The convenience of online access to bank accounts, payment apps, crypto exchanges and other transaction systems has created enormous risks, which the vast majority of individuals either choose to ignore or simply don’t understand. The Internet has become the new private network and unfortunately, it’s not so private. Open APIs, scripts, spoofing, insider crime, sloppy […]
The convenience of online access to bank accounts, payment apps, crypto exchanges and other transaction systems has created enormous risks, which the vast majority of individuals either choose to ignore or simply don’t understand. The Internet has become the new private network and unfortunately, it’s not so private. Open APIs, scripts, spoofing, insider crime, sloppy security hygiene by users and much more, all increase our risks. The convenience of cloud-based services, in many respects, exacerbates the problem. But software built in the cloud is a big part of the solution.

In this Breaking Analysis we try to raise awareness about a growing threat to your liquid assets and hopefully inspire you to do some research and take actions to lower the probability of you losing thousands, hundreds of thousands or millions of dollars.

Remember What Happened in 2019?

In September of that year, Jack Dorsey’s Twitter account was hacked.

The hackers took over his account and posted racial slurs and other bizarre comments before Twitter could regain control of the account and assure its community that it wasn’t a system-wide attack.

As concerning was the manner in which the attackers got a hold of Dorsey’s Twitter. They used an increasingly common and relatively easy to execute technique referred to as a SIM hijack or SIM swap. The approach allows cyber thieves to take control of a victims phone number. They often target high profile individuals like CEOs and celebrities to embarrass or harass them. But increasingly, they’re going after people’s money. Of course.

Cyber Criminals Cash in on SIM Hacks

Just in the past month we’ve seen a spate of SIM hijacks, many in which individuals have lost money.
It's a serious problem of increasing frequency.

**The Basic Anatomy of a SIM Card Hijack**

Some of you are familiar with this technique but most people we talk to either aren’t aware of it or aren’t concerned. You should be. In a SIM hack, like this one documented on Medium in May of 2019, four months prior to the Dorsey breach, the attackers used personal information to fool an agent at a mobile phone carrier. Note that many of your credentials have likely been posted on the dark web – your email, frequently used passwords, phone number, address, mother’s maiden name, name of your favorite pet and so forth. The attackers use this information to spoof a mobile phone carrier rep into thinking it's you. They convince the agent that they've switched phones or some other ruse and get a new SIM card sent to them.

Or, they pay insiders at the phone carrier to steal SIM card details in exchange for cash.
Once in possession of the SIM card info, the attacker now can receive SMS messages as part of two factor authentication systems used to verify identity. They can’t use face ID on mobile but what they can do is go into your Web account and change the password or other information. The Web site sends an SMS and now the attacker is in. Then the individual can lock you out and steal your money before you know what hit you.

What’s the Defense Against a SIM Hack?

First, there’s no system that is 100% perfect. If the bad guy wants to get you and the value is high enough, they will get you. But that’s the key. ROI. What is ROI? Simply put, it’s a measure of return derived from dividing the value stolen by the cost of getting that value. Benefit divided by cost. So a good way to dissuade a criminal is to increase the denominator. If you make it harder to steal, the ROI goes down.

Below is a layered system shared by Jason Floyer, the son of our very own David Floyer. Smart DNA there so we appreciate his contributions to theCUBE.
Breaking Analysis: Why Your Online Assets Aren’t Safe - Is Cloud the Problem or the Solution?

A Layered Approach

The system involves three layers of protection.

The first piece we want to call to your attention is all the high value online systems shown on the chart. We’ve identified just a few. Bank accounts, investment accounts, betting sites...e-commerce sites and so forth. Many will use SMS-based two-factor authentication (2FA) to identify users, which exposes you to the SIM hack.

The system Jason proposes starts in the middle of the chart with an acknowledgement that the logins you’re using to access critical systems are already public. So the first thing you do is go get a "secure" email. In other words, one that no one knows about and isn’t on the dark Web. Find a provider you trust – maybe one that doesn’t sell ads...but that’s your call...or buy a domain and create a private email address.

The second step is to use a password manager. For those who don’t know what that is, you probably are already using one that comes with your Chrome browser for example and remembers your passwords.

Here's a little wake up call. On your iPhone, go to Settings–>Passwords–>Security Recommendations. Or on your Android phone open your Chrome app and go to Settings–>Passwords–>Check passwords. You’ll likely see a number of recommendations – as in dozens or hundreds – based on the fact that your passwords have been compromised, reused and/or are the subject of a data breach.

