The Privacy Podcast - Ep.1: Security of Online Accounts and Nyms User Tips
Audio is available at http://www.theprivacyblog.com

Speaker: Lance Cottrell, founder of Anonymizer

Transcript:

This is Lance Cottrell and you're listening to The Privacy Blog Podcast brought to you by Anonymizer. Thanks for listening to the first of our monthly series of podcasts, focusing on security and privacy. This Podcast is for October 2012.

In this episode I will be talking about non-technical ways your online accounts can be compromised, focusing on email address and password reuse, security questions, and credit card numbers as security tokens. In part two, I will give some power user tips for getting the most out of your Anonymizer Nyms account.

[Part 1: Non-Technical Ways Your Account can be Compromised]

Back in August, a writer for Wired magazine named Matt Honan got hacked by a teenager who just wanted to take his Twitter handle. His computer, phone, and cloud backups all got wiped in the process. This generated a lot of attention at the time, mostly about how it exposed flaws in Apple's and Amazon's security practices. I'm going to review how all that went down and then talk about some of the less reported steps you can take to protect yourself.

The upshot of all that is if you have someone's name, email address, and credit card number, or even just the last four digits of the credit card number in a lot of cases, those sites will give you a new password. This is a harder trick than the one that compromised Sarah Palin's Yahoo! account during the last election. In that case, hackers used the security questions she had set to change the password. The answers to those questions could be found in her social media presence, including things like "birth date" and "high school", the usual questions they put out there.

To perform the hack that compromised the Wired writer, you actually need to get a hold of his credit card number. Turns out, that's easier than you might think. If you contacted Amazon by phone, you could add a new credit card number to the account with just knowing the account holders name and email address. After all, who would want to maliciously give you their credit card number – it's just not part of Amazon's security model. The number does not need to be real and certainly could be a stolen credit card; it just needs to pass the most superficial checks as a valid credit card number. There's a check-sum that goes on every credit card number and as long as you can match that, they'll accept that as a valid card. You can then call back and use that credit card number that you just gave them with the name and email address that you used before to request a password change – because you've identified yourself by knowing one of the credit cards on the account. Once they change that password, you get the password reset, you can log in with that new password and you'll have access to all the saved billing data that Amazon has. Now, Amazon doesn't show you whole credit card numbers of all the other stored credit cards, it only shows you the last four digits, but that's all most companies ask for. Specifically, its all Apple asked for. So now you can

change the password on the Apple iCloud account using the username and that same email and the last four digits from the nice saved credit cards you got from Amazon. Awesome! Now we have two paths into your account. We could go the name, email, credit card route, or we can go the name, email, security questions route.

What can we do about this? Well, your name, you're basically stuck with. Lying about your name is way too much trouble in most cases and probably illegal in the case of banks or financial institutions. Credit card numbers are out there and easy to get. Let's face it, you give your card to near minimum wage workers at restaurants and shops all the time. Credit card numbers are hardly reliable secrets. That leaves two things you can really control – Your security questions and your email address.

Let's look at the security questions first. To make sure they're easy to remember, they generally ask you for few of a small number of standard things – family names, places where you live, went to school, favorite books, movies, etc. While these questions are slowly getting better and more varied, they're far from robust. Fortunately, this is a case where the cost and effort of lying is low. If asked where I was born, I might say "Dubai" or "Mars". If asked the name of my grade school, I could say "Hogwarts Montessori" or "School of Hard Knocks". The key is to use strange answers and not reuse them. So you shouldn't use the examples I just gave you. This is going to require a database of some kind because very quickly you are going to end up with an awful lot of different questions to all sorts of different answers and trying to remember "what lie did I tell to each website?" gets out of control. So you really need to have some kind of a password vault program that helps you easily and securely store all this information along with your passwords. Those passwords are all different on every site, right? I mean, seriously, this is probably the most important thing you can do to protect your information, your infrastructure, your data, your computer, your devices – different passwords everywhere! Anyway, I'm going to assume you're doing that. Now, where do you store this? As a Mac, Apple ecosystem guy, I like 1Password from agilebits.com. On the PC or Linux side, there's a program called LastPass, which seems to be a pretty good choice. Either one syncs across multiple devices, stores everything encrypted in the cloud, and only decrypts it locally on your device, so you always have quick and easy access to all of these questions and answers and passwords from wherever you are. You don't have to remember any of your passwords or your answers, except one, and that's the password to unlock your password vault. As long as that's a good password, everything else goes easy. Now you can always access all those different security answers or lies you made up.

That brings us to the other thing you can control, which is your email address. Most of us have one or, at most, a handful of different email addresses. Managing more than that gets really unwieldy. But as we saw by using the same email address for multiple services, there is a huge vulnerability because that email address is the account name on so many of these websites, so guessing your account name is half the battle for your attacker and you just gave them the answer.

