Data for Nothing: Fraudsters Use Fake Gift Cards to Lure Consumers into Handing Over Personal Data

Kaspersky Lab experts have discovered the distribution of an unusual fraudulent scheme that tricks users into parting with their time and their data, for no return. By creating fake websites for the free generation of gift cards, cybercriminals are able to "sell" users' data to third party partner sites, to which they redirect victims.

While industry and law enforcement agencies from around the world are busy fighting against cybercrime, criminals themselves are constantly looking for new ways of earning money – other than just malware. Offering something valuable free of charge is always an enticing piece of marketing, and criminals can take advantage of this. Websites that offer customers the option of freely generating gift cards for well-known companies – like iTunes, Google Play, Amazon, or Steam – are nothing new. For example, legitimate apps like Tokenfire and Swagbucks buy card codes from vendors, to then give them to clients as a reward for certain activities. Criminals have apparently recognized the popularity of such websites and have decided to deceive users using a simple algorithm.

When on the fake site, the user is asked to select the gift card he/she wants in order to receive the code. After that, the fraudulent mechanism is set in motion. To get the generated code, however, the user needs to prove that he/she is not a robot. To do this, the user has to follow the suggested link and complete various tasks, the number and type of which are determined by the partner network to which the user is redirected. For example, he/she may be asked to fill in a form, leave a phone number or email address, subscribe to a paid SMS-message, install adware, and so on.

The result is predictable: either victims get tired of doing endless tasks, or they finally get the useless code. The earnings for criminals range from a few cents per every click on a desired link, to several dozen dollars for filling in a form or subscribing to paid services. Thus, the criminals make a profit virtually for nothing, getting paid from the user's actions on the websites of third-party partners, who, for their part, also benefit by getting access to personal data which can be used for private purposes.

"The success of these new fraud schemes is based on criminals exploiting the drive of users to get something for free. However, at best they will spend hours of personal time doing worthless tasks, and at worst – lose money without receiving anything in return. So, if you want to get your hands on a free gift card, try to earn it on legal and trustworthy sites," – said Lyubov Nikolenko, web content analyst, Kaspersky Lab.

To avoid falling for cybercriminals' fraudulent schemes and losing personal data, Kaspersky Lab researchers suggest that users follow a few simple rules:

– Remember that there is no such thing as a free lunch and always treat offers that seem too tempting to be true with skepticism.
– 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.
– Do not spread questionable links among your friends.
– Check with the company if it really is giving out gift codes, and whether the site is its official partner. To do this, contact the official support service by reaching out on the official website of the company.
– Use a reliable security solution with behavior-based anti-phishing technologies to detect and block spam and phishing attacks, such as Kaspersky Total Security, which blocks fake gift card sites.

To learn more about the mechanism of gift cards generator fraud schemes, read our blogpost on Securelist.com.