INTERNET CRIME COMPLAINT CENTER'S (IC3)
SCAM ALERTS
JULY 18, 2013

This report, which is based upon information from law enforcement and complaints submitted to the IC3, details recent cyber crime trends and new twists to previously-existing cyber scams.

SPEAR-PHISHING ATTACK TARGETING THE PETROLEUM INDUSTRY

The following scheme has been reported and has targeted at least five petroleum companies. The perpetrators registered domain names closely resembling the domain names of the victim companies that were slightly misspelled. The perpetrators then sent targeted e-mails to individuals who were identified as having the ability to initiate a wire transfer within the company. The e-mails appeared legitimate, were sent to the correct person at the company, and had contact information for the requester (usually someone in the company with the authority to request a transfer). The victim company contacted the requestor at the number provided in the e-mail (instead of using information contained in an internal directory) and provided him/her with the information and documents required to initiate the transfer. The perpetrator completed the form and initiated the wire transfer.

A variation of this scheme involved perpetrators creating a domain name similar in spelling to a victim company’s sub-contractor domain. The perpetrator then e-mailed the individual in charge of initiating payments to that sub-contractor and informed him/her due to various reasons, the sub-contractor needed to change the account information for all payments initiated to the sub-contractor. The e-mail contained the name of a legitimate person at the sub-contractor, but provided a number belonging to the perpetrator. The company called the perpetrator to verify the account change and changed the payment information. The company was then contacted by its sub-contractor about delinquent payments.

Most of these schemes are occurring in the aforementioned industry, but based on the success of these schemes, the perpetrators may expand their target group.

Because of the increased number of spear-phishing attacks reported recently to the IC3, on June 25, 2013, the IC3 released a PSA educating consumers on spear-phishing. The PSA is available at https://www.ic3.gov/media/2013/130625.aspx.

PREPAID RISK

The IC3 received information pertaining to the below scam from an eCommerce Industry partner.

Gift Card tampering and balance theft continues to be an evolving fraud concern, and for many merchants the activity occurs under the radar. Gift cards, as a tender, allow fraudsters to be more anonymous, offer multiple outlets to turn them into cash, and can be used as a way to launder money.

Gift cards come in multiple forms: physical, e-mail, and mobile, and can be purchased in stores and online; the multiple forms allow for multiple points of manipulation for fraudsters to exploit.

Below are some common gift card fraud methods:

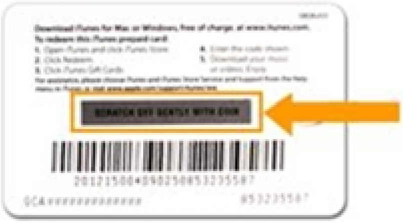
Gift Card Tampering
Method #1

- A fraudster steals gift cards from a store.

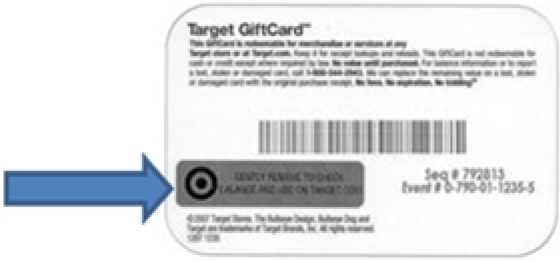
- A fraudster records the gift card’s number and access code.
- A fraudster places the gift cards back on the display in the store.
- Then, the legitimate customer buys the gift card.
  - The fraudster repeatedly checks the balance on the stolen gift card number
  - Once the fraudster is alerted to the available balance, the fraudster spends the balance online.

Method #2

- A fraudster obtains barcode information for the merchant’s gift card.
- A fraudster creates duplicate UPC stickers using UPC-generator software. (Duplicate sticker matches the fraudster’s original gift card.)
- The fraudster places stickers on unissued gift cards in the store (Thieves have become adept at getting to the access code/PIN and replacing it without damaging the card’s/packaging security features.)
- A legitimate customer buys the gift card with the sticker – and the balance goes on the fraudster’s original gift card.
  - A fraudster repeatedly checks the balance using the access Code/PIN.
  - Once the fraudster is alerted to the available balance, the fraudster spends the balance online.



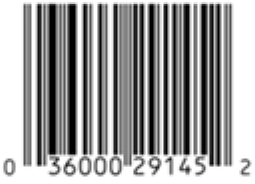
An example of a music gift card



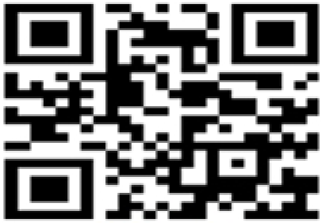
An example of a Target gift card

Method #3

- A fraudster takes a picture of a gift card’s barcode in the store
- A fraudster uses free online program to transform a linear one-dimensional barcode to a two-dimensional barcode.



1D Barcode



2D Barcode

- The fraudster combines a screenshot of a merchant’s mobile app and the two-dimensional barcode to create a “fake” mobile gift card to use in the store.
- A legitimate customer buys the tampered gift card and – the balance goes to the “Master” gift card the fraudster created by cloning the barcode and making stickers to put on other gift cards, then putting the gift cards back on the display. Each time one of those cards is purchased, the balance is not going to the purchased gift card. Rather, it is going to the sticker – that has the same information of the “Master” gift card.
  - The fraudster repeatedly checks the card’s balance on the merchant’s website or contacts the merchant’s Interactive Voice Response (IVR), the computerized voice that tells callers what numbers to push based on the service needed.
  - Once the fraudster is alerted to the loaded balance, the fraudster redeems the card.

Merchandise Theft/Return Fraud

- A fraudster steals merchandise from the store.
- A fraudster takes the merchandise to the customer service counter to “return” it.
    - A fraudster requests a “No receipt return.”
    - A driver’s license is scanned; (it can be counterfeit.)
- A fraudster receives a gift card for store credit
    - With this scheme, the fraudsters who steal are like mules in a money- laundering scheme (because there are multiple people doing multiple thefts/returns.)
    - Then, fraudsters sell to resellers on classified advertisement websites
    - Resellers sell the cards to secondary markets (such as check cashing stores) for cash or trade for drugs
    - Gift cards can be used to purchase other cards in an attempt to “launder” them.

Social Engineering

- A gift card owner posts the card for sale online (via a classified advertisement website.)
- The fraudster calls the gift card owner to “buy” it.
- The fraudster states he/she wants to verify the balance and requests the seller make a three-way call (fraudster, gift card owner, merchant’s IVR)
- The seller calls the gift card redemption number and enters the card’s number and access code to verify its balance.
    - The fraudster uses software to obtain the gift card and access code numbers.
    - The fraudster spends the card’s balance online

ADWARE VIRUS

The IC3 would like to bring attention to a widely distributed adware virus variant named Chitka. Although this virus is a few months old, the IC3 recently received information about how Chitka operates. The virus is designed to place banners onto infected systems to generate revenue based on clicks. The variant changes browser settings, registry keys, and edits the host file in Windows. This variant has also been found to act as a download for additional malware, and forwards specific credentials and cookies retrieved during the users web browsing.