E-Commerce Security Revisited

Simon Moorhead
Telecommunications Manager

Abstract: The *Journal* revisits an historic paper from 2000 flagging the potential security risks in e-commerce systems.

Keywords: History of Australian Telecommunications, e-Commerce, Security

Introduction

It is appropriate to reprise the historic paper (Blanchfield, 2000) on e-commerce security, given the significant number of online scams and fraudulent transactions occurring today. The paper was written over twenty years ago and warns of the implications of assuming security is someone else's problem, to be fitted separately outside the usual e-commerce software build cycles.

The paper recommends a pro-active rather than a reactive response to security. Often a standard design that is considered safe can contain one or more Achilles' heels that can be exploited by outsiders. Designers need to do more to ensure the security and testing of "our new and shiny house of cards".

The paper gives examples of contemporary security breaches in both government (Australian Taxation Office) and commercial (Sanity Entertainment) e-commerce systems that were supported by evidence in external links (which, unfortunately, are no longer working, given the age of the original paper).

However, a search today reveals an SBS news article (Webster, 2024) from August 2024 describing that the Australian Ombudsman has reported that "hackers were exploiting Medicare and Centrelink accounts through the myGov platform by linking them to bogus myGov accounts and making bogus tax claims worth thousands of dollars, or falsely claiming support payments" (Webster, 2024, second paragraph).

The historic paper also provides some sobering scenarios related to credit card fraud and the hijacking of websites to perpetuate credit card fraud – the takeaway being: it is much easier to

https://doi.org/10.18080/jtde.v12n4.1167

secure your e-commerce platform up front, rather than suffering the human resources cost of dealing with angry customers and the related fraud investigation and rectification.

It was difficult for the author to cover the necessary e-commerce security at a technical level, given the confines of the paper. However, he hoped to do the next best thing and "change your view on the effects of not taking into account the broader security aspects of eCommerce when considering planning, designing, and building your current or next exciting project" (Blanchfield, 2000, p. 18).

References

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

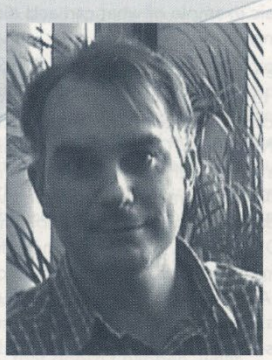
Webster, M. (2024, August 9). Revealed: How fraudsters steal from Australians through a myGov's 'side entrance'. SBS News. Available at https://www.sbs.com.au/news/article/revealed-how-fraudsters-steal-from-australians-through-a-mygov-side-entrance/8bqh9jx2c

https://doi.org/10.18080/jtde.v12n4.1167

The Historic Paper

e-Commerce Security — It's not an oxymoron !!

Dez Blanchfield



Dez Blanchfield

It is necessary to consider the possibilities of the less technical aspects of eCommerce security, and some of the peripheral aspects, which are certainly just as relevant.
Many projects are well into the development or build cycles before the security issues are even considered.
Reactive rather than pro-active response to security is not recommended. All too easily, in what might have been considered a safe, secure design, we find that perhaps we might not have done all we could, or perhaps should, to ensure the security of this shiny new house of cards.
Some illustrative examples and scenarios are described to help understand the unpleasant possibilities.

PERCEPTIONS OF SECURITY

I recently overheard a friend replace their all time favourite oxymoron one line joke 'military intelligence' with 'eCommerce security'. Upon hearing this, I knew all was not well with the state of eCommerce 'public perception'. Consider the fact that this friend doesn't actually know what the 'e' in electronic commerce actually means, and you get the idea that we might have a problem, if only perception. ..It's still an issue which requires our attention.

It's time we let our minds wander and consider the possibilities of the less technical aspects of eCommerce security, and a few of the peripheral aspects, although less technical and nerd driven, certainly just as relevant.

All too often, when talking about eCommerce, invariably the term 'security' is thrown in for good measure, almost like that dash of salt or pepper in any good pasta sauce. But when it comes to dealing with the topic in the real world of delivering solutions, even the best of us are all too often far from what might be considered ideal.

The difficulty we all face when considering what security implications a given project might have, is that all too often the term security is placed off to one side, as a component to be fitted in somewhere. Many projects find themselves well into the development or build cycles before the security issues are even considered.

How many projects throw the term security into project plans and design documents, to ensure that we can demonstrate that they have covered the issue, that they have complied with some often unwritten set of standards pertaining to security?

'Security — that's somebody else's problem. I just have to get this thing working, then I'll deal with security..'. Sound familiar?

