Romantic Phishing is on the Rise – Kaspersky Lab Suggests How Not to Lose Your Money While Losing Your Heart





Kaspersky Lab experts have detected a sharp increase in phishing activities from criminals offering users various romantic goods on the eve of St. Valentine's Day.

The total number of user attempts to visit fraudulent websites with a romantic theme that were detected and blocked during the first half of February more than doubled compared to the same time in 2018, a reminder that fraudsters are always looking for an excuse to steal users' data and money.

Phishing is one of the most popular and easiest social engineering techniques to exploit online users. It is a type of fraud where criminals use deception to acquire users' credentials – from passwords to credit card numbers, bank account details and other financially important information. Phishing emails and websites usually come disguised as legitimate ones that encourage a recipient, for one reason or another, to urgently enter their personal data. They are often fueled by the news agenda, be it major sport event or thematic holidays. St. Valentine's Day is no exception.

The overall number of user attempts to visit fraudulent websites that were detected and blocked by Kaspersky Lab solutions in the first half of February 2019 – the days leading up to February 14th – dramatically peaked from over two million in 2018 to more than 4.3 million this year. According to statistics, the most affected countries were Brazil (a more than 6.4% share of detections), Portugal (more than 5.8%), and Venezuela (5.5%). They were followed by Greece (5.3%) and Spain (5.1%).

Deeper analysis into the sent emails has shown that fraudsters are particularly exploiting pre-order gift items and performance enhancing drugs as a trap to lure users into sharing their credentials in order to please their loved ones. This again proves the findings of Kaspersky Lab's own survey, indicating that when it comes to love, users tend to lose their vigilance.

"Our research has shown that there is no difference between phishing activities exploiting major sporting events, fake payment bills, or a more romantic pretext. They all just need to drive users' emotions, be it excitement, stress, or love. Thus, almost anything can become an attack tool in the cyber fraudsters' hands. The detected spike reminds us that we should always be cautious when surfing the web even we are just buying flowers for our loved one," – warns Andrey Kostin, Senior Web-Content Analyst at Kaspersky Lab.

Kaspersky Lab advice for staying safe:

– Phishers often exploit emotions – including those connected with relationships and love. Signs that there could be phishers aiming to exploit your romantic expectations include messages that demand immediate action, ask for vast amounts of very personal and seemingly irrelevant information, or which simply sound too good to be true.

– Pay extra attention to emails promising 'one time only' offers or various goods for free. If emails come from people or organizations you don't know, or have suspicious or unusual addresses think

twice before opening. Do not click on links until you are sure that they are legitimate and start with ‘https’, especially when any personal or financial information is asked for.

– Have a separate bank card and account with a limited amount of money, specifically for buying flowers or making a table reservation. This will help to avoid serious financial losses if your bank details are stolen.

– Use a reliable security solution with anti-phishing and secure payment capabilities, such as Kaspersky Security Cloud