CONTENT ARCHIVES HACKING

CONTENT ARCHIVES JOB BOARD

2015 2014 PHISHING

CAREERS

2013 2012

2011 2010

CERTIFICATIONS

FORENSICS

SECURE CODING

PENETRATION TESTING

GENERAL SECURITY

CLOUD COMPUTING

INTERVIEWS

VIRTUALIZATION SECURITY

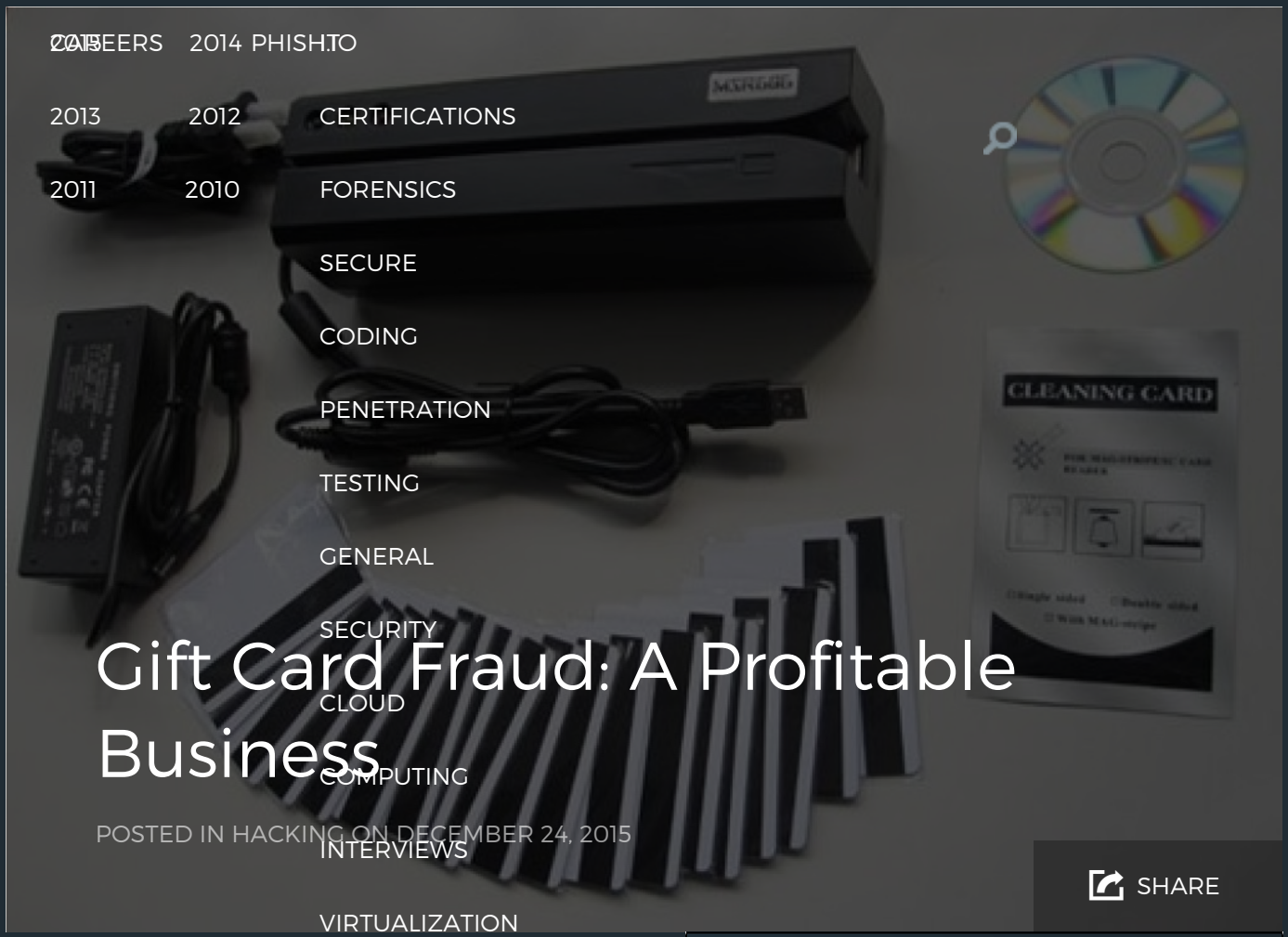
WIRELESS SECURITY

SCADA

REVERSE ENGINEERING

DATA RECOVERY

EXPLOIT DEVELOPMENT



Gift Card Fraud: A Profitable Business

POSTED IN HACKING ON DECEMBER 24, 2015

Gift cards are a very pleasant gift, especially during the holiday season, but they also can represent a good opportunity for crooks.

