan horses and spyware.

If you are a small-business owner, work for one or hope to become one, these tips can help keep your business data secure:

•**Share carefully.** Clearly identify what kind of business information should be on social networks. Don't post confidential information, such as financial information, passwords or anything else you would not want shared.

•**Guide employees.** Develop a social media policy on the potential risks and ways to participate safely. Include personal and professional best practices, and teach your people how to avoid scams. Remind employees to limit personal comments to their own personal pages.

•**Beware new twists.** Thirty percent of all viruses that infect computers originate from spam, targeting users with seemingly legitimate posts, such as "I just checked how many people have viewed my profile." Cyber thieves target easy victims first: individuals and organizations that haven't adequately protected their computers, networks, mobile devices, Wi-Fi and Internet connections. Another technique is "likejacking" or "clickjacking": When users click on a link, the site steals their Facebook account and spreads the spam to all their contacts.

Small businesses that take the time to understand the dangers will find that social media can be a customer magnet, building brand exposure and creating engagement with potential customers.

•**Don't automatically click on URL links.** If an offer in a social post sounds too good to be true—"Click here to win an iPad"—it probably is.

•**Protect your passwords and privacy.** Using the same password on every site can easily expose your business to account takeover. If that password is hacked or leaked, hackers can access your other site information. Instead, use different, strong alphanumeric (both letters and numbers) passwords for each of your social media accounts and keep them regularly updated.

•**Stay current with cybersecurity.** Keeping your computer security updated is the smartest way to elevate your defenses against cybercrime. Deluxe Security Solutions is a good security resource for current protection products and services such as McAfee AntiVirus Plus 2012, which defends against online viruses, malware and spyware. Through Deluxe, you can subscribe to a fraud and identity protection service such as EZShield Business Identity Restoration. This service offers a fully managed identity process with certified resolution specialists to assist business owners.