

Interview with a Scampire

By Eric Cameron

An email alert pops up on my phone. I wasn't paying full attention, but it appeared to be something about an invitation for an interview. I was laid off in February, and have been diligently applying for jobs in the meantime, so this is exciting news!

The Email

I open my Gmail app, and sure enough, there it is:

"Invitation for Data Analyst Position interview at Agile Therapeutics"

I don't recall applying for a position at this company, but I have been applying for positions advertised on LinkedIn, so maybe it was one I applied for and didn't think too much about, I think to myself. I open the email, and all of the warning bells go off:

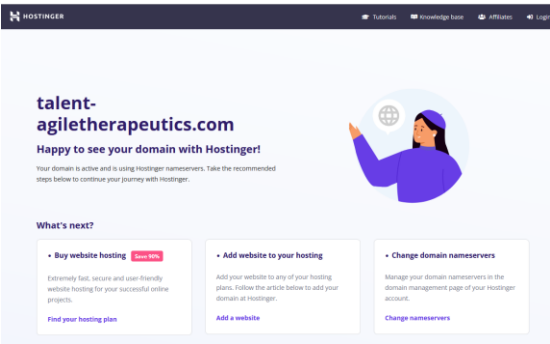


1. The domain name (talent-agiletherapeutics.com) is not the same as the company's domain name (agiletherapeutics.com) or not a subdomain (for example, talent.agiletherapeutics.com). Same issue with the email address; it is from careers@talent-agiletherapeutics.com)
2. There's a specific time attached to the email; I'd never imagine a professional dictating the time/date of an interview without giving a few options.
3. A quick search doesn't find a person with this name on LinkedIn.
4. There are a number of typos, a few odd word choices, phrases, and such. Also notice inconsistent fonts.

I know many people get taken in by scammers every year. Scammers took hundreds of dollars from one my senior neighbors, so it's near and dear to my heart, so I decide to play detective.

Sleuthing Online

First, visiting the talent-agiletherapeutics.com website shows this (as of June 5, 2024):



I would expect, if it were their talent domain, it would definitely have job information there.

Next, I take a look at the domain information (this information is publicly available using any *whois* tool), to compare it to the real Agile Therapeutics site:

Real Site	Fake Site
WHOIS search results Domain Name: AGILETHERAPEUTICS.COM Registry Domain ID: 63247799_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.corporatedomains.com Registrar URL: http://cscdns.com Updated Date: 2023-02-17T06:09:05Z Creation Date: 2001-02-21T21:18:12Z Registry Expiry Date: 2025-02-21T21:18:12Z Registrar: CSC Corporate Domains, Inc. Registrar IANA ID: 299 Registrar Abuse Contact Email: domainabuse@cscglobal.com Registrar Abuse Contact Phone: 8887802723 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Name Server: NS10.DNSMADEEASY.COM Name Server: NS11.DNSMADEEASY.COM Name Server: NS12.DNSMADEEASY.COM Name Server: NS13.DNSMADEEASY.COM Name Server: NS14.DNSMADEEASY.COM Name Server: NS15.DNSMADEEASY.COM DNSSEC: unsigned	WHOIS search results Domain Name: TALENT-AGILETHERAPEUTICS.COM Registry Domain ID: 2883576296_DOMAIN_COM-VRSN Registrar WHOIS Server: whois.PublicDomainRegistry.com Registrar URL: http://www.publicdomainregistry.com Updated Date: 2024-05-22T16:24:07Z Creation Date: 2024-05-22T16:24:07Z Registry Expiry Date: 2025-05-22T16:24:07Z Registrar: PDR Ltd. d/b/a PublicDomainRegistry.com Registrar IANA ID: 303 Registrar Abuse Contact Email: abuse-contact@publicdomainregistry.com Registrar Abuse Contact Phone: +1.2013775952 Domain Status: clientTransferProhibited https://icann.org/epp#clientTransferProhibited Name Server: NS1.DNS-PARKING.COM Name Server: NS2.DNS-PARKING.COM DNSSEC: unsigned

Notice the talent-agiletherapeutics site was just created on May 22, 2024, with a different Registrar. It’s really unlikely for a company to host these things separately.