When dealing with gift card frauds it is possible to find a wide range of fraudulent schemes, fraudsters could exploit merchandise returns, clone, or steal the card, or hack the merchant site by exploiting a security flaw.

Gift card frauds are considered minor crimes due to the small amount of money involved in any transaction, so this kind of crime are rarely prosecuted. Another important factor related credit card frauds is the possibility to arrange a criminal activity without specific skills neither specific tools

Gift card frauds are very common and often not disclosed, but they are rarely disclosed because usually customer personally identifiable information (PII) is not compromised. A few months ago, Starbucks suffered two incidents that involved gift cards. In one case, a security researcher discovered a race condition in the gift card value-transfer protocol that could be exploited to allow attackers to transfer card balances between cards without using the credit of the card.

In the second incident, attackers exploited the auto-load feature on the gist cards that allowed fraudsters to quickly drain attached bank accounts.

As usually happens crooks relies on users' bad habits, like the sharing of the same login credentials over multiple websites and web services.

Crooks use to harvest user login credentials with malware-based attacks, through phishing campaigns, or buying them in the various black markers present tin the underground.

Once cyber criminals collect login credentials they try to use them over multiple websites.

Most common schemes of gift card frauds that could be grouped in three categories:

- Hacking accounts:

- Stealing number and gift card cloning
- Acquiring lot of cards
- Hacking gift cards
- Return of merchandize

Hacking Accounts

The hacking of gift card accounts to steal the associated amount of money is quite common in the criminal underground, this kind of attack could cause greater losses in the case victims have turned on the auto-load feature.

Gift cards are excellent to cash out money from illegal activities, typically they are used to convert the value of money associated in another commodity easy to monetize, such as credit card rewards programs, travel or hotel points.

A cybercriminal obtains the login credentials to a person's credit card reward program (i.e. through phishing activities, malware based attacks discovering a set of compromised credentials reused by the victim on numerous websites) can get an e-gift card number to spend immediately. In this way the crooks rapidly convert the money, the fraudster uses the gift card number immediately in online and in-stores.

At this point, they can use a service that converts gift cards into cash, such as cardcash.com or cardhub.com, these services usually endure a conversion rate of 60% of the face value of the gift cards. In the US it is also possible to find in many malls physical kiosks that offer the same service.

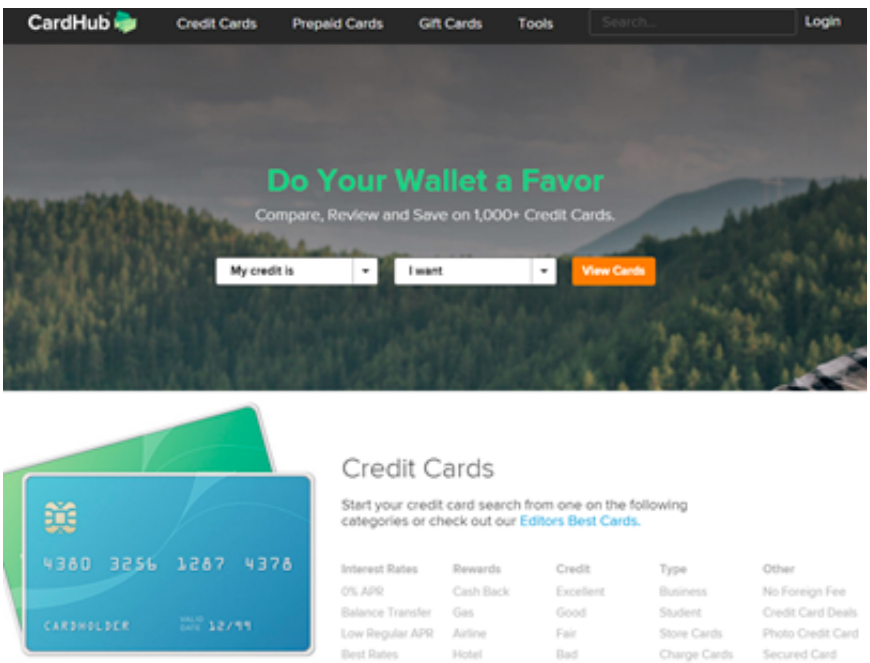


Figure 1 – Card Hub Service

By exploiting this process, the fraudster can convert a point or rewards on a hacked account into real cash.

