Online Payment Security

Uy Quang Nguyen
Kandidatnummer 420
Tema 124
uyqn@student.matnat.uio.no

Contents

Abstract

In this research topic, I will investigate the security and security measures of Online Payment Security, and the potential threats when paying online, whether it is by credit card, or through third parties like PayPal. I will also investigate how safe we really are, when we do online payments with the different methods.

1 Introduction, background and motivation

Electronic commerce, known as E-Commerce or e-Commerce is trading in products or services, and usually involves the use of a computer network, the internet, and digitally stored value systems. Electronic commerce draws on technologies such as mobile commerce, electronic funds transfer, and supply chain management[1]. Online payment goes under e-Commerce, and it is the act of exchanging money electronically.

When you send a payment over the internet, you are doing an online payment. The valuta withdrawal is done from a credit card, checking account or other third party clearing houses such as PayPal. Over the years, credit cards have become one of the most common forms of payment for online transactions.

The reason why I choose this topic for my research paper is because I've always had an interest in what kind of threats we're susceptible to when we are online. I myself have been a victim of key-loggers, spoofing and frauds. Thus, this had lead me to investigate and research how safe we really are when doing acts related to e-Commerce, and how to protect ourselves. I also believe that this assignment would be useful for everyone doing Online Payments, because it'll make you aware of the risks of it.

1.1 Introdu

Online payments are very convenient. With just a click of a button, you can make a payment to the other side of the world. But it doesn't come without issues and concerns. One of the main issues of online payments are the lack of security. Without proper security, personal information and credit card information can be compromised and exposed to third parties, which may result in financial loss and identity theft. The fear of this is what keeps most people away from doing online payments.
In a survey done by ZoneAlarm in 2012 [2], the main concerns of doing online payments were

- "The site will start sending me junk email"
- "My personal information will be sold to other merchants"
- "My credit card data will be intercepted"
- "My credit card data will be misused by the merchant"

Most of these concerns revolves around security and privacy policy. Without proper security, credit card information might be compromised, and without a proper privacy policy, customers wont be sure that their personal information will be kept secure and confidential, and not used for malicious purposes.

[1] http://en.wikipedia.org/wiki/E-commerce
[2] http://www.techrepublic.com/blog/it-security/infographic-online-payment-security/

2 The basics of security in e-Commerce

> "Information security, sometimes shortened to InfoSec, is the practice of defending information from unauthorized access, use, disclosure, disruption, modification, perusal, inspection, recording or destruction. " [3]

These days, a huge amount is being purchased on the internet. Almost anything can be bought such as music, toys, clothing, cars, and food. Millions of online payments are done on a daily basis. The huge scale, growth and financial nature of eCommerce is what makes it so prone to threats and attacks. Hackers are always looking for vulnerabilities in the security, while fraudsters are constantly looking to take advantage of shoppers new to online shopping.

Due to the amount of potential attacks and frauds on e-commerce systems, the focus on security the last few years has been huge. Countless of security measures has been done to prevent future threats and attacks. It is important to know that the concept of information security in e-Commerce is also the same as everywhere else, such as computer security and IT security. One of the main purpose of security in e-Commerce is to protect assets from unauthorized access, use, alteration or destruction. In e-Commerce systems, some of the most important security features for both customers and merchants are

1. Data Confidentiality
   Confidentiality ensures that the messages, information, and data sent are only available to the authorized entities. It's not to be confused with privacy, as privacy "protects" access to a person, and confidentiality "protects" access to data.

   Customers: Makes sure that no other than the intended recipient can read their messages.
   Merchants: Makes sure that messages and confidential data is not accesible to anyone other than the authorized customer.

2. Data Integrity
   Data Integrity is critical, because it's prevention against unauthorized data modification. In e-Commerce, integrity for example makes sure that the information being displayed on a website has not been altered by unauthorized entities. With Integrity, we can make sure that the information that is transmitted from a sender to a receiver is not altered.

   Customers: Makes sure that the information they transmit and receive has not been tampered with.
   Merchants: Makes sure that the data on their site has not been altered, and that the data received from customers are valid and legit.

3. Availability
   Availability is another dimension of security that ensures that an e-commerce system continues to function as intended. It makes sure that we have access and are authorized to resources. An availability security breach would be a DoS attack in which hackers renders a website useless, making it impossible for users to access the site.
   Customers: Makes sure that customers can log on the website and buy merchandises.
   Merchants: Makes sure that their website is operational without errors.

