Banks, Arbitrary Password Restrictions and Why They Don't Matter

18 SEPTEMBER 2019

Allow me to be controversial for a moment: arbitrary password restrictions on banks such as short max lengths and disallowed characters don't matter. Also, allow me to argue with myself for a moment: banks shouldn't have these restrictions in place anyway.

I want to put forward cases for both arguments here because seeing both sides is important. I want to help shed some light on why this practice happens and argue pragmatically both for and against. But firstly, let's just establish what's happening:

People are Upset About Arbitrary Restrictions

This is actually one of those long-in-draft blog posts I finally decided to finish after seeing this tweet earlier on in the week:

> *My bank tells me that their exactly-5-digit password policy is secure since it has 1.5bn permutations and the account gets blocked after 3 attempts. This just feels wrong but I can't come up with a strong argument against it. Any thoughts? @troyhunt @SmashinSecurity ?*
>
> *— Peter Ullrich (@PJUllrich) September 15, 20*

Subscribe

”

It feels wrong because 5 digits presents an extremely limited set of different possible combinations the password can be. (There's something a little off with the maths here though - 5 digits would only provide 100k permutations whereas 5 *characters* would provide more in the order of 1.5B.)

That said, Westpac down in Australia certainly appears to be 6 characters:

“

*Finally thought @Westpac had upped their password game, moving from the long pointless on-screen keyboard (OSK) with a character count limit, to 'normal' password entry. But nope... 6 characters... MAX... for my *online banking*. @troyhunt pic.twitter.com/9FMSdvVRiL*

— Hagen (@hagendittmer) June 3, 2018

”

Which puts us well north of a billion possibilities again. Want more? CommBank will give you 16 characters:

“

All the nonsense with @Citibank yesterday reminded me that my main bank @CommBank also has its own password security stupidity which is limiting password lengths to 16 characters. https://t.co/5BVdYbSsmO @troyhunt

— Daniel Parker (@CodyMcCodeFace) June 21, 2018

Subscribe

”

On the one hand, it's a damn sight more generous than the previous two banks yet on the other hand, why? And while I'm here questioning CommBank's logic, what the hell is going on with this:

> A password manager is a tool designed to store passwords in a virtual vault, secured with a master password. While helpful for certain types of accounts, we recommend you don't store your NetBank password in a password manager.
>
> Assess your personal risk to determine which passwords you're comfortable storing in a password manager, and keep your NetBank password in your head for added security.

1Password has an open letter to banks on precisely this because its awful advice steeped in legacy misunderstandings of both technology and human brains. That open letter is often used as a reference to persuade banks to lift their game:

“

@TSB Please remove the 15 character maximum password length restriction and allow any characters without having to include any specific ones. This is also the advice of the @NCSC https://t.co/WTmWEldLBO

— Brian Gentles (@phuzi_) June 21, 2018

”

So on the surface of it, the whole thing looks like a bit of a mess. But it's not necessarily that bad, and here's why:

Password Limits on Banks Don't Matter

That very first tweet touched on the first reason why it doesn't matter: banks aggressively lock out accounts being brute forced. They have to because there's money at stake and once you have a financial motivator, the value of an account takeover goes up and consequently, so does the

Subscribe

incentive to have a red hot go at it. Yes, a 5-digit PIN only gives you 100k attempts, but you're only allowed two mistakes. Arguably you could whittle that 100k "possibilities" down to a much smaller number of "likely" passwords either by recognising common patterns or finding previously used passwords by the intended victim, but as an attacker you're going to get very few bites at that cherry:

> *Good morning, Keep in mind with ING a 4 digit access code is the maximum we offer. However, after 3 attempts of entering an Access Code your account will be blocked. ^Alissa*
>
> *— ING Australia (@ING_Aust) August 13, 2018*

Next up is the need to know the target's username. Banks typically use customer registration numbers as opposed to user-chosen usernames or email addresses so there goes the value in credential stuffing lists. That's not to say there aren't ways of discovering someone's banking username, but it's a *significantly* higher barrier to entry than the typical "spray and pray" account takeover attempts.

