Analysis of Security in E-Commerce and M-Commerce

Nuno Dias Mata
R. de Augusto Rosa 24, 4000-098 Porto, Portugal (2020)
Lusófona University of Porto
nunodmata@gmail.com

Abstract. This study explores the security related with E-Commerce and M-Commerce. With focus on the evolution and development of techniques that positively impact our safety using these services such as two factor authentication and strong database encryption we will understand how much it has changed. In contrast the consequent rise of more creative and different methods to breach these Websites or trick users into giving their personal data will be shown through examples like phishing sites, malicious links, key loggers, and further discuss what specific measures have been implemented to fight them. Nowadays the amount of traffic that visits these markets has increased exponentially which is correlated with the number of Websites and Apps developed throughout the last decade. It's clear why there is a necessity for continuous improvements in security for such fields, not only because the existing growth of the market but also given how sensitive the user submitted data can be.

Keywords: E-Commerce, M-Commerce, Authentication, Encryption, Phishing, Key Loggers

1 Introduction

With technology moving at high-speed no company can ever claim to be 100% covered by any security measure, even the slightest change to an IT system can make its security out-of-date. What needs to be addressed is the effect it would have on a business if all a company's data were to be destroyed, trading lines were brought down for a couple of hours (or worse a couple of days), or its home page was defaced. Not only would loss be measured in financial terms, but also in that of corporate image, leading to potential loss of customers and their confidence.

According to available data, online purchases have been steadily increasing since 2014 and e-retail revenues are projected to pass the 4 trillion US dollars in 2020 [1], and further studies show that 60% of Europeans (aged from 16 to 74) shopped online in 2019 [2].

Which means a wide variety of commerce is conducted via Electronic commerce (E-commerce) and the same can be said for Mobile-commerce (M-commerce), including electronic money transfer, supply chain management, online marketing, online transaction processing, electronic data interchange (EDI), inventory management systems etc. And is now being used in all types of business, including manufacturing companies,

10.11228/dpsc.02.01.007

retail stores, and service firms. It has made business processes more reliable and eminent. Consequently, E-commerce is now essential for businesses to be able to compete in the global marketplace today, and so maintaining these service's integrity is key, which means privacy and security are a major concern if companies want to keep consumers using the Electronic and Mobile markets. And it is known that many security issues are increasing day by day on the open internet like unauthorized access, client information leakage, credit card clowning etc [3].
The future is likely to be more alarming in the sense that crimes will be emitted without the knowledge and cooperation of the victim. Preventing cybercrime in the future will require strong E-security rather than plain human prudence. And that places most of the responsibility on developers, even though it's not possible to design a breach proof platform, their job is to make it as safe as can be, which also includes implementing visual clues and design details that lead users to make less errors. Which ideally would translate to not leaking and giving out involuntarily private information.

When it comes to mobile commerce, one of the main and important steps for gaining customer trust and attracting them is providing trust in mobile software and websites for making transactions. Trust over the mobile platforms is more critical due to the open nature of wireless networks. This was a challenge among researchers to conduct models, framework and studies about mobile commerce, trust in mobile commerce and customer issues in this type of business technology. Many studies highlight that an electronic commerce website with a greater level of trust usually gains tractions with a higher retention rate of consumer and higher degree of purchase intentions, and it is only natural.
Providing initial trust in well-designed websites leads to gaining trust from mobile customers. A variety of mobile topics in prior studies have been examined that include the impact of interface design for building trust in mobile and factors distressing the mobile commerce implementation. In design, esthetics elements take account of color, photographs, layout and font style. In gaining trust, aspects like visual esthetics or website's design esthetics should be applied in making relationship with the consumer. viewed that design esthetics impinge on superficial effectiveness and effortlessness of website application.
Evidently, M-commerce differs from traditional e-commerce in terms of its user interface and its associated risk, interactivity, ubiquity, localization services, and usage patterns. M-commerce suffers from inherent limitations of small screen size, display of information, and security of transactions; nevertheless, it also provides opportunities for making transactions on the go. It comes with usability issues and restrictions, therefore, the factors influencing trust and the consequences of trust might differ across these platforms.
The ubiquity of mobile devices encourages consumers spontaneous purchase behavior which leads to enhanced sales for the seller. However, the nature of mobile technology inherently increases the risks and uncertainty of making purchases online as it distances the user from the service provider. Consumers experience high privacy and security risks due to the transmission of transaction data in a wireless environment. Trust plays an important role in diminishing the adverse effects of risk perceptions in m-commerce.

