HR Insights

Brought to you by the insurance professionals at
Highpoint Insurance Group

Unemployment Scams

The presence of unemployment-related scams has grown in the wake of the coronavirus (COVID-19) pandemic. Current unemployment scams include both fraudulent claims and unemployment-related phishing attempts. As many employers are currently dealing with the reality of a high amount of unemployment claims, organizations can take steps to prepare for fraudulent activity and to accurately identify legitimate requests. By taking proactive steps and preventive measures, your organization can be best prepared to identify and, if necessary, respond to fraudulent activity.

The Presence of Scams

According to the U.S. Federal Trade Commission (FTC), scammers often file fraudulent unemployment claims, sometimes even for people who are not unemployed. And, unfortunately, many scams are not revealed until it is too late. Many scam artists may not even be located in the United States. With the coronavirus pandemic leading to unemployment rates as high as they've been since the economic crash in 2008, more unemployment claims are being processed than ever before. Scammers seek opportunity, and this niche has received enough attention to warrant a fraud alert from the FTC.

How Scams Happen

Unemployment-related scams can happen to a current or former employee—regardless of an employee's role at an organization. While scams were also present pre-coronavirus, current unemployment scams primarily fall under the following categories:

- **Fraudulent unemployment benefit claims**—These are false claims filed using the personal information of an employed or unemployed individual. This type of scam can allow a scammer to receive someone else's falsified unemployment benefits.
- **Phishing attempts**—These generally come in the form of emails sent with the intent of tricking people into giving away personal information. This may allow scammers to:
    - File fraudulent unemployment claims.
    - Change bank account information on legitimate unemployment claims.
    - Steal additional personal information.

Employers should be prepared to identify these types of fraudulent activities. By educating workforces, reviewing emails with caution and preparing appropriate scam responses, organizations can be better prepared for attempted fraud.

Preventing Scams

Employers can take certain steps, such as the following, to help prevent fraudulent activities:

HIGHPOINT
INSURANCE GROUP, LLC.

This HR Insights is not intended to be exhaustive nor should any discussion or opinions be construed as professional advice. © 2020 Zywave, Inc. All rights reserved.

- **Educate employees on how to identify phishing attempts**—By building awareness of how to identify scams, employees can help prevent fraud. Employers may consider providing formal educational opportunities on how to identify phishing attempts and highlighting the importance of this topic using internal employee communications.

- **Train appropriate teams on how to identify unemployment claim scams**—By investing in specific training sessions, employers may be able to help designated teams look out for common scams. For example, HR professionals who will be administrating or responding to unemployment claims should be well-informed on current scam tactics.

- **Review cybersecurity best practices**—The FTC provides guidance, including a guide for small businesses, that organizations can use to help determine the best steps to take in their own organizations.

- **Communicate effectively with employees**—While strong practices, education and training sessions can help prepare your workforce to prevent scams, employee buy-in will be key to effectively preventing fraudulent activity. Ensure education and communication regarding scams are ongoing initiatives so that employees remain up to date on how to help prevent scams.

Employers should be aware that there has been falsified information about unemployment scams being shared on the internet. Federal agencies, including the FTC, generally provide the most accurate and up-to-date resources.

Organizations can take steps to prevent fraudulent activities—appropriate efforts will vary due to unique aspects of your workplace, but proactive measures such as increased awareness can be an effective first line of defense.

Identifying Scams

Government agencies and state representatives have standardized forms of messaging, which can be recognized by going through proper steps. According to a fraud alert issued by the DOL, the intent of phishing scammers is to have email recipients log in to an illicit account that impersonates the users' personal accounts in order to steal various account numbers, passwords and Social Security numbers. Here are key points that employers should consider when receiving emails or evaluating unemployment-related internal practices:

- **Hover on and review links, but don't click**—By moving a mouse cursor over a link, you'll be able to see the link without clicking and going to a potentially fraudulent site.

- **Know that state workforce agencies do not use secondary accounts**—Real government agencies do not ask users to log in to external sites and will only ask for an email address if you are creating a user account on their websites.

- **Avoid following emailed directions to log in to a personal account**—Common sites for which scammers have requested personal logins include Google, Microsoft, Apple and more. By logging in to what looks like one of these accounts, you may be providing your personal information, including a password, to scammers.

Responding to a Scam

While employers and employees hope to avoid being victims of a scam in the first place, a timely and well-planned response can minimize damage and sometimes even prevent future fraudulent activity after a scam attempt does occur. The FTC offers the following steps for how to respond to a scam attempt:

- **Alert your workforce**—Alert your employees that a scam has taken place and remind them of the need to be cautious. Ensure that employees know where to direct any notice from an entity claiming to be a government agency. This may be to a specified resource, such as IT.

- **Report the fraud**—Best practices for reporting fraud vary by state, so check your state unemployment agency's website for the correct instructions.

- **Retrain teams on what to look for**—By investing in additional education on relevant scams, employers may be able to continue to help their teams look out for common scams.
- **Refer affected employees to identitytheft.gov**—By reporting any fraudulent activity, including any identity theft, victims can get step-by-step help and the resources they need.
- **Ensure employees are aware of cybersecurity best practices**—Effective cyber protection measures require buy-in from employees. Ensure employees are aware of how they can help prevent fraudulent activity.

Protecting Your Workplace

No workplace is immune to the threat of scams, and now is as good a time as ever to ensure your organization is taking adequate steps to both prevent and respond to any fraudulent activity. Employers should continue to follow guidance from the FTC and consult with local legal counsel when updating or changing policies. For additional resources, contact Highpoint Insurance Group.