It isn't only when some hard case, often from the anonymous 'other' side of a computer screen, manages to weed out some previously unconsidered Achilles heel, we get the point.

Reactive rather than pro-active response to security is not recommended. All too easily, in what might have been considered a safe, and secure, design, we find that perhaps we might not have done all we could have, or perhaps should have, to ensure the security of our shiny new house of cards.

Sure, I can hear you scoffing already. 'Give me a break', I hear you say. 'Not my project, we know what we're doing, we wrote the book'. Is that what you're thinking? That zillion dollar project you just completed, it's leading the world in its brilliance, the press releases said so, right, but is it secure? Are

Journal of Telecommunications and the Digital Economy, ISSN 2203-1693, Volume 12 Number 4 December 2024

https://doi.org/10.18080/jtde.v12n4.1167

you sure, are you really sure? Even if you are, check again, please!

SOME EXAMPLES

It happens to the best of us. Let me give you a couple of recent examples, right here in our own back yard.

Example #1:

One of the highest profile World Wide Web sites we've seen in years, the Australian Tax Office (ATO) GST Assist program online is a classic example of what can and did go wrong.

When building an online eCommerce web site to better manage the process of allocating Australian Business Numbers (ABNs), the ATO unfortunately managed to miss some of the basics. It took a moment of fiddling for someone to stumble over a fundamental, but disastrous hole in the ATO's web site. Subtracting the value of one (1) from the account ID allocated to you by the ATO's web site, would give you the full details registered by the person who subscribed one session before you!

A bright young fellow by the name of Kelly managed to do just that. ..A self confessed 'non-hacker' (no hacking was required), Kelly, by merely adjusting his ID in the web page URL, was able to gain access to the confidential details of at least 17,000 taxpaying entities registered via the ATO site.

Kelly was able to gain access to business phone and fax numbers, postal addresses, all bank account details, and email addresses.

Kelly sent emails to most of the 17,000 people and companies whose details he had accessed, to let them know that they too had a problem. ..Imagine the nightmare the ATO had on their hands! A world leading solution to one of the government's more difficult challenges in recent years, and what should have been text book stuff for all the right reasons, became text book stuff for all the wrong reasons.

Before you choke from scoffing, review what the Sydney Morning Herald had to say about it at
http://www.smh.com.au/news/0006/29/update/news2.html
and get the full story.

Example #2:

Internet users swamped the brand new Sanity.com music web site registering for the chance of winning a free music CD – unfortunately the folks at Sanity apparently shipped quite a few free CD's before realising they had a problem. It seems the ordering process kindly permitted some customers to order CDs without having to provide their credit card details as part of the purchase process. ..Sure you can turn this into a publicity stunt, but at what cost?

Did I hear you scoff once more? Surely not, well ok, take a moment to go visit
http://www.internetnews.com/intl-news/article/0,,6_245621,00.html
and then come back and tell me that you're not thinking about eCommerce security.

Now I hate to say this, but I actually could go on like this for hours and hours. But filling this short article with war stories from the bleeding edge of business via the World Wide Web under the guise of eCommerce, isn't going to hold your interest for long.

Almost every article I've read about doing business online, and in particular about security issues facing eCommerce development, tends to be littered with the IT industry's staple diet of three letter acronyms (TLAs) and jargon such as SSL, SET, digital signatures, digital certificates, smart cards, private key encryption, etc.

I think we've all had enough of the jargon and TLAs, of nicely detailed colour graphics showing the flows and processes of how Netscape's Secure Sockets Layer (SSL) protocol works and why you would need one. If you haven't had enough of it, go visit Netscape's home page, they are dying to tell you all about it.

I've found far too few quality articles about the fundamentals, the actual 'low tech' behind the scenes, as it's more often than not the little things that trip you up. Sure, you may have super computer power running your web server but the absolute basics, such as your registered domain name, or the software you are using on your web server, the naming of your sites on that server, how people login to that server and such, are critically important.

Issues like 'plain text log files'; 'public networks being used for messaging; local area network vulnerabilities; open ports on Ethernet switches; unlocked communications racks in data centres; unshredded printouts of consignment orders; and shipping details being dropped in trash cans.

False 'mirror' web sites under similar domain names to yours, of email addresses like sales4yourcompany@yahoo.com and the like – are these things taken care of?

I'm of the opinion that what is needed currently, is a great deal more open forum style discussion of the fundamental issues we face in eCommerce today.