[3] `http://en.wikipedia.org/wiki/Information_security`

4. Authenticity
   Authenticity is another necessary asset. It is crucial, because it gives you the ability to identify the identity of a person or entity that you are doing a transaction with. An instance of an authenticity security breach might be when someone poses as a bank employee or someone else with authority, and then requests sensitive information.

   Customers: Makes sure that the customers can be assured of the identity of the person or entity they're dealing with.
   Merchants: Makes sure that they know the real identity of the customer.

5. Non-repudiation
   In e-commerce, non-repudiation is important. It prevents any party from reneging on an agreement after sale/purchase. It basically prevents someone to deny a sale or purchase that has been done. This prevents a buyer from ordering merchandise, deny that he had done so, then request a charge-back with the credit card issuer. Since the merchant has no legal valid proof of the transaction, the customer would receive both the money back, and the merchandise.

   Auditing is also necessary. With Auditing, merchants can keep a record of operations, and thus, they can prove that a customer bought a specific merchandise. This prevents fraud, and gives the merchant legal proof of the transaction.

   Customers: Makes sure that the merchant can't deny agreeing to an action.
   Merchants: Makes sure that a customer can't deny that he/she has ordered products.

6. Authorization
   Authorization makes sure that only you can manipulate your own resources in specific ways. In e-commerce systems, authorization might for example prevent you from increasing the trying to increase the balance of your account, or remove bills that you need to pay etc.

   Customers: Makes sure that you have access to your resources on a website.
   Merchants: Makes sure that customers can't manipulate unauthorized resources such as account balance, bills etc.

7. Encryption
   Encryption in e-Commerce deals with information hiding. Prevents others from spying on each other during Internet banking sessions, and other transactions. This is what gives us confidentiality during acts such as Online Payments.

   Customers: Makes sure that the information sent to the merchant is secure and only available for the merchant.
   Merchants: Makes sure that customers can't manipulate unauthorized resources such as account balance, bills etc.

Even with a top-notch security system, it is important to know that we're not 100 percent secure. It's practically impossible to create a 100 percent secure system, because it's impossible to predict what threats and attacks the future may bring. It's also important that both ends of a transactions are secured, and not only the merchant or customer. A high-end security system can still be breached by viruses, worms or Trojans and other malicious Malware. We can however lower the risks of such attacks by doing risk assessments, and regular maintenence on the systems.

3 Online Payment Methods and own research

Before we go into the specific threats of online payments, it's important to know exactly how online payments are done. There are plenty of ways to pay online. Everyone probably knows about card payments, such as credit card and debit cards. But we also have alternative payment methods that doesn't rely on card, such as online bank transfers, e-checks, Crypto-currencies such as Bitcoins. Furthermore, we have digital wallets or eWallets which acts like a virtual wallet. Paypal is probably the most known one in the USA and Europa, but there exists other virtual wallet such as C-check wallet in Japan and other Asian countries. In the recent years, the popularity of such alternative payments methods has increased sky high, and in this section, we'll look at the two most popular ones, the payment cards and PayPal.

3.1 Credit Cards and debit cards

Credit and debit cards are one of the most used online payment method worldwide, and arguably the most used one. There's no other online payment methods that has such global reach. It's accepted by millions of merchants. A credit card is a payment card that is issued to users from their bank. In Norway, we have banks such as DnB and Nordea. The bank usually has connections to other payment processors, such as Visa and Mastercard. When an user receives a credit card from their bank, they'll often receive an account and a line of credit from the bank. The credit card allows the user to pay for goods and services based on the user's promise to pay for them at an later date. Debit cards on the other hand automatically deducts the money from a connected checking/saving account, and you only spend the money you have available.

3.1.1 How it works

Credit and debit cards are both payment cards, which are cards that can be used to make payments at merchants. They're both 85.60 x 53.98 mm in size, and they both a have printed or embossed bank card number comypling with the ISO/IEC 7812 numbering standard [4].The card numbers are found on the card themselves, and they're often referred to as primary account number. They have a certain level of structure, and on all cards, they share a common numbering scheme. These numbers are allocated in accordance to the ISO/IEC 7812 numbering standard, and with this number, a bank account can be identified. A card number is commonly 16 digits, but can also be 19 digits. These cards also have magnetic stripe or an electronic chip that contains data, making them viable for local payment too. Paying with a credit card online requires the user to enter his/her credit card information, which consists of the expiration date of the card, name of the cardholder, the 16 digits on front, and the CVC number on the back of the card. It's also usually required to enter the billing address.
When using a credit card online, the payment processing happens in two phases. The authorization and the settlement phase.

