Sheakley
THE HUMAN RESOURCES PEOPLE

COVID-19 CLIENT UPDATE

May 13, 2020

In an effort to keep you updated during the COVID-19 pandemic, we will be sending you updates on the latest developments. Please do not hesitate to reach out to your Sheakley HR team member should you have additional questions or concerns!

Cybercriminals and COVID-19

Cybercriminals are exploiting the coronavirus outbreak through a variety of phishing attempts. These schemes are meant to steal important and valuable financial and personal information or introduce viruses and malware into your companies computer networks.

Hackers are sending malicious e-mails that seem to be coming from reliable sources such as the CDC and WHO. They are also doctoring e-mail messages to appear as internal, hacking systems and sending information "on behalf of the employee." Many organizations have released warnings about coronavirus phishing scams.

Sheakley has seen an uptick in hacking attempts, specifically related to changing employees direct deposit information. We have many different safe guards in place to verify that the changes should be occurring. We may be reaching out to you and/or your employees more often to confirm that changes should be taking place.

Some additional examples of recent phishing attempts include:

- Phony alerts from the CDC or other health organizations claiming to link to local coronavirus cases and other information updates.
- Fake messages from WHO offering prevention advice in attachments and embedded links or appealing for donations to a disaster-response fund.
- Communications appearing to come from internal sources announcing workplace policies to download, fake forms to complete with personal information or malicious links to click.

Here are some tried-and-true cybersecurity tips:

- Scrutinize the e-mail sender. Some phishing e-mail has come from "cdc-gov.org," rather than "cdc.gov." Likewise, all legitimate e-mail from WHO will come from addresses with the domain name "who.int." You can also hover your mouse over links to see where they lead, even if the e mail appears to be from the right address. Remember that even legitimate e-mail can be compromised.
- Don't click links. Instead, try retyping the address in a browser window.
- Be careful with attachments, especially if you don't recognize the sender or the e-mail appears suspicious.
- Don't open unsolicited e-mail from people you don't know.
- Be aware that spelling and grammatical mistakes can be red flags.
- Be wary of generic greetings, such as "Dear Sir."
- Avoid e-mail that demands immediate action.
- Beware of requests for your personal information, passwords or login credentials.

Sheakley
THE HUMAN RESOURCES PEOPLE

COVID-19 CLIENT UPDATE

May 13, 2020

State-by-State Business Reopening Guidance

The U.S. Chamber of Commerce has developed an interactive map with the latest guidelines, timeframes and other critical information about opening up the economy. This map can be viewed by visiting: https://www.uschamber.com/article/state-by-state-business-reopening-guidance.

SBA Paycheck Protection Program

As more employers receive their PPP funds, we are receiving questions about how the funds should be used. While your CPA would be the best resource for your questions on how to use and/or track the funds, NAPEO has released the attached Fact Sheet that you may find helpful.

Sheakley HR COVID-19 Resource Page:

In addition to our daily email updates, we are also working diligently to keep our Sheakley HR COVID-19 Resource Page up-to-date. You can visit this page at https://ww2.sheakley.com/coronavirus-update/.