ClubNorton
your one-stop resource center for Internet security.

Norton from symantec

Welcome | About ClubNorton | Article Library | Glossary | Norton Forums | Norton Update Center

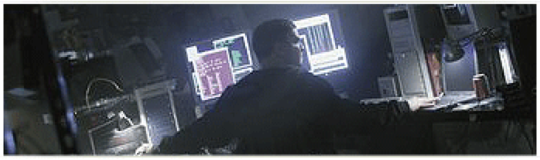
ARTICLES
- Top 5 Social Media Scams
- Meet Norton's Cyber Security Advisor
- A Life of Cybercrime
- Slow Computer? Learn How to Grease Its Lightning
- How Cybercrime Threatens You

Norton Resources
- Norton Forums
- Norton Product Reviews
- Family Resources
- Norton Today
- Norton Library

Useful Links
- Product Manuals
- Product Updates
- Order Status
- Returns
- Rebates

Tools & Support
- Symantec Security Check
- Subscription Troubleshooter
- Home & Home Office Security

ADD



Top 5 Social Media Scams

We're wired to be social creatures, and sites like Twitter and Facebook have capitalized on this to great success. According to its COO Sheryl Sandberg, Facebook draws 175 million logins every day.

But with this tremendous popularity comes a dark side as well. Virus writers and other cybercriminals go where the numbers are—and that includes popular social media sites. To help you avoid a con or viral infection, we've put together this list of the top 5 social media scams.

# 5 Chain Letters

You've likely seen this one before—the dreaded chain letter has returned. It may appear in the form of, "Retweet this and Bill Gates will donate $5 million to charity!" But hold on, let's think about this. Bill Gates already does a lot for charity. Why would he wait for something like this to take action? Answer: He wouldn't. Both the cause and claim are fake.

So why would someone post this? Good question. It could be some prankster looking for a laugh, or a spammer needing "friends" to hit up later. Many well meaning people pass these fake claims onto others. Break the chain and inform them of the likely ruse.

# 4 Cash Grabs

By their very nature, social media sites make it easy for us to stay in touch with friends, while reaching out to meet new ones. But how well do you really know these new acquaintances? That person with the attractive profile picture who just friended you—and suddenly needs money-is probably some cybercriminal looking for easy cash. Think twice before acting. In fact, the same advice applies even if you know the person.

Picture this: You just received an urgent request from one of your real friends who "lost his wallet on vacation and needs some cash to get home." So, being the helpful person you are, you send some money right away, per his instructions. But there's a problem: your friend never sent this request. In fact, he isn't even aware of it. His malware-infected computer grabbed all of his contacts and forwarded the bogus email to everyone, waiting to see who would bite.

Again, think before acting. Call your friend. Inform him of the request and see if it's true. Next, make sure your computer isn't infected as well.

# 3 Hidden Charges

"What type of STAR WARS character are you? Find out with our quiz! All of your friends have taken it!" Hmm, this sounds interesting, so you enter your info and cell number, as instructed. After a few minutes, a text turns up. It turns out you're more Yoda than Darth Vader. Well, that's interesting…but not as much as your next month's cell bill will be. You've also just unwittingly subscribed to some dubious monthly service that charges $9.95 every month.

As it turns out, that "free, fun service" is neither. Be wary of these bait and switch games. They tend to thrive on social sites.

# 2 Phishing Requests

"Somebody just put up these pictures of you drunk at this wild party! Check 'em out here!" Huh? Let me see that! Immediately, you click on the enclosed link, which takes you to your Twitter or Facebook login page. There, you enter your account info-and a cybercriminal now has your password, along with total control of your account.

How did this happen? Both the email and landing page were fake. That link you clicked took you to a page that only looked like your intended social site. It's called phishing, and you've just been had. To prevent this, make sure your Internet security includes anti-phishing defenses. Many freeware programs don't include this essential protection.

# 1 Hidden URLs

Beware of blindly clicking on shortened URLs. You'll see them everywhere on Twitter, but you never know where you're going to go since the URL ("Uniform Resource Locator," the Web address) hides the full location. Clicking on such a link could direct you to your intended site, or one that installs all sorts of malware on your computer.

URL shorteners can be quite useful. Just beware of their potential pitfalls, and make sure you have real-time protection against spyware and viruses.

Bottom line: Any sites that attract a significant number of visitors are going to lure in a criminal element, too. Norton Internet Security offers the comprehensive protection you need to defend yourself against all of these dangers. With it, you can surf with confidence.

Legal Notices ·Privacy Policy · Site Feedback ·Contact Us ·Global Sites ·License Agreements ·RSS