Gift card cloning and card thefts

Another common gift card fraud relies on stolen numbers off physical gift cards. Gift cards have a number that is printed on the card that could be used for manual key entry, the same number is also encoded on a magnetic stripe on the back of the card, exactly like a credit card.

The level of security implemented to protect information is very poor, the mag stripe store data in plain text and it is very easy to read its content with a common mag stripe reader.

In some cases, gift cards are protected by a PIN number covered with a coating. Similar to a lottery ticket, the coating needs to be scratched off, but also in this case this supplementary level of protection could be easily bypassed, a fraudster could remove the coating, get the pin, print a new coating on the gift card using a specific printer or replace it with a new sticker easily purchased from Internet.

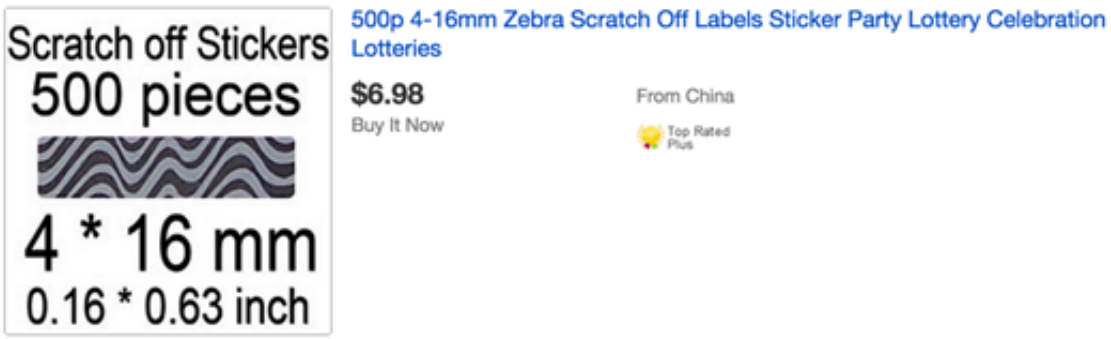


Figure 2 – Scratch-off stickers for sale on EBay

Another factor which favors this type of fraud, is that many merchants don't require users to provide the PIN.

Magnetic Credit Stripe readers could be bought on EBay or Alibaba for a few dozen dollars meanwhile a coating printer have a ranging from a few hundred dollars up to several thousand dollars.

Figure 3 – Mag stripe reader

Thefts of gift cards at its stores are very frequent, in this case the fraud is riskier because fraudsters have to steal the gift card from the store. Typically Gift cards are not usable until they are activated at the cash register, so fraudsters steal the cards, clone them with a mag stripe reader, then return the gift cards back to the store waiting for their activation.

The fraudsters will repeatedly check balances on the merchant's website and wait until the cards in their possession are activated by a legitimate purchase. Once a gift card is activated, they can transfer balances to another card or converting into cash the amount of money associated.

Clearly the exposure of the fraudsters is greater, but the support of insiders could make such kind of fraud very easy to carry on.

Another fraud scheme consists in the use of malware to compromise a POS system in order to grab gift card numbers.

In this case, poorly configured PoS system or their promiscuous use made by store operators could open the door to hackers that can hack them and steal the precious commodity.

ACQUIRING NUMBERS IN BULK

Another opportunity for crooks is represented by the criminal underground where it is possible to buy lot of gift cards. This method is much more rewarding, but requests a significant effort for the execution of the fraud.

The gift card number can be harvested in a multitude of methods, including POS hacking, phishing campaign, hacking database of the merchant, social engineering, physical theft and accidental disclosure.

Hacking Gift Cards

To better understand how it is possible to hack gift cards, I desire to share with you an interesting analysis conducted by the expert Will Caput in collaboration with the hacker group dc530.org that starting from a bunch of card have explained how to use them.