A password manager is a single cloud-based layer that works on your laptop and mobile phone and allows you to largely automate the creation, management and maintenance of your online credentials.

The third layer involves an external, cloud-based two factor authentication system that doesn’t use SMS. One that essentially turns your phone into a hardware authentication device, much like an external hardware device such as a YubiKey– which is also a good idea to use as the third layer.

So the system basically brings together all your passwords under one system with some layers that lower the probability of your money getting stolen. Again – that risk doesn't go to 0% but it’s dramatically better than the protection most people have.
One Password to Remember

Below is another view of the system.

**Single Password Manages the Layers**

In this Venn, the password manager in the middle manages everything. Yes there’s a concern that all your passwords are in one place but once set up it’s more secure than what you’re likely doing today and it will make your life easier. The key to this system is there is a single password that you have to remember for the manager and it takes care of everything else. For many password managers, you can also add a non-SMS-based third party 2FA capability. We’ll come back to that.

The mobile phone uses facial recognition if it’s enabled so it would require that someone has you at gunpoint to use your phone to get into your accounts – or they are experts at deep fakes – that’s probably something we’ll have to contend with down the road.

It’s the desktop or laptop via Web access that is of the greatest concern in this use case. This is where the non-SMS-based third party 2FA comes into play. It is installed on your phone and if someone comes into your account from an unauthorized device it forces a 2FA using the third party app that is typically running in the cloud.

Importantly, it generates a verification code that changes on your phone every 20 seconds and you can’t get into the Web site without entering that auto-generated code. Well, normal people can’t get in– There’s probably some other back door if a hacker really want to get you…but you can see that this is a better system than what 99% of the people have today.

**You’re Not Done Yet...Use an Air Gap**

Just as with enterprise tech and dealing with the problem of ransomware, air gaps are an essential tool in combating cybercrime.
So we’ve added a couple of items to Jason’s slide. Safeguard and air gap that secure password. You want to make sure that the password manager password is strong, easy enough for you to remember and never used anywhere except for the password manager, which also uses the secure email. If you’ve set up 2FA, SMS or otherwise (ideally the latter), you’re even more protected.

For your crypto – especially if you have a lot – get it out of Coinbase. Not only does Coinbase gouge you on transaction costs but store a good chunk of your crypto in an air gapped vault.

Make a few copies of this critical information, keep your secure password on you or memorize it and put the rest in a fireproof filing cabinet, safety deposit box and/or a fireproof lock box...along with all your recovery codes for the password manager and the crypto wallets you own.

Yes – it gets complicated and is a pain but imagine having 30% or more of your liquid assets stolen.

Start Searching for a Password Manager

We’ve really just scratched the surface here and you’re going to have to do some research and talk to people who have set up similar defenses. After you figure out your secure email provider, turn your attention to the password manager.
Google the topic and take your time deciding which one is best for you. There are many – some free...the better ones are for pay. But carve out a full day to research and set up and implement your full system. Take your time and think about how you’ll use it before pulling the trigger on the tools.

And document everything—off line.

Choose a Third Party Authentication App

The other tooling you’ll want is a non-SMS-based third party authentication app. This turns your phone into a secure token generator without using SMS.
Unfortunately it's even more complicated because not all your financial systems will support the same 2FA app. Your password manager might only support Duo, your crypto exchange might support Authy but your bank might only support Symantec VIP and so forth. So you may need to use multiple authentication apps to protect your liquid assets.

Sorry, we know it’s inconvenient but the consequences of not protecting your money and identity are worth the effort. And the vendors don’t make it any easier - especially the big brand tech companies and many of the larger financial institutions which want to control the full value chain and often don’t support “outsiders.”

**A Fragmented Consumer Market Reflects the State of Enterprise Security**

We know this is a deviation from our normal enterprise tech discussions but the reality is, we’re all the CIOs of our respective home IT. We’re the network admin, the storage admin, tech support help desk and the CISO. So as individuals we can only imagine the challenges of securing the enterprise.

