Lure: Ziprecruiter job opening: HR Generalist, Remote, Premiere Digital.

Premiere Digital Services appears to be an actual SaaS company, with offices in California, Connecticut, and Bangalore. Bloomberg has an entry on PDS which comments, “cloud-based digital asset delivery and content optimization solutions that enable content ingestion, preparation, management, and distribution of media assets to mobile and broadcast markets. Premiere Digital Services serves media and entertainment industry worldwide.” Their website is premieredigital.com/

First Contact: I received an email two days after submitting my application. The email informed me I was being considered along with other applicants. (attached: “Interview Invitation”) The email (from talent.acquisition@premieredigital.org) was signed “Matthew Scott L., Talent Acquisition Head;” there is a Matthew Scott T. who appears to have a private LinkedIn profile at: https://www.linkedin.com/in/matthew-scott-t-b0366021a , and who DOES appear to be a talent acquisition officer. Emerging question of, to what degree of authentication is necessary to verify the identity of a “person” engaging you online?

Further information was provided as a pdf (attached: “PDS Invite”). A company logo from the PDS website had been reused in the upper left corner as a letterhead, though no other letterhead was visible. The email provided information for a virtual interview with a woman named Alma Padilla, who appears to be an actual employee of PDS; searching her name brings up a LinkedIn page (attached: “Profile – Alma Padilla”) at https://www.linkedin.com/in/alma-padilla-4824a5203/

Syntax in both the email and the attached pdf were good, though *slightly* off from native English; some confusion with complex verb tenses (future and perfect) was present, as well as some inconsistency in capitalization. The largest red flag here was the phrasing “participate in the interview,” as well as the fact that the signature for the head of acquisition was not any more elaborate than bolded italics.

Skype Interview:
The interview was set for the next day, or the day after. Once I connected with Alma via Skype, I was informed that the interview would be “written.” Upon my consent to a written interview, “Alma” kindly provided me with the above Bloomberg description of PDS, as well as some publicly available information about company location and what I suspect is a piece of ad copy from their website. The interview was very basic, with no followup questions asked (attached: “Transcript – PDS Skype Interview”).

After the interview, I was directed to fill out an assessment (Attached: “Google Survey – PDS”) and await further communication. I did take the opportunity to practice my job interview spiel--if you’re an HR manager reading this, please grade my answers ;)

Followup:
24 hours after the text “interview,” I received a follow-up email (attached: “Talent – Job Offer”) containing another pdf (attached: “Offer Letter”), which included a more elaborate letterhead. Once again, the grammar and construction of the letter were convincing, though again with some slightly odd constructions and inconsistent use of capitalization (the “H” in “Holiday pay” was capitalized, but not the P, for example; a great example of why they appear to need an HR generalist).

This email asked that I sign the offer within 3 days and send it to a second email address, ostensibly belonging to a Joanna Hoggan (joanna.hoggan@premieredigital.org) (Joanna Hoggan appears to genuinely be the head of HR at Premiere Digital Services, with a LinkedIn profile visible at: https://www.linkedin.com/in/joanna-hoggan-mlis-mhrd-5912b312/, in keeping with their strategy of utilizing the names of actual people) (attached: “Profile – Joanna Hoggan”). I did so.

Closing Contact:
Within the day, “Joanna” wrote back and told me to await further instructions (attached: “Joanna_Hoggan_Correspondence”). The writing and grammar of this final contact were notably poorer (in particular note “You will undergo 3 days online training and orientation. Where you will learn, interact, and ask questions about your role.”), and sure enough, on Monday I was contacted again and given information on how to go about getting the necessary equipment for the role:

“We will assign you a vendor that's accredited. They will be responsible for shipping, installation and repairs during the course of your time with us. However, this is our procedure.
We will send you a check for the estimated amount on the invoice, after the check has been deposited, we will send you the vendor's details and you will make payment for the equipment, you will get tracking number immediately the equipment has been shipped. Also, the check will be scanned and sent to your email, you can deposit it directly using your mobile banking app (The feature is called remote/mobile deposit). we implemented these to save time waiting for check in the mail and the long trips to bank. I will assign a vendor now and also prepare the invoice for the equipment.”

