LABORNET

IT Security at DOL

Be Mindful of Ransomware Attacks

DOL Colleagues,

As you may have seen in news reports, the recent cyber-attack suffered by Colonial Pipeline is a stark reminder of the significant dangers and impacts a successful ransomware attack can have on an organization, and those who depend upon it.

I shared some tips on protecting yourself and DOL from ransomware attacks a few months back and wanted to bring those to the top of your inbox at this time. Pleas review the message below. Thank you.

As the Department of Labor (DOL) remains in a maximum telework posture, it is crucial that we continue to be vigilant against the growing threat of cyberattacks. Ransomware, a type of attack that denies access to a computer system or data until a ransom is paid, is one of the fastest growing malware threats worldwide. Ransomware targets users of all types and can lead to disruption of business operations, financial losses, and temporary or permanent unavailability of sensitive or proprietary information. In other words, ransomware incidents can severely impact business processes and leave organizations without the data they need to operate and deliver products and services.

Ransomware typically spreads through phishing emails or by a victim unknowingly visiting an infected site. Be mindful of these tips you can use to protect yourself and the Department against ransomware attacks:

- Be aware of phishing emails and report all suspicious emails to [redacted] (Do not click on any links within the suspicious email. Simply copy the suspicious email, paste it as an attachment in a new email to [redacted] send it, and then delete the original email.)
- Be wary of emails pretending to be from management asking you to do something outside of normal protocol or procedures
- Do not click on unsolicited links or open unsolicited attachments in emails
- Limit browsing on DOL-issued devices to websites related to your mission and job responsibilities
- Take advantage of multi-factor authentication
- Use complex passphrases that include uppercase and lower case letters, special characters, and numbers
- Ensure your devices are connected to the VPN whenever possible
- Take action on all available software updates and patches in a timely fashion
- If you suspect that your device has been infected, immediately report the incident to the Enterprise Service Desk (ESD) and inform your supervisor
- DO NOT pay a ransom – paying a ransom to malicious parties does not guarantee that you will regain access to your data
- Keep your data on approved cloud solutions such as OneDrive so that it can be retrieved if your device is no longer functioning due to ransomware

These tips will help you take the necessary measures to avoid falling victim to a ransomware attack. For more information about ransomware, visit the Cybersecurity & Infrastructure Security Agency (CISA) website. Thank you for doing your part to protect the Department and its data. If you have any questions, please contact [redacted]

You can contact the OCIO – Cybersecurity Directorate at [redacted]

For technical support please contact the Enterprise Service Desk (ESD) at [redacted]

Last updated: May 10, 2021