INSIGHTS

Cyber made simple.

one brightly cyber

JOB SEEKERS ARE SCAMMER TARGETS

BY JAY BORDEN

Being out of work is challenging enough. But now scammers are preying on job seekers.

The scams take different forms. They may be job ads on LinkedIn or Facebook, or links that come in phishing emails.

Or they may be fake websites that closely resemble a popular site but the address has a minor difference. For instance, Monsster.com in place of Monster.com or Monster.cm. So easy to miss but so damaging to anyone who goes there. Another method called domain masking displays one address but content from another site is displayed. Be aware, there are additional methods to disguise the real address of a page.

The point to remember is that the url you see, or think you see, may not be the one that you are really viewing.

Another trick is to tell the applicant to download a form that needs to be completed and submitted. That form usually comes with various types of malware to infect your device. A variation on downloading a form is to ask the recipient to click a link and complete an online form.

The goal of these scams is to collect private information like name, physical address, email address, social security number, bank information, etc and to download malware onto your device.

Above we described the methods they use. But how do they get people to fall for these scams? Sadly, its easy, especially in an uncertain job market. The posted jobs offer high salaries and the ability to work remotely. High salaries are always in demand. Remote work is a hot lure today as more companies are demanding people return to the office, RTO, at least a few days a week.

onebrightlycyber.com
(888) 773-1920

INSIGHTS

Cyber made simple.

JOB SEEKERS ARE SCAMMER TARGETS

Continued

If someone is either out of work already or knows their current position will end shortly they are very interested in getting another position quickly to prevent periods with no income. This often leads to forgetting basic security.

What are the red flags to look for? Salaries above the norm for the position. Fully remote with no need to be in the office. More benefits than usual.

Remember to look carefully at the url for simple misspellings or other variations to a company name.

Sometimes these fake positions will ask you to pay for equipment or background checks, or training needed for the position. Legitimate companies will never ask you to pay for these things.

Another red flag is if things move very quickly. Many have experienced how slow it can be to apply for a position and receive any reply. And if you get any interest, how slow it still progresses. If you don't have direct experience, you probably know someone who was in that position and complained about the snail's pace when they need the job. If things are moving very rapidly at any point, such as being offered the position after one interview over the phone or Zoom, no matter how nice it may feel, immediately step back and reevaluate the situation. The intent goes back to not wanting you to have time to think.

Never believe you are above this type of scam or too sharp to fall for it. Even cybersecurity professionals have almost gotten caught. They start down the path and all of a sudden, stop and realize what is happening.

The Better Business Bureau suggests verifying the position by going directly to the company website. Or call the company using a publicly available phone number on the company website.

Remember, never click any link or call any phone number in the email or on the ad. Even if it says calls will not be accepted on any other number.

We wish you the best of luck in finding a new position and hope you do it safely.

Need help or guidance? Learn how we can help you in so many ways.

Contact onebrightlycyber at info@onebrightlycyber.com or call (888) 773-1920.