Caput and his colleagues have illustrated how to exploit weaknesses with gift cards, balance checking, and how hackers can enumerate gift cards even without knowing the card holder. It is important to explain that the technique can be applied to any gift card that not use a CAPTCHA or a pin, for any kind of commercial activity they are intended (i.e. Retailer stores, shops, restaurants)

The team analyzed a lot of credit cards used by a prominent restaurant, the cards were not purchased, so they were not loaded or activated, this implies that they come with no balance.

Figure 4 – Gift cards used in the test

The experts started looking for the generation sequence of the card numbers by analyzing the number reported on the cards they discovered the pattern.

The above card reported the following numbers 6088 5124 5565 1064, 6088 5124 5566 2489, 6088 5124 5567 1652, 6088 5124 5568 7415 6088 5124 5570 6523, 6088 5124 5572 1163.

"Looking at the numbers above, you can determine the possible valid numbers by recognizing the pattern. The cards all have the same numbers for the first 10 digits. The 11th and 12th digits are counting up to 100 (and if they continue this

pattern, once they hit 100 the 10th digit will change to the next number and the 11th and 12th digits will start again at 00). The cards have apparently random digits in the 13th – 16th positions." states Caput.

The number of requests necessary to find a valid card is so equal to 10^4 = 10,000 because 4 are the digit used in the generation process.

The hackers operated with a stock of gift card starting from a specific number so they restricted the space of analysis to the numbers related to earlier cards in the stack that were most likely sold to a customer.

Once the attackers discover the pattern they could use the online card balance checker, in the case of the restaurant by visiting the restaurant online and look for "check gift card balance" on it.

In order to analyze every single request, they sued the Burp Proxy tool.

Below the request to the card balance checker that was intercepted for one of the gift cards:

```
POST /Payment/GetGiftCardBalance HTTP/1.1
Host: order.xxxxxxx.com
User-Agent: Mozilla/5.0(iPad; U; CPU iPhone OS 3_2 like Mac OS X; en-us)
AppleWebKit/531.21.10 (KHTML, like Gecko) Version/4.0.4 Mobile/7B314 Safari/531.21.10
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache

{"giftCardNumber":"6088 5124 5570 6523"}
```

Figure 5: HTTP Request

In the following case the gift card has no balance.

```
{"ErrorMessage":"Error with Giftcard GetBalance (6088512455706523) FD Status: OK – Txn Status: 09","ErrorMessageExtended":"","FriendlyErrorMessage":"","InfoMessage": null,"Status":3,"StatusCode":0,"Card": {"AvailableBalance":0,"CardNumber":"XXXXXXXXXXXX6523","History":[]}}
```

Figure 6: HTTP Response

Then the hacker tried to discover the response for invalid or inactive cards by try entering a random card number.

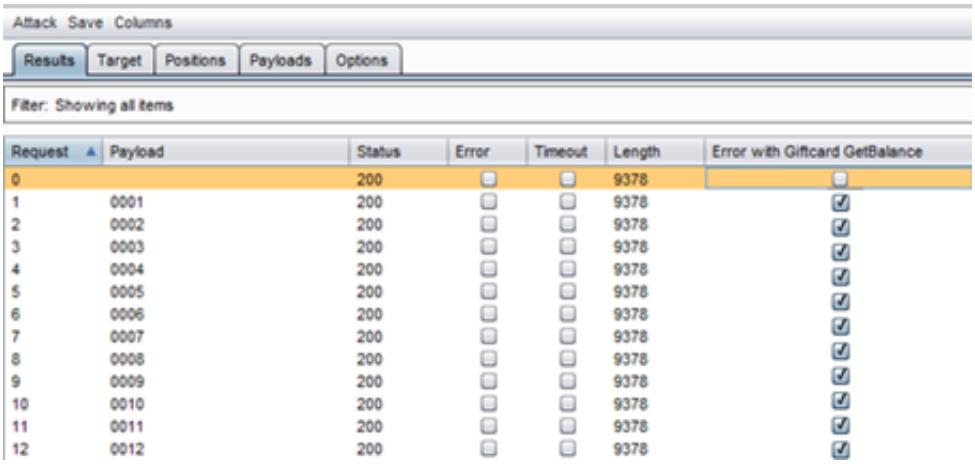
```
POST /Payment/GetGiftCardBalance HTTP/1.1
Host: order.xxxxxxxxx.com
User-Agent: Mozilla/5.0(iPad; U; CPU iPhone OS 3_2 like Mac OS X; en-us)
AppleWebKit/531.21.10 (KHTML, like Gecko) Version/4.0.4 Mobile/7B314 Safari/531.21.10
Accept: application/json, text/javascript, */*; q=0.01
Accept-Language: en-US,en;q=0.5
Accept-Encoding: gzip, deflate
Connection: keep-alive
Pragma: no-cache
Cache-Control: no-cache
```