[4] `http://en.wikipedia.org/wiki/Credit_Card`

Authorization Phase[5]
The authorization phase is the first step in the transaction.
1. The customer initiates a transaction with a merchant.
2. The customer fills in details such as billing/delivery address and payment info.
3. The merchant receives the payment information, and its sent it to an acquirer/merchant bank, which is a financial institution. In e-Commerce systems, a "payment gateway" usually links the merchant's website to the acquirer.
4. The acquirer sends the data to the payment processor (Visa,Mastercard etc.).
5. The payment processor forwards it to the issuing bank (In Norway, usually DnB, Nordea)
6. The issuing bank will verify that the card is legitimate. They'll check if it's reported as lost or stolen, and that the account has enough amount of credit or fund left to pay for the transaction. The credit card number, expiration date, billing address, cvv number is also verified.
7. If everything is alright, the issuing bank will generate an authorization number. This number will be sent back to the payment processor. With this, the issuing bank confirms that the customer can fund the purchase.
8. The authorization number is sent from the payment processor back to the financial institute/merchant bank, and then to the merchant.
9. Depending on the result of the authorization, the buyer will either get declined, or he's taken to the order confirmation page.

The customers part is usually finished after the authorization part. He has made the purchase, and can log off the website while expecting to receive his merchandise or bills cleared. For the merchant however, the whole transaction is not over until the settlement phase is complete.

Settlement Phase[6]
1. After the authorization phase, the merchant will have to submit the transaction information to the financial institute.
2. The financial institute / Merchant bank will forward the settlement request to the customers payment brand (Visa/Mastercard etc.)
3. The transaction will be confirmed with the customers issuing bank.
4. The payment brand then receives the settlement request and does two things based on if the customer used credit or debit card. If the customer used credit card, the payment brand will issue a credit to the financial institute, and the financial institute will pay the merchant. If the customer used debit, a debit will be sent from the payment brand to the customers bank.
5. The customers bank will then post the transaction to his/her account, and he'll receive his/her credit card statement if a credit card was used.

[5] `http://www.cardfellow.com/blog/how-credit-card-processing-works/`
[6] `http://www.cardfellow.com/blog/how-credit-card-processing-works/`

3.1.2 Security threats

While payment cards may be the most used online payment method, they're also the most targeted one, when it comes to threats and risks. There are two sides to the security threats of payment cards. The customers side, and the merchants site.

Merchant's side
Retailers and merchants must prioritize credit card security. It's pointless for the customer to have a secure system if the payment information can be stolen at the retailer. The ability to process payment cards comes with with many risks. To be able to process payments, merchants must implement applications on their e-commerce site. The site must be able to collect, store, and process the payment information that consists of credit card data, and other private personal information. The most typical attacks on e-commerce sites are SQL injection, cross-site scripting and session hijacking.

- "SQL Injection"
  SQL Injection is a web attack mechanism that is used by attackers to steal data from organizations. Usually, web applications allow normal customers to submit and retrieve data from a database. With SQL injection, attackers can pass SQL commands through the web-application to view private information such as credit card information, email address and password from their database.

- "Cross-site scripting"
  Cross-site scripting is a technique that allows the attacker to inject his malicious script-code into a link that looks like its from a trustworthy source. When someone clicks on the link, the malicious code is submitted as part of the client's web request and then executed on the user's computer which allows the attacker to steal information or infect the user with virus.

- "Session hijacking"
  Session hijacking is an exploit. Since HTTP is a stateless protocol, and users are usually identified by a session id, stealing that session id would let you impersonate them. By doing this, attackers might be able to get their hands on sensitive information.

Such attacks can be prevented by implementing the correct counter-measures. But even if they are prevented, it's also important that the security on the customer's side is good.

Customer's side
The customer has his own set of responsibilities to ensure a secure transaction when shopping online. It's important that the customer is on a virus-free computer, and that the internet connection is secure. Even if the merchant has a state of art secure e-commerce website, the customer can have his personal information stolen if not careful. The usual main threats for the customer is

- "Virus, trojans and keyloggers"

  The most common threat for the average user are Trojans and viruses. Viruses attaches themselves to executable code, and they're executed when the user runs the infected code. The virus can then cause damage from deletion of files to reformating the hard drive, or infecting the user with more virus. Another threat for the users are Trojans. Trojans are programs that appears to be safe and legit, but actually contains malicious codes that's hidden in the program. These trojans can install keyloggers. Key-loggers are a well used form of malware. They give attackers the ability to steal credit card numbers, personal information, and passwords by logging every key that is pressed on the keyboard. Some key-loggers are even able to take pictures of the monitor and send it to the attacker.

