Talking UP
Economic Development UPdates

University Place
WASHINGTON

May 2020

Tips for Making Work-from-Home Work for Your Business

The COVID-19 pandemic has forced businesses to change the way they operate, especially with regard to remote work. For those who are new to working from home, this has presented a number of challenges, especially with regard to internet security, virtual meetings and document access.

 Wade Stewart, owner of Tech Masters Computer Services, provides on-site and remote IT support and consulting to South Sound businesses, including many home-based businesses. Having worked from home for more than a year before he moved to his office space at 2601 70th Ave. W., he has some advice for those who are new to the experience:

- **Enable Remote Work:** Stewart says there are online services that create a secure connection between a home computer and a work computer so that the user can remotely operate the work computer as if they were in the office. Since the Governor's Stay Home, Stay Healthy order, he estimates that his firm has nearly tripled the number of computers it manages that are deployed with remote access capability.

- **Credentials:** Be sure that your business usernames and passwords for bank accounts, website management, social media, advertising, etc., are saved in a secure and shareable tool like Lastpass or 1Password so that they can be accessed remotely by authorized users.

- **Beware of Bandwidth Limitations:** High-definition video, such as that used in remote meeting tools like Zoom or Teams, requires a lot of bandwidth. Most home internet

systems are unable to handle multiple people using the network for video, file sharing, etc., at the same time.

- **Power Limitations: Employees working remotely may discover that their home computers lack the storage space and internal processors that make it possible to use cloud storage tools such as Dropbox or OneDrive.**

- **Security: Stewart says many home networks may not be properly firewalled and home computers might lack protection against hacking. This makes them susceptible to ransomware, wire transfer theft, or worse. "Many businesses are not using good security processes and there is worry that come this fall, there will be a big spike in cybercrime that will hit small businesses," Stewart says.**

Stewart has written several blogs about these timely topics. Read more of his insights [here](.).

Protect Your Employees During an Emergency

As the COVID-19 pandemic has shown us, emergencies can take all shapes and sizes: natural, man-made, viral, etc. Now more than ever, it is a good time to review your preparations for keeping your employees safe during any kind of emergency.

The Federal Emergency Management Agency (FEMA) recommends you take these steps:

- **Communicate: Review how you will connect with employees in emergency situations -- before, during and after a disaster. Whether via email, phone trees or a password-protected portal on your company website, make sure employees understand where they can get information -- and where they can share information, including ways to communicate to you that they are safe. These plans should also include accommodations for employees with disabilities. Make sure you ask in advance the best way to communicate with them in an emergency. For on-site emergencies, have plans in place to assist employees with mobility, vision or hearing limitations.**

- **Stock Up: Have a ready supply of fresh water and non-perishable food on hand should you need to shelter-in-**

place. Make sure your office has a battery-powered commercial radio and a NOAA weather radio with an alert function and extra batteries. In addition to flashlights and a first aid kit, make sure you have dust or filter masks, plastic sheeting and duct tape on hand to "seal the room" should it become necessary.

- **Store It:** Keep copies of important records including insurance policies, employee contact and identification information, bank account records, supplier and shipping contact lists, computer backups, and other priority documents in a waterproof, fireproof portable container.

- **Have-and Practice-Your Evacuation Plan:** If you need to vacate your space quickly, make sure you have a plan to evacuate workers, customers and visitors safely and quickly. Plan two exit paths and post maps that show how to reach those exits from every space within your office. Designate an assembly site near your facility and another in the general area in case you have to move farther away. Practice the evacuation plan regularly and designate an employee(s) who is responsible for accounting for all workers, visitors and customers.

- **Coordinate with Neighbors:** Speak to other businesses in your building or industrial complex and conduct evacuation drills and other emergency exercises together. This will help eliminate confusion and assist first responders when they arrive on site.

You can view FEMA's "Every Business Should Have a Plan" booklet [here](). Local businesses should also consider enrolling in the U.P. Police Department's free Public Safety Classes, which include a session called "Three Days and Beyond." This class provides practical, valuable and life-saving tips on how to be prepared for a lengthy public emergency. Watch the City's [website]() for updates on when Public Safety Classes will resume.

Visit the City's COVID-19 Business Support Page

The U.P. Economic Development Department gets regular updates on new sources of funding, training and support available to businesses during the COVID-19 outbreak and recovery period. The [Business Support page]() on the City's website is a repository of this critical information. It provides links to resources available to businesses as they try to navigate the maze of survival and recovery in these unprecedented times.

Much of this information is time-sensitive, so be sure to check the page often throughout the week.