I have about 800 email addresses the last time I checked. No, really, that's a huge part of why I wrote the first version of our Anonymizer Nyms platform years and years ago. I personally wanted this for myself and coded it up over a couple of weekends and thought, "Certainly other people will want to use this". Fortunately, it has been re-coded by people that program better than I do, but still, it's the tool I go to. It is my favorite program in the Anonymizer arsenal. And you really do want to create a different email

address for every business or service you work with. That way, the exposure of any one of these email addresses will not compromise any of the other sites. Your real address is then only known to a small number of people - friends, family, your boss - and it isn't the keys to the kingdom. It isn't the password that your bank, or Apple, or Yahoo, or Amazon knows you by, because they know you by unique email addresses which you've given out one at a time. Clever security people have been doing this, themselves, for years. If you know what you're doing, if you have a server, if you are running a mail server, it's not difficult if you have your own domain, to spin off new email addresses as often as you need – but it is usually a several step process and most people don't have a mail server and their own domain and all the other stuff involved. As with any other security process, if it's not easy and painless, people will not actually do it.

So, in the next segment, I'm going to walk you through some pro tips for getting the most out of Nyms so you can take advantage of the security it brings.

[Part 2: Getting the Most Out of Your Nyms Account]

It's interesting – I use Nyms all the time but have found that many users are confused about how to get the most out of it. Of course, you can use it in whatever way works best for you, but I wanted to share how I pictured it being used when I designed it, and how I actually use it every day.

To get the most out of Nyms, you really need to be profligate in creating them. They should be created all the time - that's how I ended up with 800 of them. And the nice thing about Nyms is that there's really no management to do. There's no cost to having a ridiculous number of Nyms. It doesn't increase your spam and it doesn't increase the amount of work you need to do. Any time a website asks for an email address, I go to Nyms.net - either to create the email address or to remind myself of what address I used to set up the account in the first place. Now, I could do that by opening up a new window, navigating to Nyms.net, going through the pages, searching for the address, but that's exactly the kind of barrier that keeps people from using security tools in the first place. So, instead I use the Nyms Bookmarklet.

A bookmarklet is like a bookmark, but it's smart. It actually has a little bit of code, in this case javascript, built right into the bookmark. You can get the Nyms bookmarklet by going to the Support section of Anonymizer.com and, in the Nyms section, you'll see instructions for adding it [instructions here]. It's really just as simple as grabbing the link that you see, dragging it up to your bookmark bar, and naming it something like "New Nym". Now, when you're asked for an email address, you just click that bookmark and it instantly pops open a new window to the "Create a New Nym Page" and it pre-fills the URL of the page you're on. You don't need to go tell it where you're coming from. The page also looks up whether you have a Nym for that site already and if you do, it tells you what it is. Click the new Nym, and it goes pop! "You already have a Nym for this site." Just copy that Nym and paste it right into the page you're on and keep going. If you don't have a Nym, you can immediately create it right there - instantly set it up, copy, close the window, paste, and you're done. It takes me maybe, 5-10 seconds to create a new Nym each time I need one - and that's really critical, that seamless process.

This is another place where password vaults and automatic form fillers like 1Password and LastPass really shine. If you use them to store your logins, and the login is your email address (n this case one of the Nyms email addresses you created) they're

already stored. It's really completely transparent to you. When you go to log in you just say, “Hey, fill in this form” and boom! The address plus that unique password is directly filled into that page.

I also keep a link to the 'Create a Nym' page stored on my iPhone on the first page of the apps. That makes it easy to bookmark to your homepage on the iPhone or save links onto your Android launch page, so that with one tap I can immediately go to the Create a Nym page. This is really useful when I’m confronted with requests for an email address in meatspace – I’m standing at a hotel check-in counter and they’re asking me for an email address on the registration form. I just whip out my phone, hit that link, and boom! Create a new Nym on the fly and fill it out in the form. It’s captured in Nyms so I don’t need to remember it. I made a little note when I created it for what hotel it went with and off I go!

Finally, there are some tricks on how to choose your Nyms. What email address do you select? The default is to generate them randomly so if you’re really in a hurry you just go. It’s going to create a big long random Nym, guaranteed not to contain any information about you at all, but it’s a little awkward to remember to work with because they’re harder to type. So I generally use the name or abbreviation for the website that I’m setting up the Nym for, followed by some random letters or numbers. Let's say I was on the New York Times website setting up an account. The Nym that I create might be (but isn’t) NYTimes547@nyms.net. That makes it hard to guess, right? Someone can’t just go, “Oh, he uses the same numbers after the name or it’s always his name followed by something else.” It’s kind of random, very difficult for someone to guess but it’s also easy to search for. If you are going into the Nyms website, it’s very easy to search the Nyms for the one corresponding with that website. Also, when you get email to a Nym, it always has that link at the bottom of the email that allows you to delete the Nym or to go in and edit the Nym, and shows you what the Nym was. If the Nym contains the name of the person you created it for, then you know where that Nym was created and if it was a spam email. You know who sold you out.

So that’s it for our inaugural podcast this October, 2012. I hope you’ve enjoyed it. I’d love to hear you feedback and get a conversation going in the comments on this post at theprivacyblog.com. I hope you’ll come back for our November episode. Thanks for listening.