

Virtual Imposters Can Cause Real Damage to Business

For the same reasons corporations and organizations protect their trademarks and brand names, they now need to proactively manage the online presence of their decision-makers and personnel.

Everyone by now is aware that they need to be discreet with what they put on social networking sites and most corporations now have policies designed to prevent unauthorized disclosure of confidential corporate information or statements by personnel that may result in bad publicity. However, the danger one poses to oneself is nothing compared to the danger embodied by a criminal bent on profit or revenge. The damages an imposter could cause a large corporation, a public figure, a sports franchise or a celebrity could easily go beyond the merely inconvenient to the financially disastrous.

First, let's look at some real examples to highlight the threat. In early 2009, an imposter created a Twitter account posing as Tony La Russa, the manager of the St. Louis Cardinals. With this account, the imposter posted numerous offensive tweets that confused many people into thinking they actually came from La Russa. Tony La Russa and the Cardinals have filed suit against Twitter in order to get the offending account deactivated and tweets removed.

When the actress Simone Lahbib found herself on Facebook in 2008 it was quite a surprise as she knew she did not have a Facebook account. She was further surprised to find out that some of her friends had been completely taken by the scam, and were interacting with the imposter and even posting photographs to the imposter's page. Ultimately, Ms. Lahbib was able to get the page taken down by Facebook, but the distress it caused and the invasion of privacy remain.

Scope of potential dangers

As bad as those were, other scenarios could be far worse. All corporations and organizations now have to consider what would happen if an imposter posed as an insider such as officer or director, and began making public statements via Facebook, Twitter or some other social network. Such statements could be directed at damaging the reputation of the company, could be designed to influence the movement of the stock market, or could be crafted to attract regulatory or shareholder attention. To some extent, this risk applies to any public figure – public officials (an imposter tweeting as the local sheriff or mayor), professional or collegiate athletes (an imposter tweeting about the coaching staff, the team or alumni), celebrities, consultants (an imposter tweeting about an ongoing audit of a Fortune 25 company), doctors (an imposter tweeting about the prognosis or treatment of an athlete or other public figure).

Online Presences Now Have to Be Managed Like Trademarks

In order to prevent this, corporations and public figures that could be damaged by imposters need to proactively manage the online presence of their individual employees.

First, this should include obtaining official accounts on all major social networking sites for their important insiders in order to prevent imposters from doing so. If these accounts are not used by a particular employee, the account should be “parked” in such a way that in the event an imposter account is created later, it is clear from the parked account that the imposter’s account is just that, an account created by an imposter.

Second, for the most important insiders a watch service should be implemented in the same manner that trademark watch services are employed. This service should monitor the creation of accounts on social networking sites to ensure that no imposter accounts are being created.

George Lewis, a professional engineer, and David St. John-Larkin are attorneys with Merchant & Gould in the firm's Denver office. They may be reached at 303-357-1670.