Online Crime's New Frontiers

(NAPSA)—More than ever, Americans are using new gadgets for entertainment, to communicate with friends and family and to perform their jobs. Thanks to technological advances, streaming movies, downloading music and e-mailing can be done with the tap of a finger.

Two of the most popular technology trends over the last couple of years are the ever-increasing use of mobile devices, like smartphones and tablet computers, and social networks. Together, the improvements have allowed people to broadcast information and interact with their friends and family, anywhere and anytime.

Unfortunately, while new devices and new ways of connecting have made getting online much easier, they're also providing cybercriminals with new, creepy ways of targeting victims. As more people use their "smart" devices to access the Internet and stay up-to-date with their social networks, online thieves have more opportunities to steal personal information, which can then be used or traded for their financial gain.

Norton by Symantec, the makers of Norton Internet Security, recently released its 16th Internet Security Threat Report. Among the top findings, the report revealed that mobile devices and social networks are among the hot new targets for crooks looking to make a quick buck.

One of the latest scams involves cybercriminals taking popular

Use security software on your mobile phone to protect yourself from cybercrime.

smartphone applications (or "apps") and creating "poisoned" versions. The versions may look like the originals but after unsuspecting users have downloaded them, a number of things can happen—potentially damaging or dangerous software may be installed onto your phone, unnecessary personal information may be requested or the application (and the cybercriminals controlling it) may be able to see and even control all your mobile phone activity.

"Many people aren't even aware that these kinds of mobile threats exist," said Adam Palmer, Norton's Lead Cybersecurity Adviser. "Taking precautions can be as simple as using a mobile security application and sticking to legitimate app marketplaces."

On social networks, once a cybercriminal has access to someone's account, he or she can post links to other websites on the victim's profile. These links will show up on the news feeds of the victim's family and friends and lead them to infected sites with viruses and other nasty items. The popularity of using shortened links also works in the scammer's favor, since people aren't able to easily tell if the link connects to a "bad" site. According to the Symantec report, of the total number of dangerous links found on social networking sites, 66 percent of them were hiding in shortened links.

Whether you are on a mobile phone, social network or just surfing the Web at home, it's important to remember that cybercrooks are constantly stepping up both the complexity of their attacks and the ways they target victims.

Here are some tips you can follow to protect yourself:

- Use security software on your computer and your mobile phone.
- Be cautious when clicking on links in e-mails, instant messages and social networking sites—even when coming from trusted sources, like friends and family.
- Limit the amount of personal information you make publicly available on the Internet (especially via social networks), as it may be collected by cybercriminals and used to scam you.

For daily updates on cybercrime and what you can do to protect yourself, visit www.NortonCybercrimeIndex.com.