{“giftCardNumber”:”6088 5124 5570 2222“}

Figure 7 – HTTP Request

The hacker tried to figure out different responses depending on the card status (i.e. invalid or inexistence, and account balance equal to zero).

At this point the last step is trying possible combinations for gift card numbers with the Burp Intruder Tool.



Request	Payload	Status	Error	Timeout	Length	Error with Giftcard GetBalance
0		200	☐	☐	9378	☐
1	0001	200	☐	☐	9378	☑
2	0002	200	☐	☐	9378	☑
3	0003	200	☐	☐	9378	☑
4	0004	200	☐	☐	9378	☑
5	0005	200	☐	☐	9378	☑
6	0006	200	☐	☐	9378	☑
7	0007	200	☐	☐	9378	☑
8	0008	200	☐	☐	9378	☑
9	0009	200	☐	☐	9378	☑
10	0010	200	☐	☐	9378	☑
11	0011	200	☐	☐	9378	☑
12	0012	200	☐	☐	9378	☑

Figure 8 – Burp Tool invalid gift card numbers

In some cases, restaurants allow users to use the gift cards by knowing only the number even without the card they were printed on, but there are also a number of exception.

The attacker need to clone the gift card by using a magnetic strip writer like the one used by Caput and his collaborators.

Figure 9 – Magnetic strip writer

The attacker needs to take an empty card and write the data of a legitimate one on it. Writing is very easy, the attacker has to prepare the strings to write on the tracks present on the magnetic stripe and as reported in the following image.

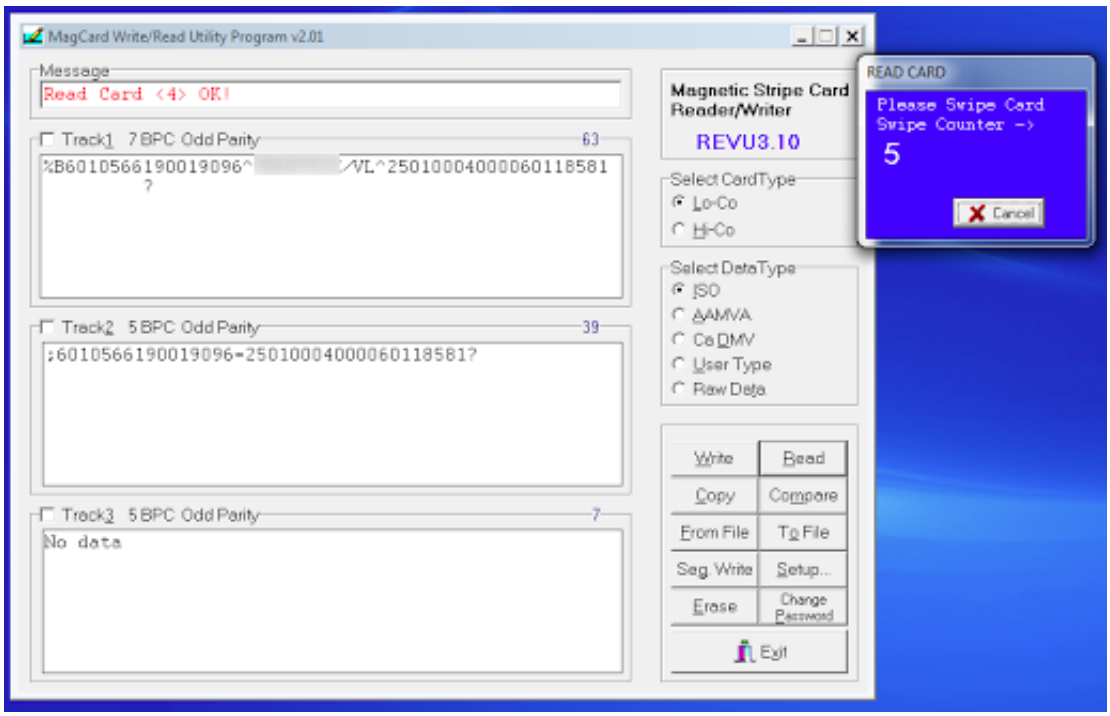


Figure 10 – Magnetic strip writer

ETHICAL HACKING TRAINING – RESOURCES (INFOSEC)