And one of the things we talk about a lot in the cybersecurity space is complexity and fragmentation – it’s just the way it is. Below is a chart from ETR that we use frequently, which lays out the security players in the ETR data set on two dimensions. Net Score or spending velocity on the vertical axis and Market Share or pervasiveness on the horizontal. We’re not going to elaborate on any of the vendors today - you’ve seen this before. But the chart underscores the complexity and fragmentation of this market. And this is just one small subset.
But the cloud, which we said at the top is a big reason that we got into this problem, holds a key to solving it. Here’s one example. Listen to this clip of Dave Hatfield, a long time industry exec, formerly with Pure Storage but now with Lacework, a very well funded, cloud-based security company that in our view is attacking one of the biggest problems – and that’s the fragmentation issue we’ve discussed.

Listen to Dave Hatfield on addressing fragmentation and treating security as a data problem.

Hatfield nails it in our view. The cloud and edge explode the threat surface and this becomes a data problem at massive scale. Now is Lacework going to solve all these problems? No, of course not, but having researched this, it’s common for individuals to be managing dozens of tools and enterprises as Dave said, use 75 on average, with many hundreds being common.

The number one challenge CISOs convey to us is lack of talent / lack of human skills to solve the problem. And a big part of that problem is fragmentation. Multiple APIs, scripts and different standards that are constantly being updated and evolved. So if the cloud can help us reduce tools creep and simplify, automate and scale as the network continues to expand – like the universe – we can perhaps keep up with the adversaries.

We understand this is not our normal swim lane but we think this is so important and know people that have been victimized. So we wanted to call your attention to the exposure and try to get you to take some action...even if it’s baby steps.

How to Take Action

You really want to begin by understanding where your credentials have been compromised – because they have. Just look at your phone or your browser recommendations.
To repeat, you’ll want to block out an entire day to focus and dig into this in order to protect your and your family’s assets. There’s a lot at stake and one day won’t kill you. It’s worth it.

Then you want to begin building those three layers.

Choose a private email that is “secure” – quote unquote

Research the the password manager that’s going to work for you. Do you want one that is Web-based or an app that you download? How does the password manager authenticate? What are the reviews? How much does it cost? Don’t rush into this – you may want to test this out on a couple of low risk systems before fully committing because if you screw it up it’s a pain to unwind – so don’t rush.

Then figure out how to use non-SMS-based two factor authentication apps and identify which assets you want to protect. Do you really care to protect your credentials on a site where you signed up six ago and never use anymore? Just delete it from your digital life and focus on your financial accounts, crypto and sites where your credit card or other sensitive information lives.

Also, it’s important to understand which institutions utilize which authentication methods

It’s really important that you make sure to document everything and air gap the most sensitive credentials

And finally, keep iterating and improving your security because this is a moving target. You will never be 100% protected. Unfortunately this isn’t a one shot deal. You’ll do a bunch of hard but important work and maintain your passwords by changing them every now and then and a couple years down the road you may have to implement an entirely new system using the most modern tooling – which we believe will be cloud based.

Or you could just ignore it and see what happens.

Thanks to Jason Floyer and Alex Myerson for their contributions to this week’s post. We’re sure many in the community have implemented similar or better systems. What did we miss? How can we help each other be more secure? Please let us know.
Ways to Keep in Touch

Remember these episodes are all available as podcasts wherever you listen.

Email david.vellante@siliconangle.com | DM @dvellante on Twitter | Comment on our LinkedIn posts.

Also, check out this ETR Tutorial we created, which explains the spending methodology in more detail.

Watch the full video analysis:

Image credit:  kelly marken

Note:  ETR is a separate company from Wikibon/SiliconANGLE.  If you would like to cite or republish any of the company’s data, or inquire about its services, please contact ETR at legal@etr.ai.
David Vellante is co-CEO of SiliconANGLE Media, as well as co-founder and Chief Analyst at The Wikibon Project, the world’s leading open source technology research community. Dave is a long-time tech industry analyst, entrepreneur, writer and speaker. As co-host of theCUBE – “The ESPN of Tech,” Vellante has interviewed over 5,000 experts since 2010. He is also a co-founder of CrowdChat, an angel funded startup based in Palo Alto using big data techniques to extract business value from social data. Prior to these exploits, Dave founded a CIO consultancy and spent a decade growing and managing IDC’s largest business unit. He lives in Massachusetts with his wife and four children where he is active in town activities including serving as the president of his town’s local “Kiddie Sports” association. Dave holds a B.S. in Applied Mathematics from Union College.

David Vellante
@dvellante
david.vellante@wikibon.org