

Don't Fall for the Latest Online Scams

10 ways to dodge the high-tech criminals

The internet is a big part of our everyday lives—and the con artists know it. Cyber crooks are coming up with more and more ways to use the web to run their scams and cheat unsuspecting people out of their money.

Fortunately, with just a few easy steps, you can fight back and keep your hard-earned cash out of the hands of these criminals. To follow are the latest online frauds making the rounds, along with some advice on how you can protect yourself.

Social networking frauds

Online social networking sites like Facebook, LinkedIn and Twitter continue to grow in popularity. According to The Nielsen Company, the amount of time we spend on social networking and blogging sites increased 210% over the past year, with the leading sites boasting hundreds of millions of users.

These virtual communities are a great way for us to stay connected with our friends and family, but unfortunately they also can connect us to scam artists.

Thieves are devising increasingly clever ways to use these popular sites to run their cons. They'll hack into an account, pass themselves off as your friend, and then trick you into downloading malicious software...or they'll make a desperate, emergency plea for you to send them cash to a mail box...or they'll lead you to a fake web site that asks you for your private banking information.



Another ploy are the quizzes and games that ask for your cell phone number so that the results can be sent to you—and you don't know you've been conned until you see mysterious charges on your next phone bill.

Protect yourself

- If something you get from a friend looks strange—an odd-looking web address or wording that doesn't sound like something they'd write—double-check with them, in-person or over the phone, and ask if they sent you the message.
- To avoid your own account being hacked into, protect your login information and use strong passwords (easy for you to remember, but hard for others to guess) that you change frequently.
- Limit what you share on your profile page or as part of online games. Revealing information like birth dates, cell phone numbers, travel plans, and activities that take you away from home can expose you to all kinds of criminal activity, including identity theft, stalking, and home robbery.
- Install and run anti-malware software that can automatically block any malicious files before they land on your computer and do damage.

Online charity hoaxes

Most hoaxes are designed to take advantage of people's desire to help, and online charity fraud is a perfect example of this tactic. The National White Collar Crime Center reports that in 2009 alone, more than \$122 million was lost in donations to fraudulent internet charities.

Reputable charities use email, web sites, and online ads to solicit contributions—but unfortunately, so do the hoaxsters. And the latest twist on the scam involves text messaging. A few years ago, legitimate nonprofits began to use "donation by text," where you can make a donation by texting a certain number on your cell, and then the amount you give is added to your phone bill. It didn't take long for the scammers to take advantage of this and set up their own phony text numbers to bilk you out of your money.



And whenever there's a natural disaster, be particularly alert: after these tragedies, even more scam artists crawl out of the woodwork to prey on people's generosity and compassion. Saddest of all, money ends up in the hands of criminals, not of those who need the help.

Protect yourself

- Be wary of unsolicited e-mails that ask you to click on a link to give money. Unless it's from an organization that you signed up with, exercise caution if you get something out-of-the-blue asking for a donation.
- For donations you make through texting, don't give out any credit card or banking information. Legitimate charities don't need any of your financial information because your cell phone account is automatically billed; if you're asked for this information, it's a scam.
- Whether you're making a donation online, via text message, or through some other means, before you give to a charity, it's always a good idea to do your research and make sure it's a legitimate organization.



Scareware scams

Here's how it works: you're surfing the web and a pop-up window says your computer has a virus. You download the scanning tool—it's free, after all—and you're alarmed to see the long list of dangerous files found on your computer. But luckily all can be fixed with a simple purchase, so you immediately buy the software, the dire warnings go away, and you feel safer knowing that you handled this critical security issue.

But the problem is *there never was a problem*. And it wasn't software that you bought—it was "scareware," a useless program that does nothing to help and everything to harm.

This scareware scam is a growing one because it's lucrative. According to the Internet Crime Complaint Center, victims of scareware lost over \$150 million last year. The peddlers of these phony products now have your credit card information, and also may have installed dangerous Trojans and keyloggers that will capture even more of your personal data. And not only have you been swindled, but you're left with a false sense of security—instead of protecting yourself, you just walked into the lion's den.

Protect yourself

- The best solution is to ignore these messages—internet pop-ups are not a valid way to learn about the security of your computer. Simply close the pop-ups unread and, for the utmost in security, also close your browser and run an anti-malware scan to make sure no malicious files were installed without you knowing it.
- Don't let yourself be intimidated or rushed into making a fast buying decision. A software scan from a responsible company will give you straightforward and useful information, not scary and aggressive alarms.
- Before you hand over your bank account information or credit card number, it's important that you research—only buy anti-malware software from established, reputable companies.