**Middle East Facing Most Challenging Year Yet for Online Security**

*Top Tech CEO Issues Stark Warning, Outlines Predictions for 2013’s Most Pressing Issues*

**DUBAI, United Arab Emirates – January 14, 2012**– 2013 will be the most challenging year yet for online safety in the Middle East, according to the CEO of one of the world’s foremost online privacy and security pioneers.

Announcing a series of predictions for 2013, David Gorodyansky, CEO, AnchorFree, highlighted key factors such as looming Apple OS-targeted viral attacks, Android’s growing malware vulnerability, surging identity theft and the declining stature of antivirus software.

“2013 will see a whirlwind of online interaction in the Middle East, from personal dialogue and political debate to enterprise connectivity and enablement,” said Gorodyansky.

“The boundaries between real world existence and online is becoming blurred. Smartphones in hand and tablets at the ready, the region will check in, reach out and connect like never before. ‘Going online’ is no longer something we consciously do – these days, it’s our default state of existence. This year, the Middle East will be subjected to its most sustained, challenging and multifaceted online security challenge yet. Individuals and businesses entering the New Year without adequate protection measures, as well as an awareness of the key issues, are soon going to be found out.”

**Gorodyansky’s 2013 predictions**

**A Flash in the Bucket**

**“**The Flashback Trojan that attacked 400,000 Mac computers in the spring of 2012 was just a preview. Apple devices – desktops, tablets and phones – once thought to be immune to viruses, will be subject to a major viral attack even more deadly than Flashback. Of course, on-device attacks are only one security risk for Apple users; they are also just as vulnerable as PC users to internet privacy and security breaches, including password hacking and identity theft.”

**Android’s on Edge**

**“**It’s no secret that Android users will continue to run the risk of downloading potentially malicious apps, but with so many enterprises using the platform thanks to its worker-friendly OS, 2013 will bear witness to the rise in infection among businesses using the Android OS. An estimated 18 million Android users will encounter mobile malware this year and next, according to [numbers released by Lookout Security](http://www.esecurityplanet.com/mobile-security/lookout-predicts-18-million-android-malware-infections-by-end-of-2013.html). Unless IT departments significantly ramp up their security programs, many of those victims will be corporations in the New Year.”

**Identity Theft on the Rise**

**“**Identity theft is on the rise across the world, and people will have to adapt to safeguard critical personal data. While more than 120 million users have downloaded AnchorFree’s software to protect against identity theft, there are still hundreds of millions more who throw caution to the wind online and leave themselves open to assaults on their identity. 2013 may not be so lucky a year for these folks…”

**Hack Attack**

**“**From Google and LinkedIn to Lockheed Martin and Citibank, major players in the tech, banking, and defense sectors were hacked in 2012. The highly publicized hack of Wired writer Mat Honan was further proof that even the most vigilant consumer is vulnerable to cybercrime. With a hack against PlayStation 3 already on the boards, the world of gaming will be the next target. Both vulnerable and lucrative to hackers, gamers who willingly hand over credit card or PayPal details provide the path of least resistance for greedy hackers, who will test the limits with bolder moves in 2013.”

**Apps Stand Up to Scrutiny**

**“**In a move likely to have global repercussions, the US Federal Trade Commission’s investigation into apps thought to be violating privacy by tracking the behavior of those too young to look out for themselves will set off a push toward more stringent guidelines, greater transparency and streamlined privacy policies. This will impact the darlings of children’s entertainment  – Disney, Cartoon Network, Rovio – and benefit consumers young and old. Consumers beware: government action takes time, so taking our own proactive steps to protect ourselves and our kids is essential.”

**Workplace Censorship**

**“**Increasingly strict corporate censorship and filtering policies will affect the ability of workers to access popular sites such as Facebook, Twitter and YouTube on the job. This problem will present corporations with additional dilemmas as more and more workers choose to bring personal smartphones and tablets to the workplace.”

**The Decline of Antivirus**

**“**Antivirus, a term that’s become synonymous with internet security, will no longer be enough to protect against the growing cache of online threats we face. In the past, antivirus was the gold standard – it ensured the security of our devices, and that was sufficient enough. But once the cloud was introduced, we had to throw that notion out the window. Now, securing online interactions and browsing via a cloud-based security and encryption solution is an essential precaution, and doing so reduces the need for traditional antivirus.”

**Protecting YOU**, **Not Your Device**

**“**A new breed of companies will evolve with a business model of protecting YOU, meaning every interaction you make on your mobile device or computer will be protected.  Until recently, the world thought about protecting computers; in 2012, major security players understood the need to protect mobile devices as well. In 2013, online protection will focus on safeguarding the user across any platform or device.”

**About AnchorFree**

AnchorFree's mission is to provide secure browsing, privacy and freedom to the more than 1.6 billion people around the world who are in need of a secure browsing solution or freedom to access internet content. AnchorFree does this through Hotspot Shield, the world's most popular privacy, security and Web access tool. Hotspot Shield ensures safe, private Web browsing and disrupts censorship of commonly blocked content such as breaking news, social networking and search engines. Hotspot Shield is available for PC, Mac, Apple iOS, and Android platforms at www.AnchorFree.com. AnchorFree is a privately held, venture-backed company based in Mountain View, California

**For more information, visit** [**http://tinyurl.com/8d8tkqt**](http://tinyurl.com/8d8tkqt)

**Media contact**

[anchorfree@wallis-mc.com](mailto:anchorfree@wallis-mc.com)

+971 4 390 1950