- "Unsecured networks"
  Even if the customer is paying on a virus-free computer, he's still vulnerable to threats when paying online if he's on an unsecured network. An unsecured network might be a home wireless network that doesn't have a password, or a public wireless hotspot. Either way, using such networks is not recommended due to the fact that attackers can have access to the network. If there are attackers on the network, and you log in to un-encrypted websites, they can potentially see what you see, and hijack your session. Your sensitive information, photos, and even your credit card information could be compromised.

3.1.3 Security Measures

Even though payment cards used to be a risky online payment method due to all the threats, in the recent times, the security has grown dramatically. Payment cards now have plenty of security measures such as

- "PCI - DSS"
  The Payment Card Industry Data Security Standard is a set of requirements designed to ensure that all retailers, merchants and companies that store, process or transmit credit card information maintain a secure environment. It was launched in 2006, but the newest version, 3.1 was released in April 2015.[7] There are 12 main requirements of the standards, some of them requiring that the retailer install and maintain a firewall that protects the customers data, and that they encrpy transmission of cardholder data etc. Thanks to the PCI - DSS, the chance attacks against retailers such as SQL-injection and cross-site scripting is less, due to the stricter security requirements of systems.

- "AVS - Address Verification System"
  Address Verification Service is a service that merchants can perform during authorization. When a customer orders merchandise from the internet, he/she has to enter his billing address. This information is then compared to their address kept on record at the bank. AVS will check if the numeric address and zip code match. Based on the results, the system will return an flag. The merchant can then make a decision based on the AVS flag returned. The system can prevent the merchant from accepting a stolen card, and at the same time, it stops a stolen card from being used.

- "CVV - Credit Card Verification"
  CVV stands for Card Verification Value. It is equivalent to CVC which is card verification code, CID, CVD and CVVC. The CVV is a number that is usually printed on the backside of a payment card. It's not stored anywhere else, neither in the magnetic stripe or chip. It's used to confirm that a cardholder actually has the card in possession when used in online payments. This can usually prevent fraudulent transactions, but if the CVV is in the hands of the attacker, then there's no use.

- "3D - Secure"
  3D - Secure is another security measure that is used with payment cards. It's designed to be an additional security layer for card transaction. It basically adds an authentication step for online payments. The step occurs after the customer has entered his card information. The customer will have to confirm his identity, usually by a code unit issued by the bank. In Norway, we use have to log on BankID

[7] `http://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard`

to confirm our identity, and we do that by entering our password and the code from the code unit, or we can use our smartphones[8] .

3.1.4 Own research and testing of threats and measures

In this subsection, I'll present my research on the safety of payment cards. As I pointed out in the beginning of this paper, I will go over the threats that I wrote about, and I'll see if they're still threats today. I'll also test the security measures, and see if they can prevent me from doing an unauthorized transaction against myself.

Security measures testing

- "AVS - Address Verification System"
  The first security measure I tested was the AVS. It's role is mainly to prevent stolen credit card information to be used. The AVS is a well known security measure in the USA. It's widely supported by VISA in the US and the UK, but how does it hold up in other countires, such as Norway?
  To test out the AVS, I first changed my Norwegian IP to an American IP by using a VPN (Virtual Private Network). The VPN I used under the testing was vyprvpn[9]. This was to reenact the role of an American hacker who could have gotten his hands on my credit card information.

  1. After setting up my IP, I created an account on Amazon.com [10]
  2. The Amazon account had random shipping/billing address located in the USA, with a random name.
  3. I added some cheap items to my cart, totaling around 2 dollars.
  4. I tried checking out, and it worked without issues.

  So what does this tell us?
  From my experience, my norwegian issued credit card was not protected by the AVS System. If an hacker had gotten hands on my payment information, he'd have been able to use the card to his benefits online. I wasn't quite satisfied by my first test, so I tried it once more, with a Norwegian IP, and trying to order merchandise to a neighbor of mine in Norway.

  1. For this setup, my neighbor had given me permission to use his wifi network. I used his IP, to reenact the role of an neighbor that had gotten his hands on my credit card information.
  2. I sat up an account with his billing address and shipping address on coolshop.com
  3. I used my credit card to order a game to his address, with his name.
  4. I tried checking out, and it worked.