The return merchandise fraud scheme

Every day, dozens of gift cards from top retailers are offered for sale online, some of these are legitimate gift cards sold through third-party sites that resell used or unwanted cards, but a good portion result of illegal activities.

Some discounted gift cards are in fact the product of merchandise return fraud.

As explained by the security expert Brian Krebs, this kind of scam mainly impacts retailers that issue gift cards when clients return merchandise at a store without presenting a receipt.

Brian Krebs reported the case of one of his readers, who was aware that crooks steal merchandise from a physical store in the retail chain and return the

merchandise to another store of the same chain without a receipt and then offer for sale the gift cards to websites like raise.com and cardpool.com at a discounted price.

Many stores for returns more than 60 days after the purchase, or if the receipt is unavailable, offer the value of the goods returned will be refunded to a merchandise card.

The Kreb's reader confirmed she was not aware that the card was a merchandise return card, a fact that was printed on the front of the card she received.

Krebs searching for available gift cards for sale online discovered that the cards are routinely sold for at least 25 percent off their value.

"Clothier H&M's cards average about 30 percent off."

The popular investigator made other interesting discoveries analyzing discounts for industries that haven't customers return (i.e. fuel stations, restaurants). The value of the cards from merchants that don't take customer returns allows discounts that tends to be much lower, between 3 and 15 percent (i.e. gift cards from Starbucks and Chevron).

Twenty-five percent off is really high and experts invite customers to be wary of such offers.

"Normally, it is around 5 percent to 15 percent." said Damon McCoy, an assistant professor at New York University and an expert on fraud involving stored value cards.

This means we are facing with a consolidated illegal activity, that according to the National Retail Foundation will cost U.S. retailers nearly $11 billion this year.

"Investigators say the crimes very often are tied to identity theft rings and drug addicts. Last month, authorities in Michigan convicted a 46-year-old father of four for running a large-scale fencing operation that used teams of prostitutes, heroin users, parolees and panhandlers to steal high-priced items from local Home Depot stores and then return the goods to a different Home Depot location in exchange for store debit cards." wrote Krebs in a blog post.

Clearly gift cards are also a privileged cash out method for criminals specialized in the sale of stolen credit cards. Crooks used stolen card data to buy gift cards from a range of retailers and offer them for sale online at 20-30 percent

discounts.

Conclusion

The gift cards are an easy target for cyber criminals, the enumeration of the card numbers is very easy and the absence of authentication systems makes easy the cloning of the cards.

The Solutionary company provided a few suggestions to protect gift cards, such as:

- Implement a CAPTCHA on your gift card balance checking site
- Use gift cards that implement authentication mechanisms using an additional PIN, and never store the gift card PINs with the gift card numbers.
- It is important to protect gift cards when they are at the store, avoiding theft, keep them in the safe and do not expose them in area publicly accessible.
- It is a good practice to limit online balance look-ups to several per hour, maximum.

On the customer side, it is important to avoid buying gift cards from untrusted sources.

Gift card fraud is a lucrative business for criminal organizations that cause every year significant loss to the retailers and potential damages to the company reputation.

Let me close with a list of suggestions to avoid gift card scams:

- Don’t buy gift cards from online auction sites, buy gift cards directly from the store issuing the gift card or from a secure retailer’s website.
- Don’t buy gift cards off of publicly displayed racks in retail stores.
- Ask the store cashier to scan the gift card in front of you, in this way you can buy only valid card. Check also that the balance is exactly the one you charged it with.
- Carefully examine both the front and back of a gift card before you buy it. Be aware of gift card that could have been tampered with.
- Register the gift card at the store’s website if the store allows it, this will allow to early discover any misuse.