To be extra certain, I used LinkedIn and locate someone in Human Resources at Agile Therapeutics. I can see the legitimate Agile Therapeutics has been on LinkedIn since at least 2022

(<https://www.linkedin.com/company/agiletherapeutics/>) and the Human Resources director for the company has been on LinkedIn since 2006. I reach out to Agile and confirm, there is no position, and they are aware of fraudulent posts about open positions at their company, and this person does not represent them. I share a screenshot of the email with them and suggest they consider pursuing it with the domain name registrar.

As mentioned earlier, there is no David Jeffries on LinkedIn associated with Agile Therapeutics, which would be a little strange for a modern-day HR professional.

My Interview with “David Jeffries”

I’ve been following the YouTube channel of [Pleasant Green](#), who fights back against scammers online. I took a lot of inspiration from his methods. I know the way to hit scammers where it hurts is to get to their money mule, so I opened up Teams and added David Jeffries by way of his email address at the talent-agiletherapeutics site. I confirmed this was a text-only interview and showed up on time to discuss the position. David led with the following word salad:

As we proceed with the briefing and interview, I will make every detail of the open position known to you so your keen and undivided attention is stipulated. Do be informed all minutes of this interview are being recorded for referential purposes.

He gave me the following information:

Should you be offered the job, we'll provide you with all the working equipment you'll use for work, all costs covered entirely by the company but you are required to purchase and own a second (separate) smart phone which will serve as your business line, best purchased through your existing postpaid account you have with your current carrier or through our partnership with Verizon wireless. You will however be reimbursed for this expense through your startup funding customarily. I believe this won't be an issue?

Now, I didn't want to appear too eager, so I asked for clarification about the reimbursement, and he told me it would be provided with my first paycheck.

He discussed salary:

Soon we'll be setting up a few branches near your location. That is why we are looking for 16 new hires to work from home. Once the new branches have been built at your location, you can either choose to work in the office or continue working from home. This is strictly an online and work from home job the working hours are flexible and you can chose to work from anywhere of your choice, the pay is \$65.85 per hour and training is \$50.50 per hour and will be get payment bi weekly via direct deposit or paycheck and the maximum amount you can work a week is 45 hours. ,if you are employed you are going to be working as a full employee and not an independent contractor. I believe working from home will not be a problem for you ?

And then he discussed benefits and flexible conditions:

Benefits: Health, Dental, Life and AD&D Insurance, Employee Wellness and 401k plans. Paid Time Off and Holidays with Generous Company Discounts

Working hours are flexible, all activities and corresponding time are to be recorded in excel spreadsheet. As for your duties, I will assist you with any difficulties by email.

I asked for some details on the health plan and he told me it was Anthem Blue Cross Blue Shield, which isn't available in my state, but he doesn't know that and I didn't correct him. He then spent about 30 minutes pasting in legitimate interview questions such as "How do you ensure data quality and accuracy in your analysis?" and "Can you describe a time when you had to communicate complex technical information to a non-technical audience?" – which look to have been lifted from [a site like this](#).

I gave a few good answers, but after determining he wasn't following up, I gave a few wildly incorrect answers to see if it fazed him (for example, he asked me about what data visualization tools I was familiar with, and I told him Photoshop and Illustrator).

David was not fazed.

We went over a few other details and he asked me to meet with him again via Teams at 10 AM the next day.

I will need you to report online here on teams tomorrow morning 10am EST because I need to forward our conversation to the Superior Department to enable them see if you are committed and good for this job.

The Superior Department would be a great band name.

Again, to not appear overly eager, I told him I needed to push it to 11 AM, which he agreed to.

Attempting to Shut Him Down, Part 1

I found a Microsoft fraud reporting through their website. I shared the email and explained the situation. The customer service rep opened a ticket for me but told me the Teams team has to handle these situations. He told me to report the conversation in Teams, and reference the case number he opened for me.