  From my own experiences, I've confirmed that AVS system isn't supported in Norway. It might be a well known security measure in the US/UK, but it's definitely not supported in Norway.

[8] `http://www.nets.eu/no-nb/produkter/kort/kortutstedelse/3Dsecure/Pages/default.aspx`
[9] `https://www.goldenfrog.com/vyprvpn`
[10] `https://Amazon.com`

- "CVV - Credit Card Verification"
  The second security measure I tested was the CVV. It's role is to confirm that the customer is actually in possession of the card they're using in online transactions. The three/four numbers on the back of the card is needed by merchants and payment gateways to complete a transaction. Testing the functionality of the CVV was very easy.

  1. I wrote down my name, the expiration date and 16 digit number of my credit card on 4 pieces of paper.
  2. I gave the pieces of paper to 4 different persons. I asked them to try to purchase 1 month of subscription on netflix.com with the information they have on the paper.

  The result was that that none of them could make a purchase without the CVC, because as pointed out earlier, it's essential. The payment system wouldn't let them complete the checkout session without typing in a CVC number.

  1. After the first test, I gave 3 of them a sequence of 3 random CVC numbers, and I gave the last person my correct CVC.
  2. Only the person with the correct CVC finished the transaction. The other 3 received errors when trying to checkout.

  From the results, we can see that CVC is effective. If a hacker gets his hands on stolen credit card information, but not the CVC, it wont be possible for him to use the card. But the scary part is, what if the attacker manages gets the CVC too? The attacker will then be able use the card, taking advantage of the victims information.

- "3D - Secure"
  The third security measure I tested was 3D - Secure. 3D secure is designed to be an additional security layer, it adds an authentication step after the initial checkout. Testing the feature out was another easy task, compared to the AVS testing. I used a similar method to my CVV testing.

  1. I passed my full credit card information to my brother, including CVC, expiration date, name, and of course the 16 digits.
  2. He first tried to purchase merchandise on elkjop.no[11], a Norwegian consumer-electronic retailer site.
  3. After entering the payment information, he was asked to log into BankID.
  4. To log into BankID, he'd either have to have the code unit that was issued from the bank, or my smartphone connected to BankID.
  5. He didn't have any of them, so the transaction was canceled.

  Although 3D - Secure was functioning, it's important to know that not all merchants support it. Under my AVS and CVV testing, I was never prompted by 3D - secure to log into BankID. From my experience, it's mainly supported by the big retailers in Norway, but that there's less support for the system abroad.

[11] `www.elkjop.no`

Figure 1: 3-D Secure in action.

Virus threat testing
After testing out the security measures and their effectiveness , I wanted to test out the threats themselves. In the earlier subsection, I wrote that the threats that affected the customers while using payment cards were virus/Trojans and insecure WiFi networks. The biggest threat of these two were definitely viruses/Trojans, so I wanted to do a test on this threat over the course of the research paper.

"How big of a threat are virus and trojans in 2015?"
This small test was done to see if viruses and trojans were still a threat to the regular customer using payment cards in 2015. The point of the test was to see how long I could surf with a computer before my credit card credentials were compromised. I started the test on the 10. April 2015, the date I received my newly issued credit card from my bank. To reenact the regular customer, I first had to set up my computer.

1. I first re-installed a new copy of Windows 8.1
2. I updated the operating system, and installed all security updates that had been released up to 10. April 2015.
3. I reset my router, and sat up a new password protected 2.4GHZ WiFi network
4. I ensured that the firewall was enabled.

After everything was set up, I used the computer as I would normally do. Everyday I did my regular routine, browsing newspaper online, social medias such as Facebook, and typical entertainment sites such as Youtube and Netflix. Since I was playing the role as a regular person who wasn't tech-savvy, I also clicked on random links that looked interesting. I didn't have any kinds of ad-block installed, and every 5 days I made sure to make a purchase with my credit card.

From the 10. April to 31. April, I had done 4 different transactions online with my credit card. I was supposed to do the 5th purchase on the 5th of May, but when I checked my transactions on that day, there were 2 unauthorized transactions that had been done with my credit card.

01. mai	Visa 100322 Sek 139,00 Match Meetic Valutakurs: 0,9238	05. mai	128,41
	Visa 100222 Sek 299,00 Match Meetic Valutakurs: 0,9237	05. mai	276,21

Figure 2: Two unauthorized transactions on my account.

