



Take on Board Podcast – Episode 379

Transcript – Helga goes solo: Phishing scams targeting board professionals

Hello, and welcome to the Take on Board Podcast. I'm your host, Helga Svendsen. I know that being on a board can be an incredibly valuable, interesting, and exciting experience. Yet, it can also be lonely, challenging, and let's face it, pretty hard. So here at Take on Board, I'll bring you weekly tips, tricks, and advice to help navigate your way onto your first board, your next board, or to build your governance wisdom. Now, on with the show.

Hi, folks. This week on the Take on Board Podcast, I want to talk to you about phishing scams. This is where you receive the email in your inbox or maybe in your LinkedIn messages, but more likely, I reckon, in my experience, in your inbox, that either has an offer that is, well, quite frankly too good to be true, or maybe it's a bit smarter than that. Not quite too good to be true, but looks interesting and asks for your help. Folks, there are more and more phishing scams. In the last month or so I've had six land in my inbox, uh, all tailored for me and my information, and they are coming with increasing frequency. So I expect there will be more in the future.

So I wanted to address that here, to share with you some of the things that I've been told about it, both phishing to me directly, but also what I'm hearing for the community, and some ideas about how you might avoid it.

So first up, there's a couple of different approaches that I'm seeing. Some are loud and flashy and, as I say, quite frankly, too good to be true. Others are a bit smarter, and I want to give you a couple of examples.

So option A, the too good to be true option. Here's an email or excerpts from an email that I received recently. "I'm reaching out to you because I'm currently leading a retained search for a chair of board position for a prominent enterprise based in the USA." Okay, interesting. Don't normally get approaches from the USA, but, hey, you never know. Uh, watch out for the too good to be true. "Offering an attractive compensation p- range of 700,000 to two million." Really? That is totally the too-good-to-be true. I'm assuming they're talking US dollars as well, not our beautiful Aussie dollars.

Goes on to say, "Given your role as chairperson of the Workplace Injury Commission and your insights from hosting the Take on Board podcast," hi, folks, "uh, your qualifications, including a Bachelor of Laws from Monash University, make you a remarkable fit." Oh, my goodness, folks. I am a remarkable fit for the chairpersonship of a prominent enterprise earning 700,000 to 2 million US dollars. Really? No, not really. Obviously too good to be true because it is too good to be true.

Why does it fail the sanity test? Ugh, so many reasons. So obviously that is a massive compensation. Obviously that is a massive compensation range, like a range of 700,000 to 2 million, and you put that in the very first email that you're approaching people. Like, no, that is not what happens. Thirdly, as I say, related to point one, it's a massive compensation. It is in the top .1% of paid board roles. Now, the top 1, .1% of paid board roles are not reaching out to people from a Gmail, I'll have you know, and reaching out to people cold in this way. That is just not the way that works. So obviously there was a number of red flags in there that just made me immediately block and delete.

Well, not quite delete, because I wanted to use it for this podcast.

The other thing that I noticed in there, and more subtle red flags, I guess, no recruiter name in the sign-off, no search name mentioned, no domain credentials, no client name. Now, the last one, no client name. Look, it is pretty common for search firms to do board roles without saying what the client name is. That's pretty common. Um, they might tell you down the track, but not first up. Uh, but all of the other stuff is a bit of a red flag. So easy, block, delete. Too good to be true is too good to be true, right?

The second one, though, a bit more subtle I'm reaching out personally regarding a confidential board level mandate I'm currently supporting. At board level, I look beyond the number of appointments held to understand the quality of judgement a candidate brings. Ooh, okay, they are a very discerning recruiter. Interesting. Read on.

Your current chairmanship... First red flag. I never say chairman. Of course I never say chairman. You know that. Who would say chairman? You are the chair of the board. Anyway, your current chairmanship of the Workplace Injury Commission, together with your previous role as, as chair of the Victorian Asbestos Eradication Agency and non-executive responsibilities at the Women's Hospital, and your earlier work with the Australian Services Union. Ooh, okay, they know a lot about me.

They then smart a low pressure close. I appreciate that your existing commitments may limit your capacity for additional appointments. Nevertheless, I would welcome the opportunity to share further context. I'd be interested in hearing your perspective. Oh, you just want to hear my s-perspective. You just want to share some cont- context. You just want to explore. Who wouldn't be up for that? Well, you won't be up for it now, and I'm not up for it because we know it's a phishing scam.

Now, why is this one a bit more insidious and a bit more dangerous? It doesn't talk about money, which makes the red flag a bit harder to see. It uses genuine governance phrasing, constructive challenge, accountable decision-making, judgement, blah, blah, blah. So it uses all of the beautiful governance terms, quite frankly. And it beautifully, that close, it acknowledges my limited capacity. It's a classic psychological trick to make the offer feel way more authentic rather than pushy, so I don't feel like I'm being pushed into something. I feel more flattered, and I might just have a yarn, and hey, you never know, it might turn into something

So folks, why are you receiving more of these? Well, obviously, it's AI scraping the web, right? But what's the end game? What's the push for this? There's a couple of things. There's three things I can

think of, and I'm sure you out there in the Take on Board community have some other ideas about this as well.

