

# Advanced 365 reveals top eight technology threats of the future for the financial services sector

Submitted by: Advanced Computer Software Group LTD

Tuesday, 16 June 2015

---

Botnet attacks and self-mutating computer viruses amongst emerging security fears

16 June 2015 - Financial services providers must better prepare for the threat that new technologies pose to their security strategies or risk damaging customer and investor confidence. This is the advice from leading managed service provider, Advanced 365 (Advanced).

Cyber-crime within the financial services industry has reached unprecedented \*levels and currently costs the global economy £266 billion each year. As companies increasingly adapt to emerging technologies, such as digital wallet service Apple Pay and Near Field Communication (NFC), the likelihood of hacks and data security breaches is rising.

Neil Cross, Managing Director of Advanced 365, explains, "The financial services industry must find a balance between embracing innovation to establish a competitive advantage whilst meeting needs for greater compliance and security in order to survive. At present, too many firms are preparing for yesterday's threat instead of updating their strategies to defend against tomorrow's."

Cross outlines below the top eight technology threats that financial services firms will face in the future.

1. Botnet attacks – The Botnet (robots and networks) of Things is a group of computers or internet-connected devices that have been hacked to commit fraud or attack servers. Industry experts estimate that botnet attacks have contributed to the loss of millions of pounds from financial institutions. Mass adoption of the Internet of Things will only exacerbate security challenges as it introduces billions of potential new bots.
2. Self-mutating computer virus – 'Pandoras' are regarded as the next generation of self-mutating computer virus attacks. They are designed to destabilise, confuse and destroy critical electronic infrastructures essential to the financial services industry. From a strategic perspective, they can be used as both offensive and defensive security mechanism.
3. Near Field Communication (NFC) – NFC allows two devices within a short distance of each other to exchange data. It is increasingly being adopted by banks to introduce new products and facilitate mobile payments. Customers are susceptible to aggressive avatar-based attacks which rely on advanced digital creation assembled from stolen aspects of an individual's identity.
4. Payments technology – Mass market adoption of new mobile payments technologies, such as Apple Pay and Google Wallet, is expected to occur by the end of 2016. Hackers are intensifying their efforts as companies and consumers increasingly adopt these new systems and related fraud cases in the United States are already totalling millions of dollars.
5. Biohacking – Biohacking applies to advanced techniques that use science and technology to affect

human performance and could be a target for radical security breaches. Smart implants will be used for identification and authentication of individuals which include the ability to access buildings and activate mobile phones, in addition to making bank transactions to replace smartphone PIN codes.

6. Big data and the cloud – In ten years' time, most of the world's data will move through or be stored in the cloud at some stage. This is expected to result in more sophisticated data security attacks targeting cloud infrastructures, shifting from device-based to cloud-based botnets, hijacking distributed processing power.

7. Mobile – 80% of internet connections could originate from a mobile platform by 2025. Industry experts predict that mobile devices will no longer be used to crack a phone code or steal data from a device itself. Instead they will be targeted by cyber criminals as a catalyst for obtaining additional data resources that can be accessed via the cloud.

8. Bring Your Own Device (BYOD) – Heavily regulated industries are struggling with the risks introduced by allowing employees to bring their own devices. A 2014 survey of financial services respondents by PwC revealed that 44% said employees represented the highest and most likely source of security incidents. This figure is 9% higher compared with the all industries' average.

Cross adds, "Financial Services providers must adapt to the new world and the demands it places on their organisation. Businesses that fail to demonstrate a greater awareness of emerging technological challenges and transform their notion of security could fall prey to damaging breaches."

Advanced 365 has recently commissioned a white paper, 'The future of data security in financial services', which highlights key trends and future technologies to combat cyber- crime. To read the white paper, visit:

<http://www.advancedcomputersoftware.com/collateral/365/register.php?doc=thefutureofdatasecurity.pdf>

-ENDS-

Notes to Editor

\*Statistic taken from a report published by Intel Security Group, Net losses: Estimating the global cost of cybercrime (June 2014).

About Advanced 365

Advanced 365 is a leading provider of IT managed services and business innovation solutions. Working with organisations within the private, public and charity sectors, Advanced 365 aligns technology to its clients' business needs in order to improve their operational efficiencies, help control costs, enhance productivity and enable growth.

Core offerings include:

- Managed services focusing on the delivery of IT services including: outsourcing, cloud computing,

application development and support, and unified communications.

- Business innovations to make legacy systems relevant to today's business environment. Advanced 365 provides a CIO advisory service which supports the deployment of technologies including modernisation, legacy system migration, application development, applications support and data cleansing.

Advanced 365 is a Microsoft Gold Competency Partner and works closely with other industry leading vendors and developers including Redhat, Gamma Telecom, IBM and Oracle.

Advanced 365 is a division of Advanced Computer Software Group Limited, a leading supplier of software and IT services to the health, care and business services sectors. In 2014, the Group won Tech Company of the Year in PwC's UK Tech Awards. Advanced was also ranked in the Deloitte UK Fast 50, which recognises the 50 fastest growing technology companies in the UK and ranked in the top 300 technology companies in Deloitte's EMEA rankings.

<http://www.advancedcomputersoftware.com/365/>

Press contact:

Angela Mycock and Ben Carey, Advanced Computer Group  
pr@advancedcomputersoftware.com T: +44 (0)1625 856513