As seen from figure 2, there were two transactions that had appeared. These transactions were unknown to me. After discovering the unauthorized transactions, I filed a charge-back request immediately through my banks website. I also called customer service to notify them about the incident, and they blocked the concerned credit card.

Figure 3: Chargeback procedure on DnB.no

The result of the test was overwhelming. Within 20 days, and with just 4 transactions, my card information had been compromised. With this, I can conclude that although the chances might be low, we're still susceptible to threats such as viruses in 2015. It also shows that the AVS, CVC, and 3-D secure system wasn't able to stop the hacker from taking advantage of my credit card information.

3.2 Paypal

Paypal is an american worldwide online payment system that was established in 1998. It is one of the largest internet paymet companies, and it operates as an a acquirer. As of 2014, Paypal operates in 203 markets and has over 150 million active accounts. PayPal allows individuals and merchants to transfers funds electronically, while also allowing them to hold funds in up to 26 different currencies worldwide.[12] Due to it's huge reach, PayPal is accepted as a payment method at most merchants.

3.2.1 How it works

A Paypal account has a paypal balance. The user can choose to add money to the account by bank transfer, credit card, or by receiving funds from other users. When a customer wants to send money to someone, he can do it by entering their email, even if they don't own a paypal account. When sending money, Paypal will check if the account has enough balance to fund the payment. If not, the user can use another payment method linked to his account, such as Credit Card. The user can also withdraw the Paypal funds to his bank account, if he wishes to do so.

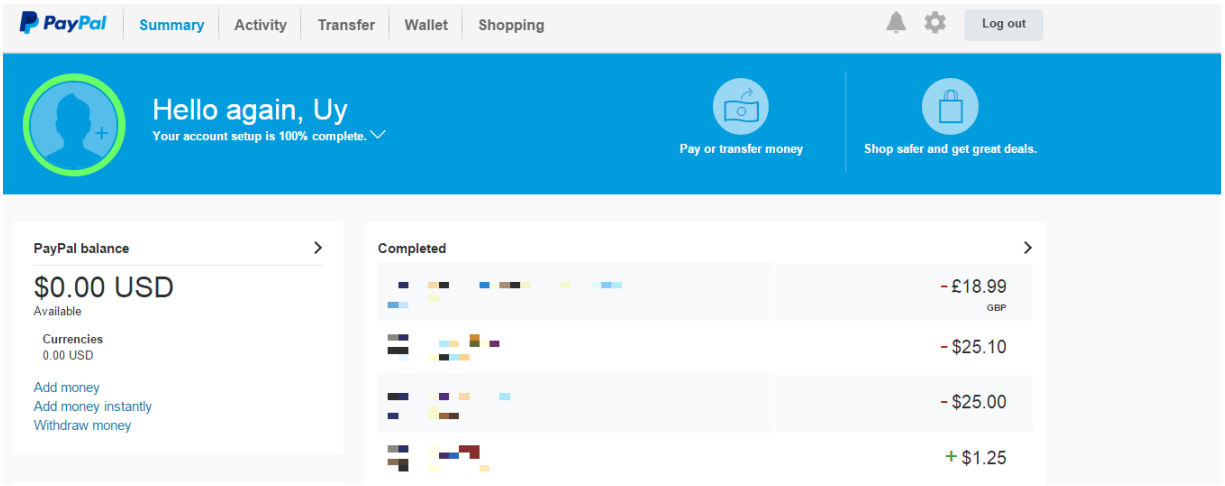

Figure 4: User interface on Paypal

3.2.2 Security threats

Paypal is vulnerable to some of the same threats as payment cards.

- "Virus, trojans and keyloggers"
  Viruses, Trojans and Keyloggers can be harmful to customers who use Paypal. Since Keyloggers can log every key that is pressed on the keyboard, a user with a keylogger installed might have his Paypal account information compromised. This could lead to hackers taking advantage of your paypal funds and linked credit cards.

- "Unsecured networks"
  Unsecured networks are also danger to customers who use Paypal. Logging into your paypal account while on an unsecure network will set your account information at risk.

[12] `https://www.paypal-media.com/about`

- "Shared password and email account"
  Another big risk of using Paypal is the shared passwords among email addresses. If an user has the same password and email address on another website, the user risks getting hacked if an hacker somehow gets his account information from the other site. Since the password and email are the same, the hacker can log into the users paypal account with the same email and password.

3.2.3 Security measures

Paypal also has some security measures up its sleeve.