This is a fake check scam. A less skeptical “new hire” will enthusiastically deposit the fake check into their bank account via a virtual banking app. As required by law, the bank will make funds from that check available within a few days while their fraud team continues to investigate. “Joanna” will then provide the name and information for their “vendor,” along with an invoice for the “new hire” to pay in order to receive their equipment.

The victim sends their money off to the bank information provided, assuming all is well. But eventually, the fake check will bounce, and the bank will withdraw that money from the victim’s account, leaving their balance reduced by whatever amount they sent in response. The victim will be the only one taking a financial loss as a result of this scenario.

Analysis:

Skype Interview (cont)

Communication was carefully constructed using publicly available information, including the names of several verified employees at a very real company. Assets from the company website were used to provide authentic-looking corporate letterhead, with convincingly corporate-speak onboarding and interviewing messages. The name of Joanna Hoggan appears to have been picked specifically for her very active LinkedIn profile.

Further, Premiere Digital Services *did* in fact have an opening for an HR Generalist posted on LinkedIn, which appears to have been copied over and used as the template for the Ziprecruiter post; the individual or team behind this spearphish is likely copying other legitimate job openings to generate new leads off job aggregate sites like ZipRecruiter.

As mentioned, this team or individual was also very good at cultivating a subtle sense of urgency: Saying the opening has been "closed" to consider "other applicants" as well as the target, setting an interview for the next day/day after, sending immediate offer with a deadline to respond after the weekend. While I was cultivated as a lead for some time before being offered the scam, the actual investment of effort to maintain each ongoing lead was probably fairly minimal, and required only putting my name on a document. Once the materials for this phish were created, the biggest challenge would have been not sending the wrong name on an acceptance letter (and likely, making sure to pick the right false information for the right scam; as we'll see below, this is not the only operation this group is running).

Commentary on Domain Fraud:

Both "Matthew" and "Joanna" contacted me from what appeared to be legit emails, but the .org extension struck me as an unusual one for a multinational media company, so I probed into it a little. The email domain name "premieredigital.org" was registered through Namecheap, Inc (source: WHOIS lookup)(attached: "WHOIS domain lookup – premieredigital.org") on Jan 5th, 2022.

The domain appears to have been registered through an Iceland-based service called WithheldForPrivacy, which advertises discreet domain registration without needing to share a Whois. Namecheap Inc. uses WithheldForPrivacy's service.

NameCheap Inc appears to have multiple lawsuits filed against it by a variety of entities, including Facebook and a law firm known as Debevoise & Plimpton who is accusing NameCheap of cyber piracy via co-opting their brand name and the names of several of their attorneys as part of a similar phishing scheme.

Legal Commentary:
For the actual legal details, check out Debevoise & Plimpton LLP v. debevoise-law.com, U.S. District Court for the Eastern District of Virginia, No. 1:21-cv-01386, or Facebook Inc. v. Namecheap Inc., No. 2:20-cv-00470-GMS (D. Ariz. Nov. 10, 2020). Facebook's case against NameCheap and Whoisguard was settled out of court on March 15, 2022.

Conclusion:
Right now, with everything going digital and hiring trends up in the air, there's a lot of confusion about how companies are onboarding new employees. But "talking to a real person" should ALWAYS remain part of the process. It's important to be highly skeptical of any hiring process which doesn't include at least a phone conversation, and the "text-only" interview should be a huge red flag for jobseekers.

Most of these phishing schemes seem to originate from countries with primarily non-native English speakers. As a result, even the best-written (and this was up there!) will have syntax which is in some way "off," which a native speaker might experience simply as being somehow indefinably weird.

Trust your instincts! Scammers give themselves away in little ways; unenthusiastic responses, spelling mistakes, poor grammar. Stay sharp and try to ask yourself, "is it too good to be true?" Getting a job offer after a text-based skype interview definitely qualifies.

Also, don't give people checks over the internet.