Microsoft responded “We’ve determined that it was not a violation of our [terms](#). If you are still concerned about another user’s shared content, please report it once more.”

It appears I had to dig a little deeper.

Follow Up Meeting with David Jeffries

David and I met at 11 AM the next day and I received great news, I was hired.

You are now given a chance to show your commitment, charisma, diligence and be a productive employee.

He had me at charisma.

David walked me through the details, but asked me for a home address. Now, my city and state are on my resume, but not my home address. I gave him a random address in my town, and he seemed satisfied. He thought he had me on his hook, because now the scam began.

*You will be provided with the latest Apple iMac (M2 Chip) 24” and MacBook Pro 16” (M1 Max), Sony Mas-A100 beamforming microphone, AKG K712 Pro Headphones and your **Agile’s** Time Keeper device from our authorized vendors whose installers will be coming over to set up your office for you.*

Here is the cost of your equipment being provided to you. Apple iMac 24” (M1 Chip) - \$4698 MacBook pro 16” (M1 Max) - \$3660 Sony Mas-A100 beamforming microphone - \$2500 Virtual Presence 2.0 - \$890 AKG K712 Pro Headphones - \$595 and the reason we provide nothing short of the best for our employees cause we firmly believe that better matters! With the list and names of the software suites you will be using for work. Your bundled software suites pack and codecs on the other-hand costs \$2,989 and I’ll provide you with the full list as we proceed for your reference.

Your funding will also include your employee sign-on bonus of \$300 which you are to take out for yourself. Once you have been cleared by the HR desk, finance will issue a check for \$15,642 to you and it will be mailed to your address. Mind you, this will serve to cover your working materials order from our authorized vendor, shipment fee, and your sign-on bonus and is not to be used for any divergent purposes otherwise. I believe I am well understood?

Now, the way this scam works is they mail a check, and expect you to cash it. You may not realize it, but checks do not clear immediately (as someone who was on eBay as far back as 2000, this is very familiar to me). This is the reason when you do a mobile deposit, your bank tells you to hold on to the check. [See more information here](#). The check is a bad check and will bounce.

However, before the check bounces, they will push me to send money to their “vendor” for equipment which I will never receive. Then their check bounces and I am out that money.

I decided to negotiate a little bit, and negotiated an extra 7 PTO days a year, and he told me he would overnight the check to me. I panicked a bit; I knew I would not receive this fake check, so I thought fast and told him I’d be willing to lay out the money up front since the check is in the mail.

I could almost hear him salivating! He told me I would need to send a payment of \$4000 to his vendor through Zelle, and I pretended to not know what Zelle was to waste his time a bit. He bit! He gave me the email address and name on a Zelle account, and I told him I would order in the afternoon.

Following up with Zelle and Microsoft

I called Zelle's number, but there isn't easy way to get a customer service rep on the phone. Their website says "If you have been a victim of fraud or scam you may use the form below or call us at 1-844-428-8542 to report your experience" – but there are no menu options to report a scam or talk to a representative, so I had to hack my way through the menus. I finally got a representative on the phone. I explained the situation and provided the email address, name, and details on the scam, and walked him through the evidence I had gathered. He was surprisingly grateful for me for taking the time to log and report it and said he forwarded the account to the fraud team with the highest priority.

Microsoft, on the other hand...I reported the message that specifically asked for money (you can't seem to report a user, just a message), and I received a message "We've determined that it was a violation of our [terms](#). Appropriate actions have been taken with the individual responsible for the violation. Thank you for reporting your concern and helping us maintain a healthier Microsoft community. "

I thought that had done it, but he was still online answering messages, so I'm not sure what "appropriate actions" were taken. I went back and reported another message (it's referenced below; one that ChatGPT identified as a "likely scam") – once again, Microsoft thanked me and said appropriate actions were taken, but David is still online and responding.

