A new trend is sweeping the nation since novel coronavirus (COVID-19) shut down our country, and we are not talking about Zoom Happy Hours. During a time when people are still trying to navigate remote working, e-learning, and surviving a pandemic, employers and staff now need to be aware of cybercriminals who continue to capitalize during this crisis.

NJSIG recently learned that there has been a significant rise in fraudulent unemployment claims. With unemployment at an all-time high, these fraudsters have been able to hide in the flood of data, and it has become the perfect storm for identity fraud. Scammers are now breaking into systems and filing fake unemployment claims in an effort to try and get benefits funded by tax dollars. These cybercriminals are taking advantage of school districts who may not be reporting to the district every day, hoping that they can get away with filing these fake claims.

If you have property coverage with NJSIG, and discover that this has happened at your school district, please contact NJSIG's Cyber Advocate, Anthony Fernandez at afernandez@njsig.org, as well as our cyber partner, Beazley Breach Response (BBR) (click here). We also suggest you contact your broker as well.

A few tips before reporting a claim:

- Be aware of patterns where it looks like there could be an incident.
- Be sure to note the date that you became aware of the fraud. This is very important due to the new policy year.
- Be sure to take down all important information.
- Prepare to have payroll/HR and IT available when you are ready to call and submit the claim to BBR.

As always, be sure you are following best cyber practices:

- Be extra vigilant about phishing emails.
- Make sure your devices are up to date on their anti-virus protection and that you're using secure and known connections.
- Only use secure WiFi.
- Report lost devices immediately.
- Consider using multi-factor authentication passwords.

For further assistance on reporting unemployment fraud, click here.
To learn more about this trend, please click here.

School Reopening Guidance:

- NJDOE Restart and Recovery Plan for Education Executive Summary
- NJDOE Restart and Recovery Plan for Education
- Office of the Governor: Mandates & Announcements
- CDC School Reopening Guidance
- NJ Department of Education

COVID-19 Resources:

- Centers for Disease Control and Prevention
- World Health Organization
- New Jersey Department of Health
- Legionnaires Disease
- NJSIG COVID-19 Resources

Wire or Money Transfer Fraud

Some scammers trick you into wiring or transferring money to steal from you. Never wire money based on a request made over the phone or in an e-mail, especially overseas. Wiring money is like giving cash—once you send it, you can't get it back.

Email accounts can be compromised. If you are considering wiring money, be sure to verify the wire instructions by calling the intended recipient directly or discussing it in person. And be suspicious of any correspondence that asks you to respond "immediately" or that claims that wire transfer details have been "updated."

To learn more about wire or money transfer fraud, and other coronavirus-related scams, visit the federal Consumer Financial Protection Bureau, at: https://www.consumerfinance.gov/coronavirus/avoiding-scams/

NJSIG Claims Off-Hours Emergency Hotline:
609-369-0535

NJSIG's Employment Practice Hotline Attorney (NEPHA Hotline):
201-623-1223

School Violence Response Hotline:
212-915-8639

24/7 Crisis Management Operation Center:
212-915-8630

Qual-Lynx
(Worker's Compensation Claim Reporting):
1-800-425-3222