Then there's the authentication process itself and it reminds me of a discussion I had with a bank's CISO during a recent workshop. I'd just spent two days with his dev team hacking themselves first and I raised the bollocking they were getting on social media due to a new password policy along the lines of those in the tweets you see above. He turned to me and said, "Do you really think the only thing the bank does to log people on is to check the username and password?" Banks are *way* more sophisticated than this and it goes well beyond merely string-matching credentials; there's all sorts of other environment, behavioural and heuristic patterns used to establish legitimacy. You won't ever see a bank telling you how they do it, but those "hidden security features" make a significant contribution to the bank's security posture:

Subscribe

Hi. I understand your concerns. Our Online Card Services login is our first line of security, but we do have many other hidden security features in place that help us to protect your account and details. ^LauraP

— MBNA (@mbna) July 9, 2018

”

Then there's the increasing propensity for banks to implement additional verification processes at key stages of managing your money. For example, one of the banks I regularly use sends me a challenge via SMS whenever setting up a new payee. Obviously, SMS has its own challenges, but what we're talking about now is not just needing to successfully authenticate to the bank, but also to prove control of a phone number at a key stage and that will *always* be more secure than authentication alone.

And if all of this fails? Banks like ING will give you your money back:

“

Hi Owen, your online banking is safe and secure with ING. We take security seriously, and use industry-leading technology to protect your accounts. Plus, we have an Online Security Guarantee in place. In the unlikely event that an unauthorised...

— ING Australia (@ING_Aust) June 21, 2018

”

“

Subscribe

> *...transaction takes place on your account, you won't have to pay for it. For more information you can refer to our website https://t.co/YFhUxNdIUL ^Sarah M*
>
> *— ING Australia (@ING_Aust) June 21, 2018*

”

Now, compare all this to logging on to catforum.com:

How much sophistication do you think is behind those username and password fields in that vBulletin forum? Exactly, it's basic string-matching and this is really the point: judging banks by the same measures we judge basic authentication schemes is an apples and oranges comparison.

However, I disagree with banks taking this approach so let me now go and argue from the other side of the fence.

Banks Shouldn't Impose Password Limits

There are very few independent means by which we can assess a website's security posture in a non-invasive fashion. We can look for the padlock and the presence of HTTPS (which is increasingly ubiquitous anyway) and we look at the way in which they allow you to create and use passwords. There are few remaining measures of substance we can observe without starting to poke away at things.

So what opinion do you think people will form when they see arbitrary complexity rules or short limits? Not a very positive one and there are the inevitable conclusions drawn:

“

> *Hey [bank], does that 16 character limit mean you've got a varchar(16) column somewhere and you're storing passwords as plain text?*

”

Subscribe

As much as I don't believe that's the case in any modern bank of significance, it's definitely not a good look. Inevitably the root cause in situations like this is "legacy" - there's some great hulking back-end banking solution the modern front-end needs to play nice with and the decisions of yesteryear are bubbling up to the surface. It's a reason, granted, but it's not a very good one for any organisation willing to make an investment to evolve things.

But beyond just the image problem, there's also a functional problem with arbitrarily low password limits:

> *Dear @FultonBank, please remove the 32 character limit from your online banking. Some of us use applications like @1Password and want to use longer passwords. pic.twitter.com/EdV5VUi2ZO*
>
> *— Sal Ferrarello (@salcode) December 12, 2018*

I've been through this myself in the past and I vividly recall creating a new PayPal password with 1Password only to find the one in my password manager had been truncated on the PayPal side and I was now locked out of my account. This is just unnecessary friction.

Summary

So wrapping it all up in reverse order, arbitrary low limits on length and character composition are bad. They look bad, they lead to negative speculation about security posture and they break tools like password managers.

But would I stop using a bank (as I've seen suggested in the past) solely due to their password policy? No, because authentication in this sector (and the other security controls that often accompany it) go *far* beyond just string-matching credentials.

Let's keep pushing banks to do better, but not lose our minds about it in the process.

Subscribe

Troy Hunt

Hi, I'm Troy Hunt, I write this blog, create courses for Pluralsight and am a Microsoft Regional Director and MVP who travels the world speaking at events and training technology professionals →

COPYRIGHT 2023, TROY HUNT

This work is licensed under a Creative Commons Attribution 4.0 International License. In other words, share generously but provide attribution.

DISCLAIMER

Opinions expressed here are my own and may not reflect those of others. Unless I'm quoting someone, they're just my own views.

PUBLISHED WITH GHOST

This site runs entirely on Ghost and is made possible thanks to their kind support. Read more about why I chose to use Ghost.

Subscribe