

Breaking up with your identity: it's not me, it's you!



Nathan Pearce, 2014-06-01

Let me tell you why I'm glad my gran is not on the Internet. When it comes to technology security most of my experience is with customers: with other peoples systems, not mine. However, today I write about a personal experience that scares me a little.

I signed up for a Gmail account back when it was an invitation-only beta service. My first impression of it was nothing short of wow! This exclamation inspired by its simplicity, and the fact that it offered an enormous amount of free space. I recall being impressed by that fact that in a time of rapid innovation the Gmail team weren't trying to do too much with it. I think it was the first time I was able to describe a web-based service as being humble and don't think I've seen anything like it since, until maybe [Medium](#).

Over the years my relationship with Google grew to include Google Docs, Google Sites, Analytics and even 'Google Apps for Your Domain'. Our relationship blossomed – not quite [this](#) far, but we were on a good thing.

Being an early adopter often means getting first pick of your account name and avoiding the dreaded nathanpearce1234. One cannot win all the time and I don't always get my way but occasionally there is room for compromise. For example, when I signed up for Twitter, @NathanPearce was already taken. Consequently, and like many others, I reversed my name and have been happily tweeting from @PearceNathan for a few years now. It did weird me out a little when @NathanPearce followed me earlier this year (are you reading this post, @NathanPearce?). For the sci-fi fans: fortunately, I didn't implode, burst into flames or leap to a parallel universe at this occurrence.

I've managed to come to terms with the fact that there are a number of people in the world named Nathan Pearce. Mum, you were wrong! There's a Nathan Pearce working at Sony Entertainment, another is a web savvy 9 year old, and then we have the most interesting Nathan Pearce of all – the web-challenged, heavy-metal loving, corn farmer. And it's not just his music and farming preferences I'm familiar with. I also know where he travels, his preferred dating sites (a niche farmer-friendly service) and a number of other interesting factoids. How do I know all this? Because Nathan-corn-metal, as he will be known hereafter, keeps providing my email address to people thinking that it is his own.

Before you start speculating as to how this mishap can occur, a lesser-known fact about Gmail is how it handles a period before the @ symbol. With Gmail, the following email addresses are all the same:

firstlast@gmail.com

first.last@gmail.com

f.irstlast@gmail.com

And, so on. I've heard of some clever people using this to their advantage: providing one format for family, another for shopping on-line, etc., and then using Gmail filters to file (delete) messages as appropriate. So, I can confirm that this isn't a simple formatting mistake. Nathan-corn-metal believes that my email address [are belong to him](#). This mistake (delusion) might seem trivial to some but has also lead to a few interesting circumstances.

Email confirmation

Nathan-corn-metal does get on the net from time to time. My first interaction was when he signed up for Decibel Magazine – a heavy metal e-zine. I've started to enjoy the monthly issues and have been following the developments of many a 'Lars' and the up and coming band, Monster Magnet. I'm still not listening to the genre but I've developed an appreciation that was never there before. I do hope he renews again this year, for the third time!

What Nathan-corn-metal has not learned to appreciate is that when one sign's up for a service on-line, there often lacks a process to confirm one's contact details. The moment he hits Submit, the subscription was handed over to me and, unfortunately, I have no way of letting him know of the error, as email is the only detail of contact provided.

Telephone bookings

I'll admit that the Decibel Magazine subscription didn't actually tip me off as to the problem at hand. It was the creation of an on-line travel account. I assume Nathan-corn-metal's account was setup over the telephone for the following reason's:

- A. the login id was the email address
- B. there was a flight booking already in the account

So, how did I know there was a flight booked, you may ask? Was there not a password on the account? Yes, there was a password on the account. However, I didn't need it as there was a link in the automated email addressed to me that went straight to the booking, providing me with access to everything including account preferences and the booking page.

Good Samaritan for the good intention

At this point I started thinking about how I would feel if I'd made such a mistake and I decided to try and fix things. Surely, the travel company had a contact phone number.

I called the travel agency asking to speak to a representative about an existing booking. To their credit, they were very quick to answer the phone. Unfortunately, every moment after this was truly shocking. I didn't play any games for, despite his apparent learning difficulties, Nathan-corn-metal, for all I know, could be a decent chap. But my attempt at doing the right thing was met with resistance. Maybe it was a lack of understanding of the urgency of the problem? I didn't know but I had to attempt a new tactic. Being told over and over again that it wasn't the travel agencies problem was not good enough.

Next, I explained it in terms of liability by advising that I would be altering the flight details and then maybe booking myself a trip to Venice using their customer credentials. Then by explaining that as they were the ones to leak said credentials it should make interesting reading in the news. Suddenly, my suggestion that they lock down the account and contact Nathan-corn-metal by telephone immediately was set in motion.

Should this have been so difficult?

Lesson learned?

When so many on-line services fail to provide sufficient checks to ensure we are who we say we are, it is suddenly very simple for a lot to go wrong. I'm delighted to say that I still communicate with my grandparents via hand-written letter for I don't believe that the Internet is a safe place for them. While the law might have clear definitions for liability, in reality, what is practiced is far from acceptable.

Some organizations are building in security checks but only from the perspective of hacking attempts. What about a simple mistake at the time of account creation as done so by the aforementioned head banging tractor driver? In this example, holding off on the creation of an account until verification via OTP (One Time Password) for example would eliminate many false positive during account creation.

Never underestimate the human element!

F5 Networks, Inc. | 401 Elliot Avenue West, Seattle, WA 98119 | 888-882-4447 | f5.com

F5 Networks, Inc.
Corporate Headquarters
info@f5.com

F5 Networks
Asia-Pacific
apacinfo@f5.com

F5 Networks Ltd.
Europe/Middle-East/Africa
emeainfo@f5.com

F5 Networks
Japan K.K.
f5j-info@f5.com

©2016 F5 Networks, Inc. All rights reserved. F5, F5 Networks, and the F5 logo are trademarks of F5 Networks, Inc. in the U.S. and in certain other countries. Other F5 trademarks are identified at f5.com. Any other products, services, or company names referenced herein may be trademarks of their respective owners with no endorsement or affiliation, express or implied, claimed by F5. CS04-00015 0113