- "PayPal Security Key"
  The PayPal security key add another authentication layer when logging into an account. After entering your password, you'll receive a OTP (One Time Pin), that'll work only for that login. The OTP is sent via SMS to the account owner. This prevents attackers that have the account information to log on the account. The original user will also be notified if attackers try to.

- "Confirmed shipping address and credit card
  When linking a credit card to a paypal account, the user has limited paying abilities. He has to confirm that he's the owner of the card before he can pay over a specific limit. Paypal usually does this by charging the user with a small sum. The charge will appear on the users card transaction with a 4-digit code. Entering this code will complete the process, and remove the specific paying limit. This measure is to prevent stolen credit cards from being used, thus protecting both the original cardholder, and merchants from future chargebacks. The user can also confirm his address. An address can be confirmed if the buyer's credit card billing address is equal to his shipping address. Confirmed addresses is another measure against stolen credit cards and identity thefts.

- "Account limitations"
  Paypal has a feature called account limitation. It prevents an user from completing actions with an account. The features that are limited are such as sending/receiving money, and withdrawing funds to bank account. Account limitation is applied to accounts that has suspicious activities. Suspicious activities might be logging in on an unknown IP address, or unusual payment activity. Account limitation is usually done if Paypal suspects that someone is using someone else's account. This limit can be removed by confirming the users identity.

- "Disputes"
  Paypal disputes have the same concept as credit card chargebacks. If there are unauthorized or fraudalent transactions, the user can send in a dispute. Paypal will then investigate, and if the dispute ends in the users favor, he/she will receive a refund.

- "SSL - Secure Sockets Layer protocol"
  PayPal uses SSL, which stands for Secure Sockets Layer protocol. It ensures that the information transit from the users computer to Paypal is encrypted by a key length of 128-bits. PayPal checks your browser . The PayPal database is also not directly connected to the internet, so it avoids troubles such as SQL injection and cross-site injection.

3.2.4 Own research and testing of threats and measures

In this subsubsection, I'll do do some experimental testing against the security measures of PayPal, almost in the same procedure which I did credit cards.

Security measures testing

- "PayPal Security Key - Testing"
  Unfortunately, the PayPal security key isn't available worldwide. On my norwegian PayPal account, I didn't have the option to enable the feature, so the optional protection layer is not available for me. Without the option to enable the feauture, I couldn't test the function. Since the function isn't available worldwide, it makes paypal more riskful to use for users not in the UK and US.

- "Account limitation - Testing"
  To test out the account limitation measure, I used a VPN (vyprvpn) to change my norwegian IP to an American one. The goal of this was to see if I could still make a payment with my PayPal account if the IP was an unknown one.

  1. I first enabled vyprvpn, and changed my IP to an IP based in USA - New York
  2. I succesfully logged on PayPal without issues.
  3. When trying to transfer money to another paypal account, I was prompted to verify my account by either a test message, or an automated call.

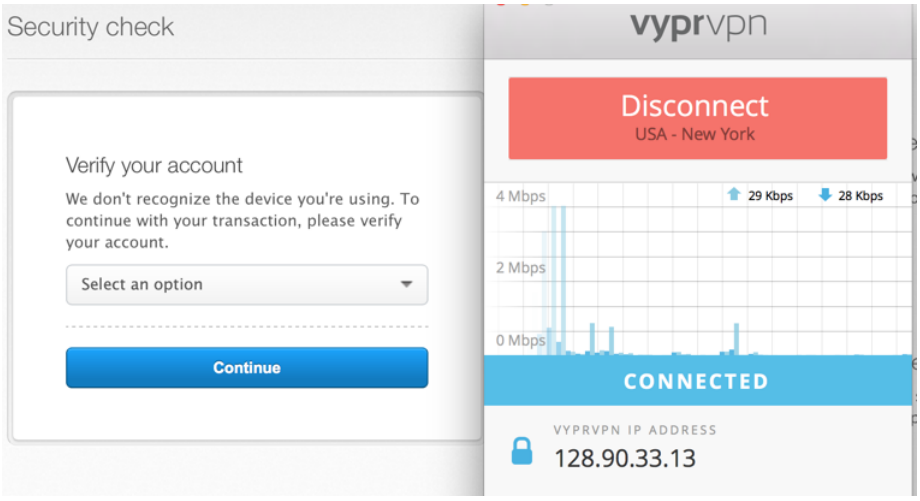

Figure 5: Account limitation on PayPal

The first test was successful. The account limitation feature was proving itself to be working, but I wanted to try another test. What if I changed my ip to another norwegian IP?