In conclusion, researchers believe that trust is associated with perceived privacy and security [4].

2 Domain Specifications

This topic involves specifying the construct domain of perceived security by developing the theoretical definition and identifying the different conceptual dimensions. The degree to which the online buyer believes that conducting an online transaction on the seller's website is safe in a manner consistent with the buyer's confident expectations.
What are the primary relevant dimensions of perceived security?
After examining issues in security, which includes not only perceived security but also objective security. The findings reveal that confidentiality, integrity, and availability are the earliest and most widely used dimensions. Recent studies have added non-repudiation, authentication, access control, communication security, and privacy to the original triad.
Evaluating these dimensions using relevance, non-redundancy, and completeness as criteria for inclusion. Relevance refers to the dimension being consistent with the definition and characterizes the essence of perceived security. Non-redundancy refers to the fact that the dimension should not overlap with another dimension. Completeness ensures that all relevant and non-redundant dimensions have been included.
Based on these criteria, we select confidentiality, integrity, availability, and nonrepudiation as focal dimensions of perceived security [5].

Confidentiality. Confidentiality refers to the degree to which improper disclosures of information are anticipated and prevented. Systems with superior confidentiality are better able to anticipate and prevent improper disclosure of information, such as leakage of information to an unauthorized party. A system's inability to anticipate and prevent improper disclosure of information may well indicate system insecurity. Common security measures to maintain confidentiality include encryption and authentication such as password-based and token-based authentication.

Integrity. Integrity refers to the degree to which improper modifications to information are anticipated and prevented. Systems with superior integrity are better able to anticipate and prevent improper modification of information, such as faulty alteration, deletion, or addition. While some erroneous modifications of information are accidental, others may be made intentionally by unauthorized parties. Common security measures to maintain integrity include digital signatures and anti-virus programs that prevent a virus from destroying data.

Availability. Availability refers to the degree to which information is available to authorized subjects when required. Systems with superior availability are better able to consistently provide relevant information to authorized parties. Common security

measures to maintain availability include back-up systems and countermeasures for distributed-denial-of-service attacks.

Non-repudiation. Non-repudiation in a buyer-seller exchange refers to the degree to which the systems can ensure that information sent by the customer is received by the person the seller claims to be. The goal is to ensure that the seller cannot later deny a completed transaction. Systems with superior non-repudiation are better able to provide verifiable proof of identity. Digital signature is a common security measure used to ensure non-repudiation.

Dimensions dropped due to their inconsistency with definition of perceived security are authentication, access control, and communication security. These variables more appropriately represent countermeasures to protect information assets from security attacks. Privacy is also excluded because researchers tend to conceptualize privacy as being distinct from security.

Based on the framework of four dimensions, we develop a measure of perceived security as a second-order construct with four first-order formative dimensions: perceived confidentiality, perceived integrity, perceived availability, and perceived non-repudiation. The specific definition for each dimension is presented in Table 1.

Table 1. Definitions of Constructs

Constructs	Definitions
Confidentiality	Online buyer's belief that his/her transactional information will not be disclosed to unauthorized party
Integrity	Online buyer's belief that his/her transactional information will not be altered by unauthorized party
Availability	Online buyer's belief about the online seller's ability and willingness to make information available to authorized subjects when required
Non-Repudiation	Online buyer's belief that the online seller cannot afterward deny the transaction that has been performed

3 Trust factors in Mobile Commerce

In this topic it will be mentioned factors more focused on M-commerce and discussed how they affect user's feeling of security while using a mobile application, so that they will be more likely to use it again.

3.1. Technology acceptance factors

3.1.1. System quality. System quality is defined as the perceived quality exhibited in a system's overall performance. Due to the facelessness of mobile platforms, the access speed, navigation and visual appeal influence the users' first impression. Multiple m-commerce studies found that users tend to develop the high level of trust on a system when they perceive the system to be of high quality, which encourages them to spend more on that particular system.

