

# Online Security for a Remote Workforce

Michele Vayle | RENOVODATA



**AS THE WORLD** reels from the impact of COVID-19, the services of 3PL and trucking companies are more essential than ever. Your customers, and your employees, are counting on you to keep going.

While planning for pandemics was not generally thought necessary in the past, we must do what we can, as fast as we can, to get on top of the obstacles in front of us, ameliorate the damage, and, where possible, forge ahead.

This crisis has created countless new challenges in both our personal

and professional lives, and the fact that team members are being forced to work remotely is one of the most difficult. Since we don't know how long the pandemic will last, we should not think of employees' working in isolation as a momentary stopgap measure.

## Management Perspective

Businesses need continuity policies now more than ever. With the realities of the pandemic fully entrenched, it's clear the idea that "we have always done things that way" no longer applies.

As early as possible, document the processes and procedures necessary for

the company to keep functioning productively, and identify the needed resources. All levels and categories of employees should be involved in this documentation process.

New procedures will have to be developed but necessary changes may be hard to anticipate. These include:

- Alterations of long-established activities;
- Realignments of duties;
- Revised training methods;
- New ways to hold meetings;
- Elimination or lessening of certain functions;
- Modification of communications at every level, involving management and staff, customers, vendors and partners.

### Heightened Security Dangers

Cyberthreats are on the rise and the fact that so much is changing distracts our attention from normal safety concerns. Malware developers can step-up their assaults because the pandemic has weakened organizations' normal protections. New varieties of fraudulent clickbait appear in the form of fictitious cures and bogus services.

Because their operations are so fast-moving, 3PL and trucking companies are among the most vulnerable targets. Malware attacks can infiltrate networks via even the smallest unguarded gap in your defenses, and current circumstances can allow new security weaknesses to appear.

### Remote Workplace Essentials

Whenever possible, remote employees should utilize organization-supplied equipment, or take home the devices they use in their offices. These machines are already set up with requisite functions and protections, from firewalls to corporate policy features and malware defenses.

- If employees must use their own equipment, it is imperative that personal devices be equipped with the same types of protection utilized in the office; chief among these is the need for strong and up-to-date firewalls.


## MALWARE ATTACKS CAN INFILTRATE NETWORKS VIA EVEN THE SMALLEST UNGUARDED GAP IN YOUR DEFENSES, AND CURRENT CIRCUMSTANCES CAN ALLOW NEW SECURITY WEAKNESSES TO APPEAR.

- Employees working with their own devices should make sure that their network connections are secure; a VPN adds an extra layer of safety by protecting passwords and other personal information.
- All updates and patches should be installed to ensure that personal devices can deliver optimum performance.
- No personal device should go into service without robust antivirus and anti-malware protection.
- Employees should be kept aware of the latest cyber threats.
- Because cybercriminals are now working overtime, employees should be especially vigilant regarding iffy links and unrecognized emails; personal details should never be shared.
- Remote employees should keep an eye on network traffic and be wary of presences that appear suspicious; a widely dispersed workforce can make it easier for bad actors to invade networks.
- The safety of all endpoint devices should be verified because they are among the most inviting targets for cyberattacks. These include computers, smartphones, tablets, USB drives, and any other items attached to the system.

- All data must be frequently backed-up and safely stored. This is especially important in remote environments where interruptions, spilled beverages, rambunctious kids, and equipment failures can cause damaging data losses.
- Security-assured solutions should be used when sharing files. Negligent file-sharing can be as damaging as outright file theft.
- A thorough backup is needed for rolling back to a previous version or time.
- When device video cameras are not in use, they should be blacked out to prevent hackers from spying.
- Employees must be sure that no one else uses computers that have been pressed into service. Games, private emails, remote schoolwork, and other online content can pose severe dangers.

This is a lot to take in and conducting business when your workforce is remote can be a tremendous undertaking. Any number of additional impediments will have to be overcome and each 3PL and trucking company will encounter its own particular problems.

But you don't have to face these challenges and quandaries alone. Reliable, experienced vendors are available to provide products and solutions that deliver key functions such as file sharing and synchronization, firewall implementation, data backup, endpoint coverage, and anti-malware with many more security features. These can be adapted to support remote users.

With strong corporate commitment and expert technical guidance, 3PL and trucking companies can prosper in an age of pandemic, even with a dispersed workforce. We are ready to lend our knowledge and experience to your data protection and planning initiative. 

*For more information call toll-free at 877-834-3684, reference our website at [www.renovodata.com](http://www.renovodata.com), or email us at [info@renovodata.com](mailto:info@renovodata.com). RenovoData is a leading, remote cloud backup and disaster recovery service provider helping companies protect critical data worldwide.*