How to: set up“virtual number” call and SMS routing for ~$30/yr.

Daniel Rosehill
Apr 1, 2019 · 8 min read

The Impetus: Getting Locked Out of Paypal

If you use almost any online service, you’re probably already familiar with two factor authentication (2FA).

Two factor authentication is an extra layer of security to web services that requires that the user enter an additional piece of information besides their username and password. Although most two factor logins now integrate tidily with Time-based One Time Password (TOTP) tools like Authy and Google Authenticator, an obstinate few insist on sending their codes over SMS to the user’s cellphone.

This state of affairs is very far from ideal and it is amazing that the list of providers that still use SMS for 2FA/MFA is both so long and illustrious. At the time of writing, this is Paypal’s default system, unless you buy a proprietary Symantec USB device (which some enterprising users have apparently reverse-engineered). And even if having to carry a piece of hardware to authenticate only one service tickles your fancy (it didn’t mine) the order link was broken when I tried to access it.

SMS isn’t an ideal medium for delivering two factor authentication codes and it’s fair to say that this was never an intended use-case. Assuming that it is at least encrypted (at the final stage, this is often not the case, rendering the packets susceptible to sniffing), the SS7 set of telephony protocols has its own set of documented vulnerabilities. In a duel between the two methodologies, IP-based OTP authentication is the clear victor!

More concerning to me than these technical details was the fact that I couldn't answer any of the following questions with a better retort than "that would be a problem":

- What would happen if I were to **lose access to my personal cellphone number,** or indeed the **device itself?**
- What if I **forgot to renew a cellphone contract**, the carrier released it to another user, and the 2FA prompts irresponsibly contained some personally identifying information?
- What if I were to find myself abroad in a country where I **didn't have a roaming plan** active, and had no immediate way to buy one, but urgently needed to log in to Paypal or online banking?
- Or what if I needed to receive a verification code in a **place without cellphone reception**?

I have multiple ways to retain 2FA backup access to my G-Suite account, including a physical Yubi key, which I carry on my keychain at virtually all times as well as a set of backup codes, which are easy enough to memorize.

Those systems, which I can access wherever I can find a computer with internet, are usually enough to initiate an email-based password recovery process for practically *any* login-based system on the internet. Relying on receiving time-limited SMS codes, by comparison, seemed like a massively vulnerable security method waiting to go wrong.

And as I learned this week-indeed, it often is.

A few days before writing this, completely out of the blue, I **stopped receiving authentication codes (and any SMS messages) from my cellphone provider**. Testing my two SIMs in another device and following other troubleshooting steps confirmed that the issue was likely carrier-side. And as both phone calls and data were working fine, I could safely assume that the issue wasn't due to suddenly defective SIM cards. Although the texts did eventually begin to intermittently arrive, they only did so after a **five or six hour delay**. And as the upper limit on time-based 2FA codes is generally at around the ten minute mark, this rendered them completely useless. It was as quandary without a solution.

More importantly, I suddenly found myself **unable to access my Paypal account and credit card** with all the attached implications (including not being able to discontinue

a recurring subscription before the impending renewal date). **Paypal could not be convinced to deactivate the protection** despite my repeated attempts to explain the situation to them. I thought about creating a virtual number through which to route texts to my email (Paypal had agreed that the account number could be changed), but ironically found myself **unable to create virtual phone numbers accounts** without being able to verify a real cellphone contact number first. I was potentially **missing SMS package notifications from the postal service** which often arrive only once. Although I think of it as a legacy technology, losing access to SMS hurt more than I would have thought!

Ultimately, after **going the best part of a week without receiving texts** and spending plenty of hours wasted talking with tech support people, my c **ellphone provider sorted out the problem**. A new SMS delivery center was having some teething problems, an APN update hadn’t been pushed out to all devices, and after re-provisioning my device on the network, I was back in action receiving messages as soon as they were sent.

However the experience had left me completely convinced **that I needed to set up a backup system for receiving authentication codes** from providers that still insist on using text messages or automated phone calls for 2FA or to verify suspicious logins — something that had long lingered towards the back of my tech to-do list. The ideal solution firstly seemed obvious — simply rent a virtual number with an email relay and forward inbound SMS messages. But I soon realized that it wasn’t quite that simple. (I briefly thought about abandoning 2FA on Paypal, but would rather find a solution than be a victim of a n attack such as this).

