E-business and E-commerce Security

Kaurice W. Woiwor

Old Dominion University

E-business and E-commerce Security

Introduction

In our technology-driven world, business is booming online. Since the invention of the internet, online businesses have grown. Now, large and small companies have a presence on the internet. Almost every store has a website online, whether it is a clothing, electronics, furniture or home goods store, there is a website. Almost anything can be bought or sold online. With the growth of the internet comes danger. The internet has allowed criminals to commit crimes easily. Stealing credit card information has become even more prevalent. For that reason, E-business and E-commerce security are very important.

E-commerce is "the buying and selling of goods and services online through a secure website, with payment by credit card or direct from a checking account (Solomon & Kim, 2016)". Online business is quite lucrative and protecting this business is important. Both parties should feel comfortable with the company's security system. E-commerce security is important to discuss because there are so many people that shop online. Shopping online is very convenient and has grown over the years (Mantel, 2013). Business having a presence online is a great way to attract customers (Mantel, 2013). According to Larry Freed, CEO of Foresee, "consumers have a better experience online than in the store (Mantel, 2013)". Freed is the CEO of the Ann Arbor, Michigan division. Foresee is a company that measures customers satisfaction for their retail clients (Mantel, 2013).

Consumers may have a better experience shopping online than in store because there are fewer objectives in the way of them buying what they need. Freed believes shopping online is more reliable (Mantel, 2013). He says it is more organized because there is no interference from sales associates on showroom floors (Mantel, 2013). Freed argues, that online shopping is more convenient because consumers can shop at any time of the day (Mantel,2013). Unlike retail stores, online businesses are opened 24/7 (Mantel, 2013). Consumers do not have to leave their homes or waste time searching for a parking spot to purchase what they need (Mantel, 2013). Most of the time, there is more inventory offered online than in-store (Mantel, 2013). Freed adds, that people prefer to help themselves than deal with a sales associate, mainly the reason they shop online (Mantel, 2013). If the customers are satisfied, then sales will increase; having an online presence can help brand loyalty and recommendations (Mantel, 2013).

As online shopping continues to grow, protection must grow with it. When customers purchase items from these companies, they expect their credit and debit card information to be safe. If these companies can easily be hacked, everyone will be affected. The company will suffer, as well the individual. A company prone to hacking can lose future profits and put their customers at risk. Customers can lose more than just money by shopping with these companies. Stolen credit and debit card information can cause enormous damage to consumer's lives. Consumer's credit cards could be maxed out and bank accounts drained of all their money. These incidents can affect a customer’s credit score and result in customer's identity being stolen; which can cause more damage to their lives.

Target’s Breach

E-Commerce has become so important in our society that we must take measures to protect it and the induvial who use it. The Target data breach of 2013 is a great place to start discussing the importance of e-Commerce security. Late November to mid-December, the Target Corporation experienced a network breach (Shu, Tian, Ciambrone, Danfeng,& Yao, Y, 2017). It is known as the second devasting data breach in history (Shu et al., 2017). 40 million debit and credit card numbers were stolen, as well as 70 million records of personal Information (Shu et al., 2017). It cost over two hundred million dollars for credit card unions to issue new cards to their customers (Shu et al., 2017). Hackers infiltrated Targets system with compromised credentials from Fazio Mechanical (Shu et al., 2017). Fazio Mechanical was a third-party vendor of Target's (Shu et al., 2017).

When the attackers hacked into Target's networked, they used Target's weak points and exploited them (Shu et al., 2017). They used vulnerabilities in the system to access sensitive data and transferred data out Target's system (Shu et al., 2017). Due to Target's poor segmentation, the hackers were able to access the sale networks (Shu et al., 2017). Once the attackers had access to Target's business section, they gained accesses to other parts of Target's network. The attackers even gained access to areas containing sensitive data (Shu et al., 2017). The attackers installed a malware known as BlackPos onto Target's point of sales (Shu et al., 2017). This malware allowed the attackers to keep track of card information, like credit and debit card numbers. Any card scanned at the card readers connected to Target's point of sales devices were likely to have their card information stolen (Shu et al., 2017). From there the stolen card numbers were encrypted and moved to a secondary location (Shu et al., 2017). From there the stolen card numbers were encrypted and moved to a secondary location (Shu et al., 2017).