Journal of Telecommunications and the Digital Economy, ISSN 2203-1693, Volume 12 Number 4 December 2024

https://doi.org/10.18080/jtde.v12n4.1167

The more the fundamental issues are debated openly, the sooner we can deal with them and hopefully re-educate those of us who too easily throw in a quick patch up, rather than solve a serious issue right up front. ..It's the fundamentals that often trip us up; technology is making it harder to see the delimiting lines. Those lines are getting more and more grey by the day, and the guys in the black hats look more and more like you and me.

Certainly pressures such as economics, time and politics in even small firms can force us to grey the lines a little, but that's often when we should be on our toes more than ever.

Perhaps it's primarily a case of education on both sides of the browser? Let's talk through an example of some of my current favourites, you might be surprised by this simple little story.

Recent research conducted by Citibank indicates that 60 percent of Australians still do not trust the Internet with their credit card details.

That same 60 percent said they would gladly provide their credit card details over the phone to pay for a purchase made on an Internet world wide web site. Oh no!

Most folk I tell this to simply nod their heads in agreement, even the die-hard geeks. Almost all say that they don't trust the systems currently being used online to take payments.

Even when an SSL enabled server is handling the transaction, and their World Wide Web browser reports that the link is secure by displaying a safely 'locked' session with a nice little icon on the screen too! Gosh!

I choke at this and ask how they feel about some young kid, let's call him little Johnny, on the other end of the phone writing down their own personal copy of your details as they enter them into a computer database to record the purchase, over a computer network.

A CAUTIONARY TALE

What happens if that credit card is used, let's say by our same little Johnny, to make a purchase over the phone, of some shiny new music CD's. Being a cunning little fellow, he makes arrangements for them to be delivered to a false address, where little Johnny might be sitting on the steps of a stranger's house waiting to sign for the delivery. He then gets on his razor scooter and rides off into the sunset, chuckling all the way listening to his new CD's.

OK, so you get your credit card statement in the mail. If you're diligent, you pick it up and get on the phone with the bank, they make you go down to your branch, fill out a declaration stating you did not make that purchase. Some 24 hours later the money gets put back into your account by the bank, and is taken out of the merchant's account.

So if you are the owner of the credit card, you don't lose, the merchant does, which is fine, that is unless you're the merchant.

More than likely, if you are like most of today's modern lifestyle society, you won't notice a $29.95 purchase on your statement under 'Sanity Online', as you won't have paid your account with the first notice from the bank. When the second 'late' notice comes through without a detailed statement, you panic like the rest of us, and hurriedly pay your monthly bill just hoping they don't take your card away.

Either way, little Johnny got his free CD and is now enjoying it with his pals, with the volume turned all the way up to eleven.

'Yeah, sure, that doesn't happen, what rubbish' I hear you say.

Well consider this scenario:

Scenario #1:

Picture an Internet Service Provider (ISP) who has an eCommerce-enabled subscription form. Our little Johnny uses your stolen credit card details to pay this same ISP for an Internet dialup access account. He connects to the ISP's home page, clicks on 'join', chooses the flat fee monthly account at $29.95 for unlimited access. The ISP web page lets Johnny enter the basic details the ISP needs for login, password, and payment details, including your credit card number and expiry date. (These are the same details you provided when you purchased that pizza, remember).

Because Johnny is a bright kid, he makes sure he clicks on 'receive invoices by email', so now the ISP will email the monthly accounts to 'gotcha' via the ISP's email server rather than sending them to a postal address. A postal invoice would be a problem as it could be traced or would be sent 'Return To Sender' possibly if it went to a false address, but our Johnny isn't that silly.

Johnny signs up with the login 'gotcha' and off he goes, one month's free Internet access.

It doesn't sound like a big deal to most of us — that one little $29.95 a month Internet account, but if you end up with even ten

Journal of Telecommunications and the Digital Economy, ISSN 2203-1693, Volume 12 Number 4 December 2024

https://doi.org/10.18080/jtde.v12n4.1167

people doing this each month for let's say three months each, that's around $89.95 per person, and a total of $899.50 per month. Multiply that by three months and you get a total of $2,698.50 per quarter.

Now factor in the human resource time to deal with it:

- a receptionist taking the angry phone calls as they come in
- accounts admin staff handling the enquiries
- technical support and admin staff providing answers to the accounts admin staff
- finance staff sorting out the billing issues as well as the on-flowing effect to cash flow
- financial management dealing with the bank who took money from the company account
- company management answering bank requests for an explanation to what the bank sees as ongoing wrongful billing
- marketing and sales management
- marketing communications staff team dealing with any press which might arise

and it goes on. Certainly I've stretched it a little to illustrate the point, but here's the moral of this little story:

A single phone call to the card holder's phone number provided with the order online to perhaps confirm the purchase, or even better, to provide the login name and password as well as confirm the order, would have saved that ISP almost immeasurable cost and resource.

