**From:** DCF BWF Work Programs Help Desk <BWFWorkProgramsHD@wisconsin.gov>
**Sent:** Wednesday, May 5, 2021 9:06 AM
**To:** DCF DL DFES BWF W-2 Agency CARES Coordinators <DCFDLW-2AgencyCARESCoordinators@wisconsin.gov>; DCF DL DFES BWF W-2 Agency Directors <DCFDLDFESBWFW2AgencyDirectors@wisconsin.gov>; DCF DL DFES BWF W-2 REGIONAL STAFF <DCFDLDFESBWFW-2REGIONALSTAFF@wisconsin.gov>
**Subject:** Cyber Employment and Grant Scam Information

Good Morning,

Fraudulent cyber employment scams have increased in the past year with over 16,000 victims in 2020 totaling more than $59 million in losses according to a recent FBI warning released this April. As of early March 2021, there had already been over 2,300 victims nationwide of cyber job scams. It is important for us to be vigilant and inform our W-2 participants of these scams targeting job seekers.

Scammers often pose as existing legitimate companies; they create fake job postings and sometimes have spoofed websites. They post hiring advertisements on popular online job listing platforms, such as Indeed.com, Craigslist, and Monster.com. The FBI reported that victims have said cyber criminals impersonate different company personnel from recruiters to human resources and department management, and even go as far as interviewing and "offering" a position. While these scams often may seem legitimate, there are key red flags job seekers should be aware of:

- Job posting appears on job boards, but not on the company's website.
- Emails from the potential employer use a non-company email domain or are unprofessional, containing errors in spelling, grammar, and capitalization.
- Emails do not contain contact information.
- Interviews are not conducted in-person or through a secure video call.
    - Nonsecure messaging services are not used by legitimate companies.
- The potential employer asks for confidential information.
    - Banking or credit card information, Social Security number and birthdate.
- Recruiters or managers do not have profiles on the job board, or the profiles do not seem to fit their roles.
- Potential employer asks applicant to pay for something in order to apply.

Additionally, W-2 participants should be aware of cyber scams which advertise free government grants, enticing people to call a toll-free number. Grant scammers also call individuals about fake grants to get credit card or banking information from the individual, claiming to be from a reputable agency. The Federal Trade Commission (FTC) has stated that "money for nothing" grants are almost always a scam and individuals should never give out any personal information, unless they are familiar with the company and know why the information is necessary. To avoid scams via phone, FTC recommends adding your phone number to the National Do Not Call Registry. For more tips to avoid a grant scam, please visit the U.S. Department of Health and Human services avoid grant scams webpage.

Please take a moment to read the ten warning signs of an employment scam in the attached graphic, and please feel free to share this job scam what to know website.

Cyber job scams can be reported to the FBI El Paso Field Office at (915) 832-5000 or visit the FBI's Internet Crime Complaint Center at ic3.gov.

Complaints regarding government grant scams can be filed with FTC online, or by phone at 1-877-FTC-HELP (1-877-382-4357).

This email will be posted to the BWF Work Programs Help Desk Home Page.

# 10

# EMPLOYMENT SCAM WARNING SIGNS

## THE JOB SEEMS TOO GOOD TO BE TRUE

**1** Scammers often post positions promising high salary, flexible schedules, work from home options, with no experience required. Many use vague job titles such as "Executive Assistant" or "Business Analyst".

## YOU'RE HIRED BEFORE INTERVIEWING

**2** Legitimate employers rarely offer candidates a position without conducting at least one in-person interview. Phone and IM messaging interviews are NOT in-person interviews. Beware if your request for an interview is denied.

## SIMPLE QUALIFICATIONS

**3** Avoid offers for which the job requirements are so minimal that nearly every person qualifies (i.e., 18+ yrs of age, valid drivers license, access to internet, U.S. citizen, etc.)

## PERSONAL ACCOUNT INFO REQUESTED

**4** Be cautious of any employer who requests bank account, credit card, passport, social security and/or drivers license numbers as a condition of employment, especially if the information is requested over email or phone.

## POORLY WRITTEN EMAILS

**5** Be on guard for employment-related emails written with poor grammar, spelling, verb usage, or with sloppy formatting and sentence structure, as well as those containing simple signature lines.

## HIRING WHILE "AWAY ON BUSINESS"

**6** Be cautious of recruiters who hire while claiming to be out-of-state or overseas "on business". These people will often say they are unavailable to interview in-person due to busy travel schedules.

## USE OF GENERAL EMAIL ADDRESS

**7** Legitimate hiring managers will not use personal email accounts to conduct professional business or to communicate employment information with job applicants.

## EMPLOYER ASKS YOU TO CASH A CHECK

**8** A common request of fraudulent employers is for you to accept a mailed check, cash it, and then either mail the money back to them, or wire the money to another individual. Never accept this type of job offer.

## WEBSITE DOMAIN NAME IS OFF

**9** Fraudulent employers create websites that appear identical to those of well known companies by copying the content and simply altering the web address by one character. Do your research and make sure the website is legitimate.

## THINGS JUST DON'T ADD UP

**10** Don't allow the allure of these "too good to be true" jobs to cloud your common sense and good judgement. If something feels wrong, there's likely a reason. Take your time accepting the job offer, and do your homework!