Public Service Announcement

FEDERAL BUREAU OF INVESTIGATION

April 28, 2014

PHISHING ATTACKS ON TELECOMMUNICATION CUSTOMERS RESULTING IN ACCOUNT TAKEOVERS CONTINUE

Phishing attacks targeting various telecommunication companies' customers continue. Individuals receive automated telephone calls that claim to be from the victim's telecommunication carrier. The IC3 released an advisory about this scam in May 2013. Since then, the attacks have increased and recently, victims have reported receiving SMS texts with a similar phishing message encouraging them to go to web sites to claim their reward. Victims are directed to a phishing site to receive a credit, discount or prize ranging from $100 to $2,500. The monetary amounts being offered are increasing to make the scam more enticing. A fraudulent web site example would be www.My(insertphone company name)900.com. Other fraudulent web sites may contain words such as, MyBonus, ILove, ILike, Reward, Promo, or similar words, along with a telephone company's name.

The phishing site is a replica of one of the telecommunication carrier's sites and requests the victim's log-in credentials and the last four digits of their Social Security number. Once access is gained, the subject makes changes to the customer's account and may place orders for mobile phones.

The IC3 urges the public to be cautious of unsolicited telephone calls, e-mails and text messages, especially those promising some type of compensation for supplying account information. If you receive such an offer, verify it with the business associated with your account before supplying any information. Use the phone numbers that appear on your account statement to contact the business.

If you have fallen victim to this scam, immediately notify your telecommunication carrier and file a complaint with the IC3, https://www.ic3.gov.