1. I first enabled vyprvpn, and changed my IP to another norwegian IP
2. I succesfully logged on PayPal without issues.
3. This time, PayPal didn't prompt me to verify my account. I could make a money transfer without problems.

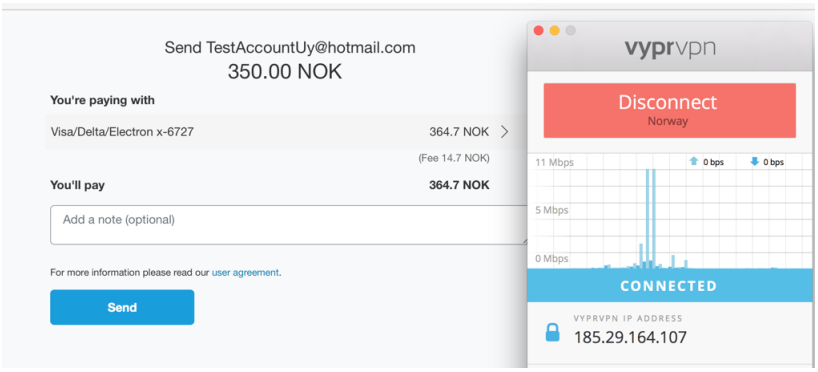

Figure 6: Successful payment on PayPal

The second test was rather surprising. Even though the IP was unknown, I was still allowed to do money transfers and purchases. PayPal has probably allowed IP's in the same country to work and bypass the account verification step, perhaps to make it easier for customers to buy merchandise from their home and job offices. But this is a security risk in itself. If an attacker from Norway had gotten his hands on my account credentials, he could have taken advantage of my account and funds. Or even worse, an attacker from the US could have just used a VPN to change his american IP to a norwegian one, and it would have bypassed the account limitation feature.

3.3 Comparison between Payment Cards and PayPal

After my own research on both payment cards and PayPal, I'd said that they both lack in security. Credit cards security measures such as the AVS and 3-D Secure seemed excellent at first glance, but the issue is that they're not supported globally. On the other hand, Paypal's security key isn't supported globally either. If these features were supported everywhere, both payment methods would have been much more secure. They both are also vulnerable to viruses. Keyloggers can for example compromise your paypal account information, while also managing to log your credit card credentials. The important thing to know is that Paypal isn't as safe as it sounds. If your paypal account is compromised, and you have linked your credit card to it, then you'll also risk having hackers taking advantage of your credit card and your paypal funds. Both of them are riskful to use without proper anti-virus software and secure network.

4 Conclusion

Online Payment Security has gone a long way the recent years. From updating the PCI - DSS to new payment methods such as Paypal, with new multi-factor authentication. Unfortunately, the potential threats that threatened online payment when it first came are still there. Keyloggers, virus , trojans and other malicious malware still threatens online payment security. Account and payment information can still be compromised, and some of the new security measures are easily bypassed. Some security measures aren't even supported globally. Is Online Payment safer than it was several years ago? Definitely. But is it safe enough so that the regular user can skip the precautions of installing anti-virus and making sure that he's on a secure network? Definitely not. Not yet.

References

[1] Wikipedia, "E-Commerce"
Read 6. April 2015
http://en.wikipedia.org/wiki/E-commerce

[2] Selena Frye, "Infographic: Online payment security"
Published February 10, 2012, Read 6. April 2015
http://www.techrepublic.com/blog/it-security/infographic-online-payment-security/

[3] Wikipedia, "Information Security"
Read 6. April 2015
http://en.wikipedia.org/wiki/Information_security

[4] Wikipedia, "Credit Card"
Read 10. April 2015
http://en.wikipedia.org/wiki/Credit_Card

[5] Ben Dwyer, "Credit Card Processing: How it Works"
Read 10. April 2015
http://www.cardfellow.com/blog/how-credit-card-processing-works/

[6] Wikipedia, "Payment Card Industry Data Security Standard"
Read 10. April 2015
http://en.wikipedia.org/wiki/Payment_Card_Industry_Data_Security_Standard

[7] Nets, "3-D SECURE"
Read 10. April 2015
http://www.nets.eu/no-nb/produkter/kort/kortutstedelse/3Dsecure/Pages/default.aspx

[8] Paypal-about, "About PayPal"
Read 19. April 2015
https://www.paypal-media.com/about