The stolen credit card numbers were tracked to a server in Russia (Shu et al., 2017). The attackers were able to collect 11 gigabytes of data in less than a month (Shu et al., 2017). The stolen credit cards numbers were later found on the black market for sale (Shu et al., 2017). Target had all the measures in place that a company needs to secure their business (Shu et al., 2017). Target had firewalls up and used Virtual Local Area Networks (VLAN) (Shu et al., 2017).

However, Target dropped the ball in some areas (Shu et al., 2017). According to “Breaking the Target: An Analysis of Target Data Breach and Lessons Learned”, Target did not look into security warnings created by different security tools. Target failed to isolate their sensitive networks as well. Using Virtual Local Area Networks (VLAN) is not completely secure, it is said to be easy to get around (Shu et al., 2017).

The article states that Target’s point of sale terminals was not hardened enough (Shu et al., 2017). This allowed for unauthorized software to be installed and configurated (Shu et al., 2017). As a response to the lack of hardening, the malware was able to spread to credit card information in the point of sales terminals (Shu et al., 2017). Lastly, Target did not enforce proper access controls on accounts and groups of third-party partners (Shu et al., 2017). If Target enforced these access controls the incident would not have happened (Shu et al., 2017). In return, the incident affected Target’s business.

Customers and citizens were shaken when they heard about the data breach. This incident proves why E-commerce security is important. A business, as big as Target, is not untouchable. If Target can experience such a substantial data breach, what does that mean for other companies? Small businesses automatically have a higher risk than larger ones. An incident like this could destroy a small business. Small businesses may not have the money or resources to rebuild their credibility. E-commerce security is important to both small and large business. Both businesses want to thrive and keep their customer's information safe.

Small Business and E-commerce Security

According to Dr. Syed M. Rahman and Robert Lackey, co-authors of “E-Commerce Systems Security for Small Business”, small businesses are the perfect place for malicious attacks (Rahman & Lackey, 2013). Small businesses do not have effective measures to respond to an attack; unlike larger businesses (Rahman & Lackey, 2013). Cybercriminals take advantage of the circumstances small businesses are in. Most small businesses do not have the highest level of security implemented, because they cannot afford it. Small businesses attacks seem to increase every year (Rahman & Lackey, 2013). In 2011, "The Small Business Breaches" chart showed an increase of breaches from 2009 to 2010 (Rahman & Lackey, 2013). In 2009, there were 141 attacks on small business. In 2010, there were 761 attacks on small business (Rahman & Lackey, 2013). The attacks increased from 27% to 63% in one year (Rahman & Lackey, 2013). These attacks do more harm to small businesses than large, small businesses may not recover from a malicious attack.

Effects of a Breach on Small and Large Businesses

Whether a business is small or large, both can experience the same results of being attacked. Both businesses can be affected directly or indirectly (Rahman & Lackey, 2013). A direct loss could be financial; companies could lose money by receiving fines or having to pay legal fees. An indirect loss is equal to the company losing credibility with the public (Rahman & Lackey, 2013). Nobody wants to spend their money with a company they cannot trust (Rahman & Lackey, 2013). Consumers will be skeptical spending their money at these businesses, whether the issue was major or minor. More examples of loss a company may face, include loss of productivity and stolen confidential information (Rahman & Lackey, 2013). Employees may not be able to perform duties if the systems are down. Down systems, will cause the company to lose productivity (Rahman & Lackey, 2013).

In an attack, stolen confidential information like business secrets, employee's records, and customers information could be disseminated anywhere (Rahman & Lackey, 2013). In any breach, there is a chance of technical issues. A breach could cause damage to a company's files and system (Rahman & Lackey, 2013). Files could get lost and servers could be damaged if the attack is malicious (Rahman & Lackey, 2013). A malicious attack could cause errors in a systems configuration, causing the system to perform differently than normal (Rahman & Lackey, 2013). A breach can also cause errors in applications performance (Rahman & Lackey, 2013).