The Problem with Using Commercial Virtual Number/SIP Trunking Providers For 2FA Verification Code Forwarding

I soon discovered that what I was looking for was a bit of a gap in the market, as the below T&C from Sonetel against using their virtual cellphones for verification purposes illustrates.

> Please note that the Sonetel service may not be used for identity validation or verification at websites related to banking or any other third party website or online service.
> It is free to receive SMS on your phone numbers, but there is a fair usage restriction.

- Programmatic SMS providers, which work by API, abound. But most providers with a human-friendly UI that I contacted expressly **stated that they did not support passing along verification codes.**

- VOIP/SIP trunking provider that offered call and SMS relaying on virtual +972 cellphones had **pretty extensive identity verification processes**, and I couldn't find reliable Trustpilot reviews about many of them.

- **Fraud is a big concern in the virtual number space.** This makes sense, given that they effectively allow you to spoof your location.

Thankfully, I had some spare kit on hand to set this up for myself.

I'm not claiming that it's as ideal a solution as having a virtual number managed in a professional data center, and obviously **requires having a cellphone powered on 24/7** (which makes it not ideal for digital nomads without a home base). But it should do the trick for the time being, seems to route verification SMS messages more reliably than the several virtual number providers I trialed, and possibly also works out cheaper than using them in the long run.

Hardware, Software, and Other Resources

- Just about the **cheapest 4G/LTE Android on the market:** the Doopro P4 Pro (at the time of writing: $49.91 on Aliexpress). I kept the battery in and also hooked it up to the mains over micro USB. It's connected to a WiFi connection and both it and the router powering the connection are drawing power through a UPS (giving the cellphone two non-concurrent backup power reservoirs). A 3G handset would, of course, also have worked fine. But the UPS and cellular data provide some redundancy in the event of both WiFi and power outages.

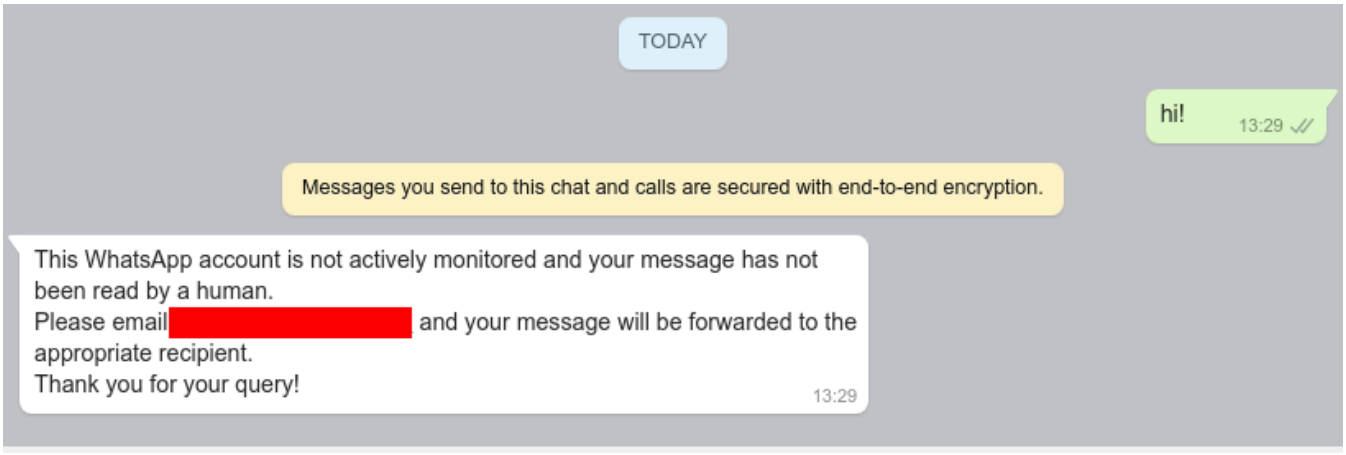
- The **cheapest line subscription that I could find** (the device's sole purpose is obviously to receive texts, route them to email, and receive calls and forward them to my personal cellphone). **The average monthly bill is about 10 NIS ($2.73)** as generally no data is used. In other geographies, it **may be cheaper to use a pre-paid plan**, work out the carrier's automatic disconnection period (in my experience, usually independent from the time zero credit is reached), and then set a reminder to top up the credit right before that.

