Five CyberSafe at USPS® tips to help remote workforce members stay secure

The coronavirus caused many businesses to adapt to a partial or full teleworking environment. While necessary, the remote work reality opened a new area of security vulnerability for enterprises across the country, revealing the importance of individual teleworkers' home IT habits.

To help protect the Postal Service, the USPS Corporate Information Security Office (CISO) responded to the COVID-19 crisis by putting together a series of CyberSafe at USPS teleworking tips to help protect remote workforce members as well as the agency's IT network infrastructure. Educating the workforce is a critical component of the USPS® cybersecurity program. An educated workforce member is less likely to fall for a compromising trap.

These five tips represent some of our favorite CyberSafe at USPS tips and can be applied to almost any remote worker in the coronavirus era. They are suggestive only, and do not represent formal guidance from the United States Postal Service. We hope you find them useful for your own enterprise's cybersecurity efforts.

- Tip #5 Watch out for COVID-19 branded phishing attacks
- Tip #14 Secure your meeting
- Tip #16 Home security (routers)
- Tip #22 Webcam spy (Protect your laptop and home)
- Tip #30 Cabin Fever? (Beware of unknown wifi)

***