Firstly, they're fishing to push their services. So if you respond, "Here's my resume, here's a chat." "Oh, your resume looks amazing. However, we need it in a particular format, and we have this awesome service that might be able to support you to make it that way." Or, "You might just need some extra help to shape it in this way," or whatever it may be. So they push services to help you shape up your application. Often they are not highly priced services because they are doing this to tons of people, right? So they get 50, 100 bucks, 500 bucks from everybody. Woo! Off you go. They are pretty amazing. Sometimes they are higher priced, but, uh, sometimes the aim is just to get 50 bucks from every sucker who responds, and that turns into a fair bit of money for them.

So obviously, it is some sort of audit fee or service fee or support fee is, is one aim of this.

Secondly, it might be around identity and credential harvesting. So they just want to make sure that you are who they think you are, and they might even ask for additional ID. "Oh, to apply for this incredible role in the US, if you could just provide a copy of your passport, your driver's licence, your Medicare card," whatever it may be. So sometimes to get before the remuneration committee of this incredible organisation, you need to do some pre-identity checks. So definitely be on the lookout for people who are requesting that sort of information.

Thirdly, they might just, heavy inverted commas, be profiling you. They might want to see if anybody responds from that email address. They want to make sure it is your email address and the correct one. They might just be testing those sorts of things. So I really, really, really... If you think it is a scam, do not respond and say, "Hello, I think you're a scam." Do not respond. Do not respond. Block, delete. Block, delete. Block, delete. Or send it to me, and I'll use it as a podcast. Anyway

So what can you do about this? If these are landing in your inbox more often like they are for me, what should you do? First up, never respond immediately. Take the time to think. Cross-reference. Search the recruiter on LinkedIn. Uh, are they a verifiable firm? Are they a verifiable person? Do they really exist? Check the email address that it came from. As I said, if it's a Gmail, well, no recruiter worth their salt is using Gmail as their email, so that is a red flag. Check the domain that you are being sent to. Is it actually the recruiter or not? And check the network of the individual if you have it. Check it via LinkedIn or whatever it may be.

Now, none of those are foolproof because you can... I don't know, I'm not a tech person, I don't know the right words, but you can clone websites or whatever it may be. And in fact, one person, you'll hear about them in a moment, that I spoke to, they rang the recruiter, you know, the landline, and said, "Hello, recruitment firm. I have purportedly been contacted by Mary Smith of your firm who says X, Y, and Z." And they went, "Oh, no, that is not us." So there can be identity theft of the recruitment firms as well. So check, double-check, triple-check, quadruple-check everything, particularly if they are asking you for identity...

Well, before you respond in the first instance, but if you respond in the first instance and then they start asking you for ID or if they start asking you for money, red flag, red flag, red flag

So I will say, though, if you do fall for it, even in the short term, happens to everybody. I have heard of people who were deep in tech falling for a number of scams. So it happens. Don't worry. Well, yeah, be careful, be careful, be careful. But if you do fall for it, I encourage you to have the growth mindset of one person that I spoke to recently who said, uh, she was the one where the recruitment firm was cloned, I guess, and she rang them.

So she came back and said, "It was a scam." How very embarrassing for me. But also, the AI recruiter who stole a real recruiter's identity forced me to get my board CV up to date. So I guess it could have been worse. And I should say she didn't pay for that. She did that herself. She just got her board resume up to date. Always a good thing to do if you're in the mix for board roles.

I would also say for those of you in the Take on Board community who are in the recruitment game, who use recruiters, who know recruiters, encourage them to make it very clear on their websites what they do and don't do and how they do and don't approach people because I think if you are getting these sorts of things that are purportedly from a recruitment, if you can go to the website and it says, "We will never reach out cold. We will never ask you for money. We will never do this." That helps you to know it's a red flag and a scam.

So I think this is, you know, generative AI is making this easier. It makes shall we say, custom flattery cheap, scalable, accessible. So if it feels like it was written just for you, it absolutely was by scraping all of your LinkedIn data, and it's a script that is just going out to loads of people.

Now, finally, I will say, yes, they're scraping your data probably from LinkedIn. To me, that is not a reason to get off LinkedIn. LinkedIn is a valuable tool. It is useful. It is used 99% legitimately, 1% illegitimately. So it's not, in my humble opinion, not a reason to get off LinkedIn, at least not yet. Let's see how it progresses. It is a reason to check, double check, triple check, quadruple check.

So folks, hope that's been helpful. I hope you haven't had some too good to be true offers land in your inbox. Uh, if they have, I would love to hear about it. If you've had different types of phishing, I would love to hear about it. If you've got some different ideas about how this can be dealt with, well, I would love to hear about it. May your inbox be full of legitimate offers and awesome advice as opposed to crappy phishing scams. And that's it for this week. Look forward to seeing you next week on the Take on Board podcast, and please feel free to get in touch if you've got some insights about this topic or any other topic. Thanks, folks. See you next week

So that's a wrap for the Take on Board podcast today. Thank you for being here and for being part of the community. I do this podcast because I love bringing good women and gender diverse peoples together. So I invite you to join us over in the Take on Board Facebook group, an active group that helps, supports, and cheer squads each other. Just search Take on Board in Facebook to find us. Or you might like to let me know your email address, and you'll then have the Take on Board times and the Take on Board community's digest delivered straight to your inbox.

You'll also get advance notice of events and programs so you can meet others in the community.

Finally, I'd really love it if you could do some of the podcast things. Share this podcast with someone you know who you think might get some value from it. Subscribe if you haven't already, either on podcast or over on YouTube, and I also love it when people rate and review. Thanks again for being

part of the Take on Board community. Now go and put these tips, tricks, and advice into action so you can be your best in the boardroom.

This transcript has been automatically transcribed by [Descript](#).