SOCIAL MEDIA PROTECTION

MONITORING | TAKEDOWN

Sales Team
sales@menainfosec.com

Client Portal
portal.menainfosec.com

Corporate Website
www.menainfosec.com

Imposters with malicious intent are turning to social media as a simple method of social engineering for a variety of purposes. They would normally establish trust and gain a large number of followers by regurgitating genuine news and information, before using the profile for a malicious purpose.

Some of the potential uses for a fake social media profile are to:

› Direct customers to a phishing site to gain login information

› Direct customers to a drive by download malware site to infect their machine

› Sell communication or a contact list of a company's customers (followers) to a competitor

› Communicate false information in an attempt to influence the share price of a company, or;

› Simply sell a successful social media profile for a brand back to the legitimate brand owner.

THE COSTS OF SOCIAL MEDIA BRAND ABUSE

Social media brand impersonation could have financial impact on a company, but whatever its uses, it is likely to do serious damage to a brand's reputation. The risks of not acting on social media brand abuse are:

› Financial losses
› Damaged reputation
› Aggravated customers

TAKE CONTROL OF SOCIAL MEDIA

Don't be caught out by a professional social media impersonator. MENAInfoSec provides a comprehensive solution to monitor hundreds of popular global, and localized social media sites for fake social media profiles impersonating the client's brand. Our monitoring and detection will alert the client to a potential social media impersonated profile for confirmation by the client prior to taking down.

HUMAN SECURITY EXPERTS 24

http://portal.menainfosec.com
www.menainfosec.com
sales@menainfosec.com
+968 99882929

MENA InfoSecurity