TechNewsDaily™
Where technology meets daily life.

New Internet User? Watch Out for These 3 Traps

By Joseph Fieber, TechNewsDaily Contributor
22 June 2011 10:57 AM ET

Credit: Dreamstime

The Internet is like a digital microcosm of the real world. It is full of a virtually limitless amount of information and entertainment, but it also contains not-so-nice people looking to take advantage of you.

The more experience you have on the Internet, the more aware you become of what a scam looks like, but when you're starting out with your first computer, you're obviously more vulnerable. Here are three types of Internet scams, and what you can do to try and avoid them.

Ads: Wasting your time

Many websites generate income through advertising, and like radio or television, this can be a good way for you to get useful Internet content for free. Unfortunately, some scammers set up websites that have poor quality content created specifically to lure you in the hope you'll click on an ad so they can get paid. Thankfully, this scam usually won't harm your computer or invade your privacy, but it can be a big time-waster. To avoid this scam:

- **Stick to reputable sites**. Those you're already familiar with or have heard of stand a better chance of having high-quality content.
- **Trust your gut**. If the site doesn't feel right when you get there (maybe the site doesn’t seem very professional, to many ads, misspellings, etc), use the back arrow and investigate a different one.
- **Look around the link you want to click on**. Many advertisements will have an "ad" or "advertising" disclaimer nearby.

Phishing your information

A more serious concern on the Internet is a technique called phishing. Phishing is the method by which scammers trick you into providing sensitive information. They often do this by putting up Web pages that look like sites you are familiar with, hoping you'll type in your username, password, credit card details, etc. To avoid this scam:

- **Use an up-to-date Web browser**. The latest versions of Microsoft's Internet Explorer, Mozilla's Firefox and Google's Chrome all have built-in filters that can warn you about known phishing sites.
- **Look at the address of the page you are on**. If you're on a login page for Yahoo Mail, for example, the beginning of the address should contain "yahoo.com.” If it doesn't, be wary!
- **Also be wary of links within emails.** If you get an email from a site you use telling you to go to your account and update some info, go to the site by typing in the URL directly into the address bar of your browser.
- **Look for "secure" pages, which are less likely to be fake.** Modern Web browsers will show an indication when a page is secure, usually with a small padlock icon on the left or right side of the address bar.

Malware: How it controls your computer

Possibly most serious of threats is malware, which is software that scammers use to trick you into installing on your computer. Once installed, this software can do almost anything, from sending out emails to copying every letter and number you type (even on secure websites). Some malware even pretends to be antivirus software, and will make your computer almost unusable as it tries to get you to pay for the update that will fix the "virus" that it claims to have found. To avoid this scam:

- **Don't install any software you didn't seek out yourself.** Be sure anything you do install is from a reputable company.
- **Viruses send emails pretending to be from your friends.** Don't open attachments in your e-mail, even from people you know, unless you already know what it is, and confirmed that the person intended to send it to you.
- **Be careful with "pop-ups."** Websites can create pop-ups that pretend to be messages from your antivirus software. When one appears, close the windows and don't click on any buttons.