Kaspersky Lab: avoiding online fraud at all costs

According to Kaspersky Lab's latest report based on Corporate IT Security Risks Survey results - a global survey of more than 5,500 company executives and professionals from 26 countries - 60% of businesses admitted experiencing at least one IT security incident which can lead to or may be related to financial fraud.

©ximagination via 123RF

Direct money loss due to cyber attacks is also a major topic on the business security agenda, with the importance of mitigating the risk of fraud on par with such major issues as malware attacks and data leakage. Online fraud is perceived as complex and hard to prevent even by the banks themselves: they struggle to separate fraudulent actions from legitimate ones and are yet to decide who is responsible for attack mitigation and response.

The Corporate IT Security Risks survey confirms that online financial fraud is one of the most sensitive topics for businesses. Other types of cyber security breaches, even the most dangerous ones such as cyber espionage, may still provide enough time to mitigate risk. However, loss of money affects operations and reputation almost immediately. At the same time, we observed that the perception of online fraud is sometimes far from realistic or as uniform as we would like it to be. Businesses have yet to decide on who has ultimate responsibility for the prevention of such attacks.

The scope of solutions aimed at securing financial transactions of any type is also not well defined: some companies rely on banks, some use third-party solutions in-house or develop their own routines, and some have not yet fully implemented a fraud prevention solution at all.

The main findings for South Africa of the report are:

• 37% of South African businesses carry out financial transactions using Wi-Fi on a mobile device, while 57% on their computers.
• 50% of local businesses feel they need to improve their protection of financial transactions.
• 76% of local companies are looking for a financial services provider with a stronger security reputation.
• Financial organisations themselves are yet to come up with the uniform approach on who is actually responsible for fraudulent actions against their customers. Popular options are banks' IT department, senior management, security department or even police or government.

The evolution of financial cyber attacks

"While the most feared and frequently used method of online fraud attacks remains 'good old' phishing and malware, our experts see financial cyber attacks evolving into sophisticated state-of-the-art campaigns. To ensure reliable protection, security of many other entities has to be taken into account, such as mobile devices, Wi-Fi networks and channels used for money transfers outside of the corporate perimeter. When complexity meets a lack of well-defined protection strategy loss becomes inevitable.

Businesses need to have a clear understanding of the threat, the strategy to prevent it, and the procedure and tools to mitigate it. The role of the security industry is therefore not only to provide new technology designed to prevent online fraud but to share intelligence to help businesses define their strategy and shape the appropriate mitigation and response", commented Ross Hogan, global head of the fraud prevention division at Kaspersky Lab.

Kaspersky Lab's report *Financial Fraud: The Impact on Corporate Spend*, the latest in IT Security Risks Special Report Series is available here.