Takeaways

How did scammers find me?

I do most of my applying through LinkedIn, so I went through my "Applied" and "Saved" jobs and had no evidence of applying for this position. I wonder if they set up an account, posted a job, and then it was flagged as a scam. As job seekers know, there's a lot of pressure to apply quickly to a job before it closes, so I am assuming this is what happened. If that's the case, I wish LinkedIn would have informed me I applied to a scam job.

How did Zelle handle it?

They obviously aren't going to tell me what happened, but I am hoping their fraud team shuts down the account and makes the scammers work a little harder to find a new money mule. They need to have an option when you call to get an operator to report a scam, though. I sat through menus, tried the old "hit zero a bunch of times" trick, and finally got through by going through a menu saying I received Zelle funds but my bank doesn't support Zelle payments.

How did Microsoft handle it?

David is still online in Teams. The whole conversation is an obvious scam. I even asked ChatGPT, who Microsoft is invested heavily in, to weigh in. I pasted this part of the conversation into ChatGPT and asked, is this a scam?

Here is the cost of your equipment being provided to you. Apple iMac 24" (M1 Chip) - \$4698 MacBook pro 16" (M1 Max) - \$3660 Sony Mas-A100 beamforming microphone - \$2500 Virtual Presence 2.0 - \$890 AKG K712 Pro Headphones - \$595 and the reason we provide nothing short of the best for our employees cause we firmly believe that better matters! With the list and names of the software suites you will be using for work. Your bundled software suites pack and codecs on the other-hand costs \$2,989 and I'll provide you with the full list as we proceed for your reference.

Your funding will also include your employee sign-on bonus of \$300 which you are to take out for yourself. Once you have been cleared by the HR desk, finance will issue a check for \$15,642 to you and it will be mailed to your address. Mind you, this will serve to cover your working materials order from our

authorized vendor, shipment fee, and your sign-on bonus and is not to be used for any divergent purposes otherwise. I believe I am well understood?

ChatGPT was on it! Here was their analysis:

This message appears to be a scam for several reasons:

- *Excessive Costs and Equipment: The prices listed for the equipment are excessively high, especially for items like the Apple iMac 24" and MacBook Pro 16", which are priced significantly above their retail value. This is often a tactic used in scams to make the offer seem more substantial and valuable than it is.*
- *Unusual Payment Methods: Reputable companies typically do not send checks to new employees to cover equipment costs, especially before the employee has officially started working. Companies usually provide equipment directly or reimburse legitimate expenses through established payroll or reimbursement systems after proper documentation.*
- *Sign-On Bonus Included with Equipment Costs: Including a sign-on bonus in the same check as the equipment costs and shipment fee is unconventional. Bonuses are usually handled separately through payroll.*
- *Instruction to Use Authorized Vendor: Scams often involve directing the victim to purchase items from specific vendors, which might be controlled by the scammer. This ensures the scammer receives the money.*
- *Emphasis on Immediate Compliance: The phrase "and is not to be used for any divergent purposes otherwise" implies an urgency and strict compliance, which is a common tactic in scams to pressure the victim into following the instructions without question.*
- *Overall Tone and Presentation: The message's tone, wording, and structure often appear informal or awkward for a professional business communication, further suggesting it is not from a legitimate source.*

I don't understand how this account hasn't been deactivated.

What are My Next Steps?

Well, I documented the story here, and I hope that this is interesting and this is educational for someone.

I reported another one of the messages to Microsoft's Trust and Safety team and I would have expected the account to be shut down or at least suspended by now. I'm going to keep pushing Microsoft.

I told "David" I'd reach out tomorrow to follow up; I'm hoping at that point his mule has been suspended, and maybe I can get another Zelle scam account out of him before he figures something is up.

I received another fake job offer over email, this one from Omnicell Inc, another healthcare company I didn't apply with (makes me wonder, why healthcare?). I have an invite to interview with Mr. Connor Millstone for another position and I've been in communication with Omnicell to let them know.