Small and large businesses experience the same effects from a breach. Smaller businesses may be hit harder than the larger ones because they do not have the same resources as the large business. Financial loss and credibility are very concerning for any business. No company wants to lose money at the expense of hacking; that is why e-Commerce security is so important. Companies work hard to establish themselves and make a profit; losing money and credibility because their systems lack in some department is not pleasing.

Improving and Preventing E-Commerce Security Issues

Improving and preventing e-commerce security is a responsibility that falls on everyone. Technology developers, e-Commerce Business owners, government, payment processors, and consumers, can all do something to help (Khurana, 2017). Ajeet Khurana, former CEO of Society for Innovation and Entrepreneurship, believes using Secure Sockets Layer (SSL) or two-factor authentication are great ways to help mitigate the issue (Khurana, 2017). “Secure Sockets Layer (SSL) is a standard security technology for establishing an encrypted link between a server and a client—typically a web server (website) and a browser, or a mail server and a mail client” (“What Is SSL”). A Secure Sockets Layer (SSL) certificate helps protect sensitive information traveling on the web (“Knowledge center”). It prevents information from potential security threats and attacks (“Knowledge center”). It is recommended for businesses to have an SSL certification with high encryption levels. Higher encryption levels equal more security for the business (“Knowledge Center”).

Two-Factor authentication also known as 2FA or Multifactor authentication, is a two-step verification (Rouse). Users must provide two authentication factors to verify their identity (Rouse). Users may be asked to provide answers to a security question after logging or before completing a transaction. PIN codes created by the site and given to users to provide back to the system; is another two-factor authentication measure. (Rouse). Incorporating two- factor authentication into transitions is a good way to prevent false purchases. If more businesses incorporated this into their transaction stage, this could lessen false purchases.

Tokenization

Tokenization is a solution suggested for customers to use to protect themselves from fraud. “Tokenization is a payment technology to minimize credit card information by merchants during transactions” (Shu et al., 2017). Tokenization technology, helps customers protect their credit card information. Customers are essentially using a middleman to make purchases. Customers give their credit card information to an acquirer, the acquirer then creates a one-time token based on the customer’s credit card information (Shu et al., 2017). The acquirer sends the one-time token to the seller to complete the customer's purchase (Shu et al., 2017). Customers can use this service by using acquirer systems like PayPal, Apple Pay or Google wallet (Shu et al., 2017). Customers can also use an acquirer through their bank. Some banks offer this service; banks will create a one-time credit card number for their account holders to make purchases (Shu et al., 2017).

If customers decide to utilize this service, they can protect themselves more when making purchases. Customer’s credit card information will not be as easy to obtain in an attack. Tokenization is something that could help many people avoid stolen credit card information. More banks should offer services that include tokenization to their account holders. Tokenization can help customers feel more secure when making purchases online.

EMV Systems

In the article “Breaking the Target: An Analysis of Target Data Breach and Lessons Learned”, authors Xiaokui Shu, Ke Tian, Andrew Ciambrone and Danfeng (Daphne) Yao, discuss different credit card security solutions and options for customers to improve security. EMV systems were one of the credit card security solutions they discussed. According to the article “EMV payment system is the major technology developed to address the security issue in credit cards” (Shu et al., 2017). EMV systems were created to help mitigate credit card security problems. EMV systems provide tamper-resistant chips to cards (Shu et al., 2017). Most credit and debit cards use this system; nearly every bank card has a chip. The chip holds private account information and uses encryption and digital signatures (Shu et al., 2017). Authentication is established through the chip and by identifying the user. Users identify themselves by providing a signature or a pin number (Shu et al., 2017). Data on the chips are encrypted, making it difficult for fraud to be committed by an attacker (Shu et al., 2017).

Having chips on cards help lower attacker’s chances of stealing other people’s private information. It is not one hundred percent effective, but it does work. With more improvement to EMV systems, customers may be able to protect themselves even more.

