Beat: Technology

Fake Facebook sites account for 60% of social network phishing in early 2018

Technology

Jeddah - Saudi Arabia, 06.07.2018, 03:04 Time

USPA NEWS - In the first quarter of 2018, Kaspersky Lab´s anti-phishing technologies prevented more than 3.7 million attempts to visit fraudulent social network pages, of which 60% were fake Facebook pages. The results, according to Kaspersky Lab´s report, “˜Spam and phishing in Q1 2018´, demonstrate that cybercriminals are still doing what they can to get their hands on personal data.
Social network phishing is a form of cybercrime that involves the theft of personal data from a victim´s social network account. The fraudster creates a copy of a social networking website (such as a fake Facebook page), and tries to lure unsuspecting victims to it, forcing them to give up their personal data “ such as their name, password, credit card number, PIN code, and more “ in the process.

At the beginning of the year, Facebook was the most popular social networking brand for fraudsters to abuse, and Facebook pages were frequently faked by cybercriminals to try and steal personal data via phishing attacks. This is part of a long-term trend: in 2017, Facebook became one of the top three targets for phishing overall, at nearly 8%, followed by Microsoft Corporation (6%) and PayPal (5%). In Q1 2018, Facebook also led the social network phishing category, followed by VK “ a Russian online social networking service - and LinkedIn. The reason for this is likely to be the worldwide 2.13 billion active monthly Facebook users, including those who log in to unknown apps using their Facebook credentials, thereby granting access to their accounts. This makes unwary Facebook users a profitable target for cybercriminal phishing attacks.

This all reinforces the fact that personal data is valuable in the world of information technology ““both for legitimate organizations and attackers. Cybercriminals are constantly searching for new methods to hit users, so it´s important to be aware of fraudster techniques to avoid becoming the next target. For example, the latest trend is spam emails related to GDPR (Europe´s General Data Protection Regulation). Examples include offers of paid webinars to clarify the new legislation, or invitations to install special software that will provide access to online resources to ensure compliance with the new rules.

“The continuous increase in phishing attacks - targeting both social networks and financial organizations - shows us that users need to pay more serious attention to their online activities. Despite the recent global scandals, people continue to click on unsafe links and allow unknown apps access to their personal data. Due to this lack of user vigilance, the data on a huge number of accounts gets lost or extorted from users. This can then lead to destructive attacks and a constant flow of money for the cybercriminals,“ said Nadezhda Demidova, lead web content analyst at Kaspersky Lab.

Kaspersky Lab experts advise users to take the following measures to protect themselves from phishing:
“¢ Always check the link address and the sender´s email before clicking anything “ even better, don´t click the link, but type it into your browser´s address line instead.
“¢ Before clicking any link, check if the link address shown, is the same as the actual hyperlink (the real address the link will take you to) “ this can be checked by hovering your mouse over the link.
“¢ Only use a secure connection, especially when you visit sensitive websites. As a minimum precaution, do not use unknown or public Wi-Fi without a password protection. For maximum protection, use VPN solutions that encrypt your traffic. And remember: if you are using an insecure connection, cybercriminals can invisibly redirect you to phishing pages.
“¢ Check the HTTPS connection and domain name when you open a webpage. This is especially important when you are using websites which contain sensitive data “ such as sites for online banking, online shops, email, social media sites etc.

“¢ Never share your sensitive data, such as logins and passwords, bank card data etc., with a third party. Official companies will never ask for data like this via email.
“¢ Use a reliable security solution with behavior-based anti-phishing technologies, such as Kaspersky Total Security, to detect and block spam and phishing attacks.

Other key findings in the report include:
Phishing:
“¢ The main targets of phishing attacks have remained the same since the end of last year. They are primarily global Internet portals and the financial sector, including banks, payment services and online stores.
“¢ About $35,000 USD was stolen through one phishing site that appeared to offer the opportunity to invest in the rumored Telegram ICO. Approximately $84,000 USD was stolen following a single phishing email mailshot related to the launch of “¯The Bee Token´ ICO.
“¢ Financial phishing continues to account for almost half of all phishing attacks (43.9%), which is 4.4% more compared to the end of last year. Attacks against banks, e-shops, and payment systems remain the top three, demonstrating cybercriminals´ desire to access users´ money.
“¢ Brazil was the country with the largest share of users attacked by phishers in the first quarter of 2018 (19%). It was followed by Argentina (13%), Venezuela (13%), Albania (13%), and Bolivia (12%).

Spam:
“¢ In the first quarter of 2018, the amount of spam peaked in January (55%). The average share of spam in the world´s email traffic was 52%, which is 4.6% lower than the average figure of the last quarter of 2017.
“¢ Vietnam became the most popular source of spam, overtaking the U.S. and China. Others in the top 10 included India, Germany, France, Brazil, Russia, Spain, and the Islamic Republic of Iran.
“¢ The country most targeted by malicious mailshots was Germany. Russia came second, followed by United Kingdom, Italy, and the UAE.

Article online:
https://www.uspa24.com/bericht-13728/fake-facebook-sites-account-for-60-of-social-network-phishing-in-early-2018.html

Editorial office and responsibility:
V.i.S.d.P. & Sect. 6 MDStV (German Interstate Media Services Agreement): Zayad Alshaikhli

Editorial program service of General News Agency:
United Press Association, Inc.
3651 Lindell Road, Suite D168
Las Vegas, NV 89103, USA
(702) 943.0321 Local
(702) 943.0233 Facsimile
info@unitedpressassociation.org
info@gna24.com
www.gna24.com