- **SMS Forwarder** to copy all SMS messages to my email.

- **Teamviewer QuickSupport** in case I need to remotely make configuration changes

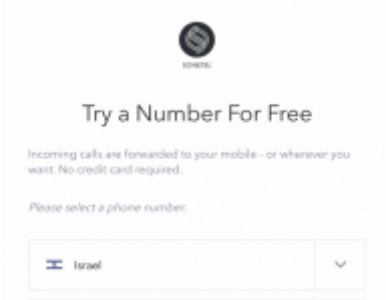
Some Finishing Touches

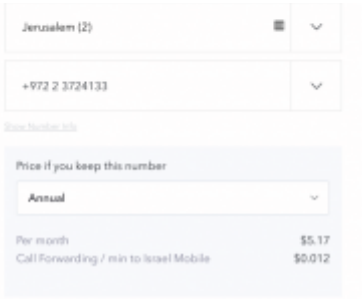
- A **microphone blocker** app to disable the microphone at the application level.
- Some black **masking tape** to physically block the device’s front and rear cameras. A blocker app as an additional precaution against malware camera activation.
- I configured the **call forwarding with the carrier,** but could also have usedfor the same purpose.
- AutoResponder for WhatsApp to let recipients know that their message hasn’t been read and to provide my email address (I could have foregone using WhatsApp on the line but figured it could be useful).



The first year cost of this, including the handset purchase, is **$82.76**, falling to about **$32.76 per year thereafter.** I imagine that electricity costs are pretty minimal. And this process could be replicated just about anywhere on Earth.

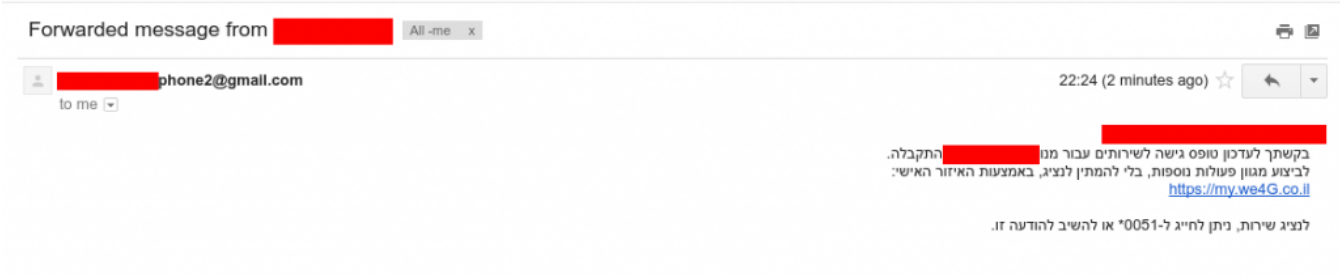
By comparison, Sonetel would have come in at around **$62.04**, but would have also involved a **per/minute charge on all calls routed through the virtual number** and may not have supported authentication codes for two factor authentication.