References

http://www.tripwire.com/state-of-security/risk-based-security-for-executives/risk-management/gift-card-fraud-how-its-committed-and-why-its-so-lucrative/

http://www.scambusters.org/giftcard.html

http://securityaffairs.co/wordpress/42778/cyber-crime/gift-cards-and-return-fraud.html

https://www.solutionary.com/resource-center/blog/2015/12/hacking-gift-cards/

AUTHOR

Pierluigi Paganini

Pierluigi Paganini is Chief Information Security Officer at Bit4Id, firm leader in identity management, member of the ENISA (European Union Agency for Network and Information Security)Treat Landscape Stakeholder Group, he is also a Security Evangelist, Security Analyst and Freelance Writer. Editor-in-Chief at Cyber Defense magazine, Pierluigi is a cyber security expert with over 20 years experience in the field, he is Certified Ethical Hacker at EC Council in London. The passion for writing and a strong belief that security is founded on sharing and awareness led Pierluigi to create the blog "Security Affairs," recently named a Top National Security Resource for US. Pierluigi is a member of the The Hacker News team and he is a writer for some major publications in the field such as Cyber War Zone, ICTTF, Infosec Island, Infosec Institute, The Hacker News magazine and for many other security magazines. He is the author of the books The Deep Dark Web and Digital Virtual Currency and Bitcoin.

FREE PRACTICE EXAMS

- CCNA Practice Exam
- Network + Practice Exam
- PMP Practice Exam
- Security+ Practice Exam
- CEH Practice Exam
- CISSP Practice Exam

EDITORS CHOICE

- Gift Card Fraud: A Profitable Business
- Malware Researcher's Handbook (Demystifying PE File Part 2)
- Deep Packet Inspection in Cloud Containers

RELATED BOOT CAMPS

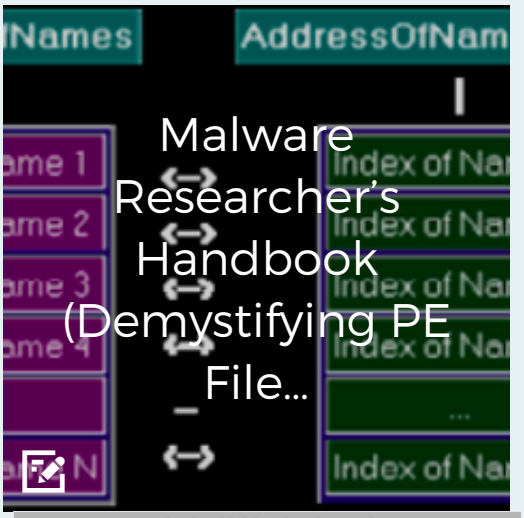
- Information Security
- Security Awareness
- CCNA
- PMP
- Microsoft
- Incident Response
- Information Assurance
- 8570

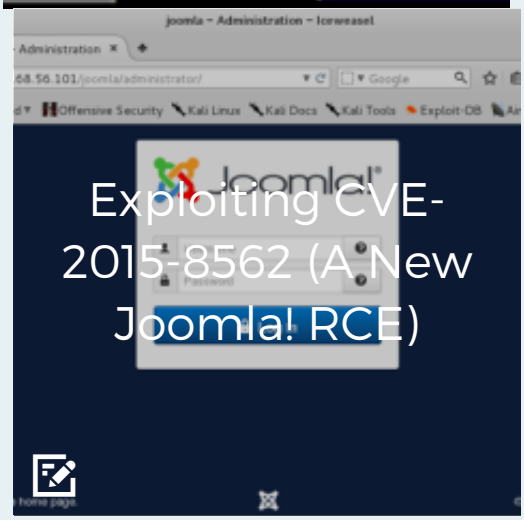
MORE POSTS BY AUTHOR

Why Throwing Away Your Old Boarding Pass is so Risky

Will IoT Security Awareness Protect Me From My Toaster?

ISIL, Terrorism and Technology: A Dangerous Mix





About InfoSec

InfoSec Institute is the best source for high quality information security training. We have been training Information Security and IT Professionals since 1998 with a diverse lineup of relevant training courses. In the past 16 years, over 50,000 individuals have trusted InfoSec Institute for their professional development needs!

Connect with us

Stay up to date with InfoSec Institute and Intense School - at info@infosecinstitute.com

Join our newsletter

Get the latest news, updates & offers straight to your inbox.