E-Commerce Security Issues, Then and Now

Thoughts Stimulated by an Historic Paper by Dez Blanchfield (2000) on E-Commerce Security

Graham Shepherd
Life Member, TelSoc

Abstract: Simon Moorhead's recent historical reprint (December 2024) revisiting Dez Blanchfield's December 2000 paper in *TJA* on e-commerce security has stimulated this author to make additional comments on the weaknesses of major websites and of email systems today in permitting fraud and deception, in comparison to 24 years ago.

Keywords: Internet security, e-commerce, phishing, spam

Introduction

Simon Moorhead's paper 'e-Commerce Security Revisited' (Moorhead, 2024) has usefully drawn our attention to the astute warnings by Dez Blanchfield (Blanchfield, 2000) in this *Journal's* predecessor, the *Telecommunication Journal of Australia*, concerning the dangers of designing online systems without sufficient regard to security.

Moorhead's introduction to the historic paper, and Blanchfield's original, have stimulated this reviewer to make some additional observations on the hazards of some current practices in the operation of both consumer websites and email. The History section editor of the *Journal*, Peter Gerrand, suggested that these observations deserved publication as a companion paper, despite its slimness.

The Dangers of Outsourcing Security

Practically no e-commerce sites today, except the very big ones like Amazon and Google, use their own internal security systems for transactions. Most sites, even big ones, pass the buyer off to a renowned gateway, such as PayPal, Stripe, Square, or one of the big banks. In the process, credit card numbers never get transmitted through or stored on the e-commerce site. To a large extent, the e-commerce sites are passing off this part of the risk to the gateway for

https://doi.org/10.18080/jtde.v12n4.1182

a small fee per transaction. The big risk remaining for these sites is securing personal details, particularly names, email and physical addresses, and phone numbers. The website software alone must protect this information or avoid saving it. This is still a bane for website administrators, who have to choose from a small number of highly secure Content Management Systems to do that hard work and to keep up-to-date. Weekly updates would be the norm, indicating that the author of the original paper was very perceptive about the growing scale of the problem.

Vulnerability to Phishing and Spamming

Today, this is where phishing and spam emails come in. They rely on huge email address lists stolen by specialist hackers. This way only a few consumers need to be hooked to make a big payoff. Companies, on the other hand, pay the price in ransom demands and reputation. The scale of this problem in 2022 was that an estimated 3.4 billion spam emails were sent every day, that is, over 48% of all emails. Of this number Google blocks only 100 million per day, barely scratching the surface (https://aag-it.com/the-latest-phishing-statistics/). In 2022 the number of ransomware attacks in the United States alone amounted to around 217.5 million (https://www.statista.com/statistics/1377918/ransomware-target-countries/). Australia has not been free of the problem: e.g., Optus, Medicare, Canva, ANU etc. (https://www.upguard.com/blog/biggest-data-breaches-australia/).

Poor Verification of Email Sources

Whilst most Internet protocols are subject to constant upgrading to stay ahead of the game, email remains a very weak link.

The email protocols SMTP (client) and IMAP and POP (server) have been around for a very long time and have only been patched in simplistic ways to try and verify that an email comes from whom it purports to be: for example, DMARC (Domain-based Message Authentication Reporting & Conformance), SPF (Sender Policy Framework) and DKIM (DomainKeys Identified Mail) records are (often, but not always) attached to the domain name server (https://dmarcian.com/). Most spam still gets through. The telecommunications operators who once invested heavily in standards have largely abandoned the field to the vendors, who have less interest in keeping the traffic on the Internet valid, perhaps the opposite. The email service providers, like Google, Apple Microsoft and Yahoo, have a poor record and little interest in collaboration and so the patches have come from smaller players with smaller impact.

https://doi.org/10.18080/jtde.v12n4.1182

Shifting Risk onto the Customer

At about the time the original paper was being written, banks were closing branches and shifting as many transactions as possible online. The risk for them was loss of confidence if their security systems were breached, particularly by hijacking a credit card number. In the early days they bore that risk and usually refunded the buyer (not the vendor because they needed the warning to sort their systems out). However, the banks have largely stopped accepting this risk, so the old saying, "buyer beware", is still very pertinent.

Recommendations

The huge growth in both the good and malicious uses of the Internet has focused attention on how critical cybersecurity is for our ordinary everyday lives. The Internet Engineering Task Force (IETF) is the premier standards development organisation for the Internet, but by design it is entirely voluntary, has no membership, nor does it enforce compliance (https://www.ietf.org/). Email is amongst the technologies it addresses, including DMARC mentioned above, and a new protocol, JMAP (JSON Meta Application Protocol), to replace IMAP (one day, if sufficient service providers take it up). However, security and trustworthiness of email for consumers and businesses do not appear to be considered matters of great urgency at the moment. The Internet Society also has a mission addressing "the development of the Internet as a global technical infrastructure, a resource to enrich people's lives, and a force for good in society" (https://www.internetsociety.org/).

Another approach to trust is blockchain technology, which creates direct "trustless" (as opposed to "untrustworthy") contracts directly between users. But blockchain is a long way from achieving a central place in e-commerce and has its own problems, such as enormous energy usage, its avoidance of government regulation and its attraction to speculators and money launderers.

Fixing email remains the most attractive path for solving the problem.

The ICT (information and communication technology) industry would seem to be the best lobby group to initiate the requirements definition and development (within the IETF) of a much more robust email protocol to replace the aging IMAP and its associated protocols. Australia has a number of active ICT industry bodies which collaborate on major issues, including TelSoc, the Australian Computer Society (ACS), The Pearcey Foundation and the Australian Information Industry Association (AIIA). Sponsorship for a series of forums on this subject could be sought from the telcos, banks, Google, Microsoft and others, with the aim of developing a new and evolving set of protocols to address this challenge.

https://doi.org/10.18080/jtde.v12n4.1182

References

Blanchfield, D. (2000). e-Commerce Security – It's not an oxymoron!! *Telecommunication Journal of Austr*alia, *50*(4), 13–18.

Moorhead, S. (2024). E-Commerce Security Revisited, *Journal of Telecommunications and the Digital Economy, 12*(4), 178–185. https://doi.org.10.18080/jtde.v12n4.1167