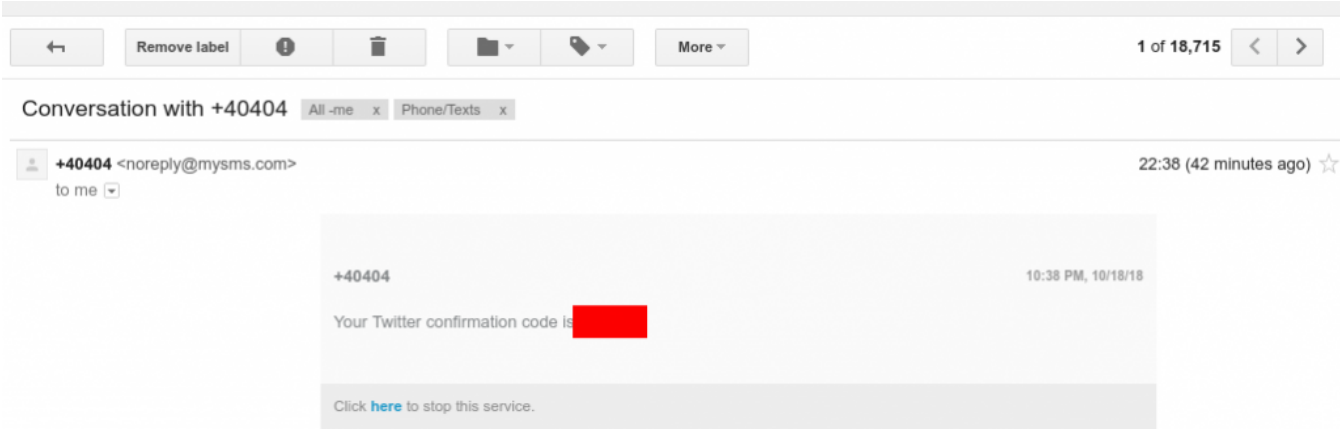


Result: successful self-managed forwarding of 2FA codes and to email and calls to my cellphone. The system should work no matter where I am in the world!

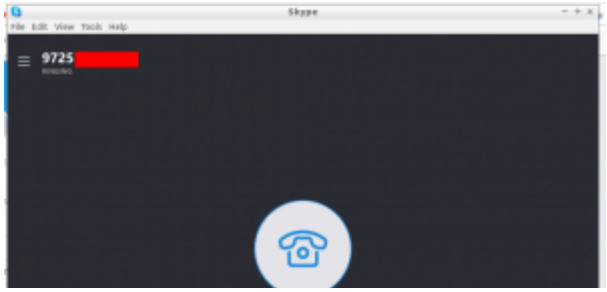
First text success:

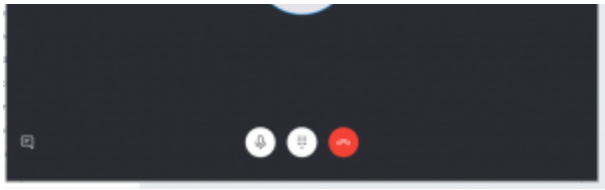


Successful mobile verification code from Twitter. Received over email from phone. MySMS doing the forwarding on this particular message.

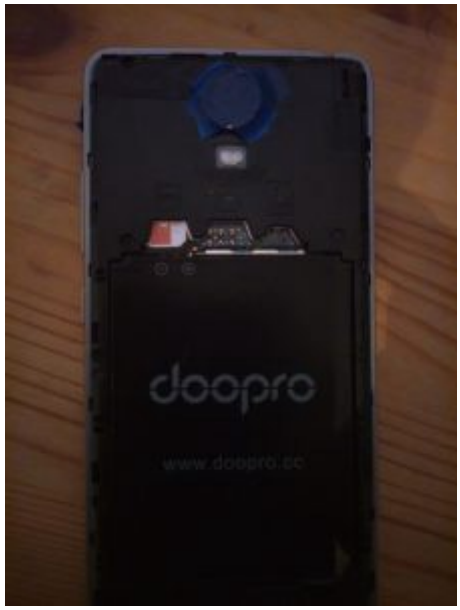


First test call through Skype. Pulled through the intermediate handset to my actual phone in about ten seconds. (Modified desktop created with Apex).

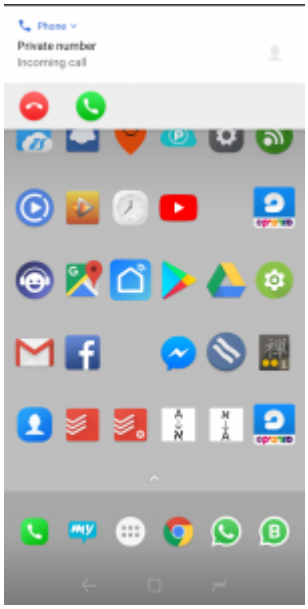




➡



➡



• • •

Originally published at https://www.danielrosehill.co.il

2fa DIY Virtual Number Sms Two Factor Authentication