3.1.2. Information quality. Information quality reflects the relevance, sufficiency, accuracy, and timeliness of the information provided by m-commerce systems. Users search for various information while using any m-commerce services. Inaccurate or out-of-date information undermines users' experience and signals that the system is incapable of providing timely and quality services, which further affects their trust in the system [6]. Extant research has highlighted the importance of information quality on trust in ecommerce, mobile banking, and financial services. Across different studies in m-commerce, researchers have found that trust is significantly influenced by the information quality. Thus, the following hypothesis is proposed:

There is a significant, positive relationship between information quality and trust in m-commerce.

3.1.3. Service quality. Service quality reflects the ability of a system to provide reliable, responsive, assured and personalized offerings to the users. Reliable and efficient service provides a sense of high quality which enables the users to build trust in the system [7]. Existent literature has found service quality as a determinant of users' trust. When service quality experienced by the users exceeds a certain level, users form trust as they perceive the service provider to be competent. However, untimely and unreliable services build distrust in the users about the system. Hence, we get that:

There is a significant, positive relationship between service quality and trust in m-commerce.

3.1.4. User interface. User interface in m-commerce refers to the user environment (such as menus, options, and various functions) for controlling the mobile devices. Previous studies on trust formation in m-commerce revealed that user interface is an important determinant of users' trust in the system. Well-designed user interface reduces the perceived system complexity, facilitates navigation and interactivity, and makes the users trust the system [8].

3.2. Risk factors

3.2.1. Perceived risk. Perceived risk is defined as the users' subjective evaluation of incurring losses while using a system. In 2017 researchers used perceived uncertainty as their study variable to examine the perceived risk associated with loss of privacy and security [9]. In a mobile environment, users are affected by a sense of insecurity due to potential undesirable behavior related to unauthorized access to their personal or financial data. Lack of information concerning data security makes the users hesitant of using mobile technologies as it is perceived to be risky. Research suggests that trust is affected by perceived risk.

3.2.2. Individual factor: disposition to trust. Disposition to trust remains stable over time in an individual and refers to the ability of an individual to form trust in general. Due to differences in disposition to trust, individuals tend to develop trust differently under the same circumstances. Individuals across different cultures with different life experiences differ in their disposition to trust. It is shaped as a result of personality types, experiences, and background. Several researchers in the domain of m-commerce found that an individual's disposition to trust has a direct effect on the formation of trust [10].

3.2.3. Structural assurance. Structural assurance refers to the existence of technological and legal structures that safeguard. It represents an institution-based mechanism and provides assurances related to confidentiality and protection of information. In the context of m-commerce, structural assurance in the form of promises, guarantees, regulations, insurances, and contractual terms and conditions signals credibility of the vendor and helps in building trust in the system [11]. Many prior researchers found that structural assurance leads to trust among users.

3.2.4. Ubiquity. Ubiquity refers to the ability of users to conduct business activities or transactions using their mobile devices at anytime from anywhere. Mobile technology enables users to minimize the temporal and spatial constraints by providing an opportunity to conduct ubiquitous transactions. However, ubiquitous connectivity may be hindered as a result of poor connectivity and service failures [12]. Such service interruptions lead to users' frustration and dissatisfaction which ultimately impact the user experience. Contrary to that, ubiquitous connectivity signals vendors' ability to providing efficient service which further fosters users' trust in the platform.

In conclusion, all factors discussed previously influence an individual's capability of trusting a mobile platform, specially security concepts that are meant to protect not only users but information and critical data from the sellers. Good consequences can reflect from feeling safe while using an electronic commerce platform like user satisfaction and loyalty towards a trusted platform which will translate in the likelihood of a user coming back to buy from the seller.