I consider this to be just a tiny part of what can only be considered a step in an eCommerce security procedure. Surely one, which at $0.40c per phone call, would be an enormous saving to that business.

While running an ISP myself, I regularly had a pile of uncollectable invoices placed on my desk each month. This was a reminder that we had ongoing problems like this – last tally I recall the total of uncollectable or bank-recovered credit card billing to be around AUD$114,000 over 12 months, and I am of the opinion that we ran a very tight ship. I should note that the $114,000 was the sum of the invoices — it did not take into account the peripheral costs of human and technical resources incurred to reach that cost.

The problems faced when considering eCommerce security are not just those found behind the black boxes selling you goods —, consider the issues for the unwary traveller on the internet for a moment and you will quickly see yet another mine field.

Let's consider some of the less considered traps a new web venture might fall prey to.

Consider this scenario (the company name has been changed so I don't get sued!):

Scenario #2:
To register that all important DOT COM domain name for your Internet start-up you just need a valid credit card and email address.

So, little Johnny pops into the scene once more. Johnny jumps on the Internet with his dad's home computer. He again chooses to use the credit card details you gave him 'securely' over the phone while ordering those pizzas for the recent late night with the sales team planning your next eCommerce project.

Johnny pops on over to the web site http://www.networksolutions.com/ where it takes him around five minutes to register MelodyMusic.COM which Melody Music Company Pty Limited hasn't yet registered – they are happy with Melody.COM which they are currently using.

To activate his newly-registered domain name Johnny jumps onto a free web site network like GeoCities, which is sponsored by Yahoo! He signs up for a free web page, with his own domain as the address, and agrees to have Yahoo! place banner advertising on his free web site to let the nice folk over at Yahoo! recover their running costs in providing this wonderful service of free web sites.

A little web page editing later, Johnny now has a free web page online. It's actually a copy of Melody.COM – Johnny is a smart kid, he just copied the original HTML source code right off the home page from Melody.COM.

Five minutes' worth of cutting and pasting from his browser, which has this neat feature of allowing visitors to 'View Source' from your page, and Johnny has uploaded Melody.COM's home page to his MelodyMusic.COM Web site. Oh yes, Johnny had to make allowances for that silly free pop-up banner ad in the upload, but he's a HTML guru as a result of a TAFE computer course his parents recently paid for, so a few layout changes to the site took another five minutes, no big deal.

Now this is where you enter the scene – it would be no fun if you didn't play a part, so I've included you – just for fun.

You get on the web; you've just finished

Journal of Telecommunications and the Digital Economy, ISSN 2203-1693, Volume 12 Number 4 December 2024

https://doi.org/10.18080/jtde.v12n4.1167

reading about the Melody Music Company and their wonderful new eCommerce enabled web site in the Financial Review, and you figure you might go and buy that Kylie CD you've heard so much about.

You can't recall the address or URL of the site, and Mary down the hall has pinched the Financial Review and taken it to lunch to read, so you pop on over to your favourite internet search engine http://www.WebSearch.com.au and go hunting for the Melody music web site.

What you don't know at this stage is that our little Johnny has had the foresight to pop on over to http://www.jimtools.com and use their neat free Internet site registration utility. He just typed in his Internet World Wide Web page address (or URL), and through the magic of computers, MelodyMusic.COM gets submitted to over 8,500 Internet search engines and directories like WebSearch.COM.AU and Yahoo! where it's sure to be found.

Melody Music Company Pty Limited and their Melody.COM have not submitted their site to any online directories or search engines, and so it's not likely that their site will be found by anyone searching for them in the likes of the directories provided by LookSmart, or Yahoo! or search engines like WebSearch.COM.AU, Altavista or similar.

You, meanwhile, unwittingly search for Melody Music on good old http://www.WebSearch.COM.AU and hey presto, they find MelodyMusic.com which looks like the site you wanted, so you click on the link and off you go.

WebSearch.COM.AU is one of the 8,500 search engines and directories that are capable of accepting automatic site submissions from places like Jimtools.COM, so within 24 hours of little Johnny using Jimtools.COM the bogus Melody Music web site will appear in the WebSearch.COM.AU search engine.

So, now you are connected to the MelodyMusic.COM World Wide Web site, and it looks great. Right there on the front page, they have lots of copies of that new Kylie CD you wanted, so you immediately click on ADD TO SHOPPING CART, then you click on CHECKOUT, and start punching in payment and delivery details.

