By Ronan Kavanagh, Global Sales and Marketing, SpamTitan

SpamTitan Technologies recently revealed its annual security predictions for 2013 and today we'd like to share those with you and get your opinion on their importance to your business. These predictions emphasize the impact social networks and mobile applications are having on network security for small and medium sized businesses. 2012 was an eventful year in email and web security as we saw a number of new and more sophisticated vulnerabilities rise, impacting both individuals and businesses. The all encompassing reach of social networking has upped the security stakes for SMBs with social media becoming the core distribution method for malware and attacks becoming more frequent and unfortunately more damaging

1. Ensuring social networking activity in the workplace is responsible and productive will become even more of a crucial issue.

How many survey results or headlines have you noticed in 2012 about our growing addiction to social networking, some people can't stop friending, poking, tagging and posting. Psychologists tell us as human beings we crave connection hence the extent of our addiction, social networking taps into a basic human need. We predict that social networking will become even more ingrained in our everyday lives in 2013, the challenge for business is how to manage this behaviour in the workplace.

Most business managers know a significant number of employees are messaging on Facebook, shopping on Amazon or watching YouTube videos and they're not sure what do about it. Social media risk and subsequent web and network security issues will continue to be a serious concern for businesses in 2013 hence we predict a greater adoption of web protection products in the SMB sector as small and medium sized businesses start managing the risks using appropriate technologies.

2. The bring your own device (BYOD) trend will continue into 2013

The BYOD trend will continue to grow as similar consumer-driven IT initiatives become more widely accepted. The dilemma facing businesses as to how best support these devices will persist in 2013, the main issue being costs and security. We predict that many CTOs having reviewed their organisations experience with BYOD will decide that it's not worth the pain and will look to enterprise and cloud based tools as a better alternative.

We will continue to see severe shortcomings in corporate security policies in relation to supporting devices. Regardless of who owns the device, employees must abide by corporate security policies if they are using the device for business however this requires a policy to be in place which will be a priority for many organisations in 2013. CTOs and IT departments have a lot to consider.

3. Cybercriminals will continue to get better at profiling social media users

With social networking and social commerce continuing to grow so is the level of malware attacks on social networks, these attacks aim to steal payment credentials as well as personal details. The black market value of these credentials is growing as cybercriminals buy and sell this information. Cybercriminals will continue to get better at profiling social media users so that they can monetize this information by gaining access to bank and other accounts.

Spam is still a problem, however we have seen significant changes over the past 2 to 3 years with spam email volumes falling over that period, spam now accounts for about 70% of global email volume, down from approximately 90%. 2012 has seen an increase in awareness amongst users about phishing and social engineering attacks across both email and social networks. Despite this social media will again be the platform of choice for phishing attacks in

2013.

4. Social media will be the platform of choice for phishing attacks in 2013

In 2012 both Twitter and Facebook have been the most successfully used channels to spread phishing attacks, this shift to on-line phishing is a natural response to the growth in the user communities of the main social networking sites. We see this trend continuing in 2013. Attacks via social media can be deployed speedily and cost the cybercriminal little in terms of outlay hence their attractiveness. Organizations need to implement suitable technology controls as well as ensuring employees are awareness of the dangers successful phishing attacks present.

5. As market consolidation continues end user businesses will be uncompromising in considering alternative solutions

We believe "consolidation" will be a keyword in the information security industry in 2013, the market has already seen and will continue to see massive consolidation. The vast number of mergers and acquisitions are reshaping the information security industry. This year we've seen some significant deals including Trustwave buying M86 Security 2012 and Commtouch acquiring Eleven GmbH

Are acquisitions beneficial for end-user businesses? Sometimes consolidation forces end user businesses to make changes in order to address issues that arise as a result of a consolidation. As the market consolidates further in 2013, end-user businesses will benefit if they take the opportunity to scan the market and are uncompromising in evaluating other possible vendors that meet their needs. Businesses will often find that niche companies producing specialist products deliver better products with a certain enthusiasm and attention to the product that they may not have experienced before.

Go SpamTitan

Ronan Kavanagh is responsible for Global Sales and Marketing for the SpamTitan suite of products. Educated in NUI Galway, Ireland, he joined Copperfasten

Technologies in June 2004.

Prior to joining Copperfasten Ronan worked with Eurokom, an Internet Security Services provider, delivering a wide range of solutions to both Government and large blue chip companies in Ireland.

During his time with Eurokom Ronan was responsible for the ongoing sales development of Eurokoms managed email service which culminated in Eurokoms inclusion in the Government VPN, a multi million euro central government led initiative to provide centralized WAN services to all Government Departments.

Prior to EuroKom, Ronan worked with WorldofFruit.com, a company set up by the Fyffe's Group in Dublin to provide an Internet portal for the global fruit industry. The company offered online sales and distribution facilities for the multi-billion dollar global fruit produce industry through the World of Fruit website. Ronan was responsible for developing and managing a European sales team.