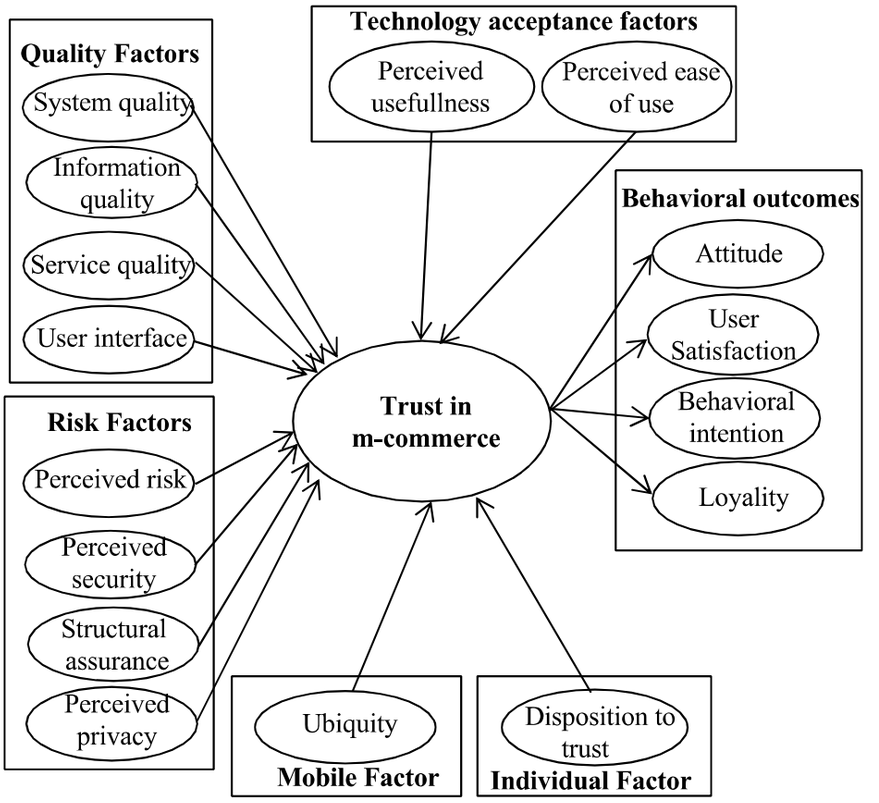

Fig 1. Relationships that influence trust

4 Defending Information Systems and E-Commerce

Defending information systems regardless of their nature is similar, the objective is keeping information secure, physically and digitally.
There are a lot of techniques to do so and this topic will only highlight a few of the security measures, dividing it into three categories: Access control, encryption, and PKI, Security in e-commerce networks, and General protection and social engineering.

4.1 Access Control, Encryption, and PKI

Access control determines who (person, program, or machine) can legitimately use the organization's computing resources (which resources, when, and how). Access control involves ***authorization*** (having the right to access) and ***authentication***, which is also called user identification (user ID), i.e., proving that the user is who he or she claims to be. Each user has a distinctive identification that

differentiates it from other users. Typically, user identification is used together with a password.
After a user has been identified, the user must be ***authenticated***. Authentication is the process of verifying the user's identity and access rights. Verification of the user's identity usually is based on one or more characteristics that distinguish one individual from another.

Biometric Systems

A biometric authentication is a technology that measures and analyzes the identity of people based on measurable biological or behavioral characteristics or physiological signals. Biometric systems can identify a previously registered person by searching through a database for a possible match based on the person's observed physical, biological, or behavioral traits, or the system can verify a person's identity by matching an individual's measured biometric traits against a previously stored version. Examples of biometric features include fingerprints, facial recognition, DNA, palm print, hand geometry, iris recognition, and even odor/scent. Behavioral traits include voice ID, and signature verification [13].

Encryption and the One-Key (Symmetric) System

Encryption is the process of encoding data into a form (called a ciphertext) that will be difficult, expensive, or time-consuming for an unauthorized person to understand. All encryption methods have five basic components: plaintext, ciphertext, an encryption algorithm, the key, and key space. Plaintext is a human-readable text or message. Ciphertext is an encrypted plaintext. The encryption algorithm is the set of procedures or mathematical algorithms used to encrypt or decrypt a message. Typically, the algorithm is not the secret piece of the encryption process. The key (key value) is the secret piece used with the algorithm to encrypt (or decrypt) the message.
Encryption has two basic options: the symmetric system, with one secret key, and the asymmetric system, with two keys.

Public Key Infrastructure

A public key infrastructure (PKI) is a comprehensive framework for securing data flow and information exchange that overcomes some of the shortcomings of the one-key system. For example, the symmetric one-key encryption requires the writer of a message to reveal the key to the message's recipient. A person that is sending a message (e.g., vendor) may need to distribute the key to thousands of recipients (e.g., buyers), and then the key probably would not remain secret. The PKI solution is using two keys, public and private, as well as additional features that create a highly secured system. In addition to the keys, PKI includes digital signatures, hash digests (function), and digital certificates [14].

