reddit_linkedin_10_percent.docx

I don't know if this is a very *new* teacher, or a not-so-new one, but when I was in college I was going out with someone who was studying to become a teacher. When the program began properly (sophomore year), rules were passed on to us that we were to be very careful about the things we posted on the wall, and tagging pictures without permission was strictly verboten. This was because the College of Education monitored social media accounts of students as part of the program. The idea is that it was to enforce distance between them and their students, and to be very aware than there needs to be a strict separation between their personal lives and the work lives, and that when you combine students and the Internet, one can breach its way into the other, whether you like it or not. Hell, even my high school teachers, and college professors/staff/faculty had a strict rule: I will not connect with you on any social networking site (except LinkedIn) until you graduate/drop-out/are no longer a student here.\n\nSo I have to wonder: what the *hell* was this teacher thinking?!

I will generalize to a tech startup that just had a major data breach. If it's not publicly verifiable -- you should deny it completely. But assuming, like LinkedIn, that it's already obvious that the event occurred, I'd recommend taking two strategies in parallel:\n\n1. Be transparent while showing what you've learned. You want to see human here. This was a mistake. You keep customer privacy and security as a high priority. What you want to emphasize most though is that you realized the problem and it has been fixed. This will not happen again.\n\n2. Downplay the damage. Instead of focusing on the 8 million passwords, focus on the fact that it's only a small percentage of your userbase. Say you've always recommended secure passwords, and if users followed your instructions then they should be alright (although it's always a good idea to change their password anyway).

LinkedIn via Twitter says:\n\n> Our team continues to investigate, but at this time, we're still unable to confirm that any security breach has occurred. Stay tuned here.\n\nhttps://twitter.com/LinkedIn/status/210390233076875264

This is what you should do:\n\n1) On your Resume and cover letter use your middle name (full name) ex. John Paul Smith\n\n2) set up web 2.0 accounts (tumblr, facebook, twitter, linkedin) under your full name.\n\n3)put up some content on each web 2.0 account, and link to them with the anchor tag being 'profile' {facebook, twitter, } and 'resume' for linkedin.\n\n4) Try to get your friends to link to the new web 2.0 accounts with your full name.\n\nTherefore when an employer searches your name, they will likely copy/paste in your full name to google. Then google will return the new sanitized web 2.0 property, and your problem is solved.\n\nAlso, trying changing your facebook profile name to include your full name (name + middle name) for a faster hack.

The only "communication" I've seen from LinkedIn is when I logged in to change my password and top 3 trending tech stories were all about the password breach.

[Disappointment]

LinkedIn confirms breach:\n\nhttp://blog.linkedin.com/2012/06/06/linkedin-member-passwords-compromised/\n\nsummary: they have invalidated compromised passwords, users with these will get an email about password and about what happened *[Rebuild]*