Johnny again has had the wisdom to use the free secure payment services (SSL). Johnny chooses to use a service provided by a great bunch of folks he found on an adult pornography site. A payment gateway service company called EasyPaymentGatewayServices Inc.

EasyPaymentGatewayServices Inc will let Johnny use their payment gateway and SSL servers for a small fee of just 15% of any transaction made through his web site MelodyMusic.COM. What a fantastic service. No set-up fees. Just sign up on line and you're ready in 5 minutes!

There is a further benefit of using EasyPaymentGatewayServices Inc. It turns out that EasyPaymentGatewayServices Inc likes their 'affiliates' to spend their earnings online.

So the folk over at EasyPaymentGatewayServices Inc will let Johnny redeem his payments online through their network of other affiliated web sites.

So Johnny now can spend his earnings from online CD sales through his bogus copy of the Melody Music Company web site, by spending it online with World Wide Web sites affiliated with EasyPaymentGatewayServices Inc.

The great thing about this whole set-up of course is that at no stage does our cunning little Johnny have to transfer his fraudulently earned income to a bank account in his or any other traceable name. Everything is online, it's virtual, and practically impossible to back step to an actual human.

Oh, guess who just happens to be an affiliate site to EasyPaymentGatewayServices Inc. Yes, you guessed it. None other than our friends over at the Melody Music Company and their site Melody.COM!

Now this is really getting interesting.

After a few days, Johnny has loads of credit, as a result of his bogus sales to you and thousands of others which he sent SPAM email to, as part of launch of his bogus web site.

So once again, our little Johnny is sitting on yet another set of random house steps, where the owners are away. He has taken the day off school, he has to sit and wait for the courier to deliver his box of 50 CD's he ordered from Melody.COM – why go to school, he's too smart to waste the day at school anyway – there's some serious eCommerce to be done!

God help that US firm taking the payments online for Johnny, and for Melody Music Company who can't work out why whole boxes of CD's get delivered and signed for by Mr Gotcha Smith, time and time again. As for the fulfilment house, they are still trying to read the signature, seems it looks a little like 'Gotcha Again' but it's not easy to read.

Journal of Telecommunications and the Digital Economy, ISSN 2203-1693, Volume 12 Number 4 December 2024

https://doi.org/10.18080/jtde.v12n4.1167

And as for the residents at #1 Gotcha Street where little Johnny had the CD's delivered — well they are still filling out the statutory declaration forms for the police, and everybody's getting a little flustered!

Now there's the matter of you not getting your CD's some weeks after you placed your order. You still don't realise of course that you've been interacting with the false site.

Of course you placed an order with little Johnny's copy of the Melody Music site, not the real one, but you won't realise this until you get weird responses from the 1800-MELODY-HELP phone support service. They of course have no record of your purchase.

In fact, due to the fact that 1800-MELODY-HELP is outsourced to a call centre, they are invariably not Internet savvy. Because MelodyMusic.COM sounds like what they have on their 'script' to follow when trying to help you, they don't pick up the significance of the different URL while talking to you on the phone.

As far as 1800-MELODY-HELP are concerned, you're some crank on the phone screaming at them because you think you purchased a CD online. They can't see you in the purchasing system; they simply tell you that it's impossible that you made any such order, and apologetically they advise you to check that you visited the correct site, and hang up, click!

Now if that second scenario doesn't give you something to think about, perhaps you shouldn't be considering eCommerce.

Unfortunately, it would be difficult for me to cover eCommerce security at a technical level, even in brief detail within the confines of this article. I'm still working on the book. So I've hoped to do the next best thing, that is, change your view on the effects of not taking into account the broader security aspects of eCommerce when considering, planning, designing and building your current or next exciting project.

If I can have achieved one thing here, I hope it is to have you re-consider what you previously understood to be the scope of eCommerce security at the very least, and hopefully given you reason to open your browser and go hunting for further reading on the topic.

THE AUTHOR

Des Blanchfield has 16 years of experience in IT, in most aspects of software, systems, and telecommunications from development to implementation, from hands-on to management. Currently Dez is a consultant to a select few eCommerce and Telecommunications firms in Australia, New Zealand and Hong Kong. Key areas of interest over the past few years have seen Dez develop technologies in Clustering, Network Redundancy, Systems, Network and eCommerce Data Security, Firewalls, Load Balancing, Content Servers, Search Engines, Ad Serving Engines, and Remote Monitoring. He may be contacted at:

dez@blanchfield.com.au

https://doi.org/10.18080/jtde.v12n4.1167