Digital Signatures and Certificate Authorities

Digital signatures are the electronic equivalent of personal signatures on paper. They are difficult to forge since they authenticate the identity of the sender that uses the public key. Digital signatures are legally treated as signatures on paper.

Secure Socket Layer

PKI systems are further secured with SSL: A protocol for e-commerce. The PKI with SSL makes e-commerce very secure but cumbersome for users. One of the major protocols in use today is Secure Socket Layer), which has been succeeded by Transport Layer Security (TLS based on SSL).

4.2 Securing E-Commerce Networks

Several technologies exist that ensure that an organization's network boundaries are secure from cyberattack or intrusion, and that if the organization's boundaries are compromised, the intrusion is detected quickly and combated.

Firewalls

Firewalls are barriers between an internal trusted network (or a PC) and the untrustworthy Internet. A firewall is designed to prevent unauthorized access to and from private networks, such as intranets. Technically, a firewall is composed of hardware and a software package that separates a private computer network (e.g., your LAN) from a public network (the Internet). Firewalls are designed mainly to protect against any remote login, access by intruders via backdoors, spam, and different types of malware (e.g., viruses or macros). A popular defense system is a DMZ. The DMZ can be designed in two different ways, using a single firewall or with dual firewalls [15].

The Dual Firewall Architecture: The DMZ

In the DMZ architecture (DMZ stands for demilitarized zone), there are two firewalls between the Internet and the internal users. One firewall is between the Internet and the DMZ (border firewall) and another one is between the DMZ and the internal network. All public servers are placed in the DMZ (i.e., between the two firewalls). With this setup, it is possible to have firewall rules that allow trusted partners access to the public servers, but the interior firewall can restrict all incoming connections.

Virtual Private Networks (VPNs)

A virtual private network refers to the use of the Internet to transfer information, but in a more secure manner. A VPN behaves like a private network by using encryption and other security features to keep the information secure. For example, a VPN verifies the identity of anyone using the network.

Intrusion Detection Systems (IDS)

No matter how protected an organization is, it still can be a target for attempted security attacks. For example, most organizations have antivirus software, yet they are subjected to virus attacks by new viruses. Therefore, an organization must continually monitor for attempted, as well as actual, security breaches. The monitoring can be done by using intrusion detectors. An intrusion detection system (IDS) is a device composed of software and/or hardware designed to monitor the activities of computer networks and computer systems in order to detect and define unauthorized and malicious attempts to access, manipulate, and/or disable these networks and systems.

Dealing with DoS Attacks

DoS attacks are designed to bombard websites with all types of useless information, which clogs the sites, detecting an intrusion early can help. Since there are several types of DoS attacks (e.g., DDoS), there are several defense methods. Intrusion detecting software (mentioned previously) also identifies the DoS type, which makes the defense easier and faster [16].

4.3 General Protection, Spam, and Social Engineering Controls

The objective of IT security management practices is to defend information systems. A defense strategy requires several controls.

The major types of controls are: (1) General controls, which are designed to protect all system applications. (2) Application controls guard applications. In this and the following sections, we discuss representative types of these two groups of information system controls. Later in the section, we cover spam and fraud mitigation.

Protecting Against Spam

Sending spam that includes a sales pitch and looks like personal, legitimate e-mail and may bypass filters is a violation of the U.S. Controlling the Assault of Non-Solicited Pornography and Marketing (CAN-SPAM) Act of 2003. However, many spammers hide their identity by using hijacked PCs or spam zombies to avoid detection and identification. For protecting your system against botnet attacks, which also spread a huge volume [17].

Business Continuity and Disaster Recovery

Disasters may occur without warning. A prudent defense is to have a business continuity plan, mainly consisting of a disaster recovery plan. Such a plan describes the details of the recovery process from major disasters such as loss of all (or most) of the computing facilities or the data.

Example: Hospital Paid Ransom after Malware Attack Hollywood Presbyterian Medical Center paid a ransom of $17,000 in Britain (so the) blackmailer-hacker cannot be identified. The hacker encrypted the data that were not

backed up. The hospital failed with its disaster recovery plan, so there was no choice (per the hospital management) but paying the ransom [18].

4.4 Why Is It Difficult to Stop Internet Crime?

The following are the major reasons Internet crime is so difficult to stop.

