


## Exploring the security implications of social media

By David Stubbley, CEO, 7 Elements



The use of social media has become a ubiquitous component of the ever more interconnected world in which we now live. The use of social media platforms such as Twitter, Facebook and LinkedIn can provide organisations with new and innovative ways in which to engage with their customers and staff. However this highly dynamic and end-user focused environment can also bring with it a number of security concerns.

## Information Disclosure

The data held within social media can provide an attacker with a wealth of information about the internal workings of your organisation. This information can include detail on roles and responsibilities, projects, commercial relationships and expose information about internal IT systems, including the ability to identify security vulnerabilities.

This information can provide a valuable insight into your organisation and increase the likelihood of a successful social engineering attack or even a direct attack against your systems. For example, during a recent client engagement, we used openly available social media information to map their internal organisational hierarchy to within 86% accuracy and detect vulnerable operating systems and browser software that could have resulted in them becoming an easily identifiable target.

## Reputational Damage

Social media offers the ability for organisations to spread messages in real time to a much wider audience and promotes a two way interactive dialogue between the end-user and the organisation. However, organisations need to understand both the positive and negative impact that social media can have on their brand and manage this channel of communication effectively. This will enable them to avoid potentially damaging stories around poor customer experience, service outages and other issues going unmanaged.

## Malware and Viruses

URL shortening services are now an essential component for social media. This approach is commonly used by malicious parties to spread malware and viruses, as the use of shortened URLs can hide the real destination. 7 Elements recently conducted an analysis of URL shortened links within Twitter, and of the 3,465 links assessed, 520 linked to malicious content such as malware. Clicking on a shortened link would on average take the user to two different sites (via automatic redirections) for each single URL advertised, which could further increase the likelihood of coming into contact with malicious content.

## Bringing it all together

Without doubt, the use of social media provides a new avenue for organisations to exploit, but at the same time introduce fresh and potentially serious threats.

Organisations should confirm that they have the appropriate policies and procedures in place, such as an effective acceptable use policy, training and awareness for social media and a social media handling policy. This will ensure that they are able to explore this opportunity without unduly exposing themselves to new threats and associated risks.