Laws and Training and Preparation

More laws geared at attackers will make a difference in e-commerce security. Training for professionals in this field and business having an attack plan will make a huge difference improving e-commerce security issues. There should be harsher laws to discourage attackers from committing these attacks. If the punishment is more severe, some attackers may be discouraged to commit the crime. Not all attackers will be persuaded by these harsh laws, but some will. Harsh laws could be a great way to lessen the number of breaches and attacks that occur. Better training for professionals in this field can help as well. The more knowledge and experience professionals have the better they can do their job. Companies should offer training within the company to help prepare all employees in their departments. Companies should perform data breach scenario training, to examine where their employees are lacking, then offer more training to help them.

Lastly, being prepared is the best way to lessen e-commerce security issues. Companies should include more testing and monitoring to prevent attacks from happening. The more they monitor their systems, the less can go wrong. If anything looks suspicious or out of the ordinary, they will know first, because someone will be monitoring the system. Companies should also have proper security systems in place to ensure the safety of customer's card information and well as their private information. Those systems should be checked regularly, to make sure everything is up-to-date. If systems are not up-to-date, they will have a higher chance of being attacked. Companies should have a system in place to stop an attack and a plan to trap an attacker if needed too. Having a plan in place to secure your company, and customers are important.

Conclusion

E-commerce security should be important to everyone, it affects us all. People use the internet worldwide make purchases daily. The more people that shop online, the more opportunities attackers have to steal credit and debit card information. There should be more interest and ideas to help secure e-commerce security. Breaches like Targets and many others, were eye-openers for many, it shed light on the importance of securing these networks. Thousands of people were affected by these breaches. Not only are cardholders affected, the card company and business all suffer. Therefore, we need more ways to improve security technologies and prevent further breaches from happening.

These breaches affect large and small business. Both businesses will experience the similar problems. Small businesses feel the effect more than large ones. Breaches can ultimately destroy a small business. However, there are many options available to help prevent customer's credit card information from being stolen, like Secure Sockets Layer and Two-Factor authentication. Secure Sockets Layer and Two-Factor authentication are recommended to customers to provide more protection. Tokenization and EMV systems are recommended as well. As much as those technologies are important, it is important to have laws, proper training for professionals and preparation plans. These solutions are helpful in solving the e-commerce security issue, but there is still work to be done.

E-commerce security will never be perfect, but with time anything is possible. Someone may create the next application that solely prevents these attacks until then we must be vigilant and smart. Consumers should always be cautious when shopping online. Business, large and small, should take all measures possible to protect their customers. If everyone works at a collective, breaches can be a thing of the past.

References

Khurana, A. (2017). How to safely and securely share bank details online and prevent fraud. Retrieved from https://www.thebalancesmb.com/security-issues-in-ecommerce-1141591

Knowledge Center. (n.d.). Retrieved April 18, 2018, from https://www.net4.com/aspx/article/ssl-certificate-secure-website.aspx

Mantel, B. (2013). Internet shopping. *CQ Researcher, 23*, 573-596. Retrieved from http://library.cqpress.com/

Rahman, S, M., & Lackey, R. (2013). E-commerce systems security for small business. AIRCC, 5. Retrieved from http://airccse.org/journal/nsa/0313nsa15.pdf

Rouse, M., & Cobb, M. (n.d.). What is two-factor authentication (2FA)? Retrieved from https://searchsecurity.techtarget.com/definition/two-factor-authentication

Shu, X., Tian, K., Ciambrone, A., Danfeng, D., Yao, Y. (2017). Breaking the target: An analysis of target data breach and lessons learned. Retrieved from https://arxiv.org/abs/1701.04940

Solomon, M, G., & Kim, D. (2016). Fundamentals of information system security (3rd ed.) Burlington, MA: Jones & Bartlett.

What Is SSL (Secure Sockets Layer)? (n.d.). Retrieved from https://www.digicert.com/ssl/?msclkid=dd707371700919875177729a6e5e682aa&utm_source=bing&utm_medium=cpc&utm_campaign=SSL (Generic)&utm_term=ssl&utm_content=SSL