Making Shopping Inconvenient: Strong EC security may make online shopping inconvenient and may slow shopping time as well. Therefore, shoppers may not like some security measures
Shoppers' Negligence: Many online shoppers are not taking the necessary (but inconvenient) precautions to avoid becoming victims of identity theft or fraud.
Design and Architecture Issues: It is well known that preventing vulnerability during the EC design and pre-implementation stage is far less expensive than mitigating problems later; unfortunately, such prevention is not always made.
Ignoring EC Security Best Practices: Many companies do not have prudent IT security management or employee security awareness. Many widespread threats in the United States stem from the lack of user awareness of malware and hacking attacks [19].

5 Conclusion

In this paper the issue of e-commerce and m-commerce security was investigated, not only from the developer perspective, but also keeping in mind the user experience and their requirement for a platform to be trusted.
In addition, there were clarified many terms that are often used when talking about security in computer science, and more specifically what they differ when compared in m-commerce vs e-commerce.
Comprehending the topics on this study it is fair to state that as long as the internet remains insecure, it is virtually impossible to authenticate the other party to a transaction.
In conclusion, digital security is an ongoing evolving subject, and every day there are new methods to exploit breach platforms but there are also new ways to defend them, and all signs lead to it remaining this way.

References

1. E-commerce statistics for individuals, Eurostat from Information and communication technology, 2019
2. Popularity contest between E-Commerce and Traditional Retail Business, from International Journal of Technology for Business, 2019
3. Mehrbakhsh Nilashi, Othman Ibrahim, Vahid Reza Mirabi, Leili Ebrahimi, Mojtaba Zare.: "The role of Security, Design and Content factors on customer trust in mobile commerce" in Journal of Retailing and Consumer Services, 2015
4. Subhro Sarkara, Sumedha Chauhan, Arpita Khare.: "A meta-analysis of antecedents and consequences of trust in mobile commerce" in International Journal of Information Management, 2019
5. Edward Hartono, Clyde W. Holsapple, Ki-Yoon Kim, Kwan-Sik Na, James T. Simpson.: "Measuring Perceived Security in B2C Electronic Commerce Website Usage: A Respecification and Validation" in Decision Support System, 2014
6. Silic, M., & Ruf, C. The effects of the elaboration likelihood model on initial trust formation in financial advisory services. International Journal of Bank Marketing, 2018
7. Wang, W., Ou, W., & Chen, W. The impact of inertia and user satisfaction on the continuance intentions to use mobile communication applications: A mobile service quality perspective. International Journal of Information Management, 2018
8. Stewart, H., & Jürjens, J.: Data security and consumer trust in FinTech innovation in Germany. Information and Computer Security, 2018
9. Rana, N. P., Barnard, D. J., Baabdullah, A. M. A., Rees, D., & Roderick, S.: Exploring barriers of m-commerce adoption in SMEs in the UK: Developing a framework using ISM. International Journal of Information Management, 2019
10. Matemba, E. D., & Li, G. Technology in Society Consumers' willingness to adopt and use WeChat wallet: An empirical study in South Africa. Technology in Society, 2018
11. Oliveira, T., Faria, M., & Abraham, M.: Extending the understanding of mobile banking adoption: When UTAUT meets TTF and ITM. International Journal of Information Management, 2014
12. Lin, H.-F.: An empirical investigation of mobile banking adoption: The effect of innovation attributes and knowledge-based trust. International Journal of Information, 2011
13. Wang, S. W., Ngamsiriudom, W., & Hsieh, C.: Trust disposition, trust antecedents, trust, and behavioral intention. Service Industries Journal, 2015
14. Scott, J. Cybersecurity 101: What You Absolutely Must Know! - Volume 1: Learn to be Pwned, Thwart Spear Phishing and Zero Day Exploits, Cloud Security Basics, 2016
15. Teo, F. "Monitoring Your Internal Network with Intelligent Firewalls." Enterprise Innovation, 2016.
16. Teo, F. "Monitoring Your Internal Network with Intelligent Firewalls." Enterprise Innovation, 2016
17. Alison Quine in: "How to Prevent Denial of Service Attacks", 2008
18. Lenovo. "Lenovo Recommends 15 Steps to Reducing Security Risks in Enterprise Mobility." White Paper, 2013.
19. Smith, C. "It Turns Out Target Could Have Easily Prevented Its Massive Security Breach." March 13, 2014. bgr.com/2014/03/13/targetdata-hack-how-it-happened, 2016