Problem
Technology has become extremely powerful allowing you to connect to the Internet and communicate anytime you want, anywhere you want. From tablets and smartphones to lightweight laptops you can potentially work anywhere in the world. However, when working away from the office there are several risks you need to be aware of.

In this newsletter we will explain how you can securely work while away from the office. Remember that to work from home you must first have permission from your supervisor. In addition, depending on the type of information you are working on you may also need permission to work while traveling, such as if you are attending a conference or visiting another office. If you have any questions about when you can work remotely, and what information you can work on, be sure to ask your supervisor first.

Solutions
1. Working At Home
If you have been authorized to work from home, remember your home network and Internet connection is not as secure as our organization’s network. As a result, there are several extra measures you should take to protect yourself and our organization.

While working from home make sure you only use devices authorized for work. You may not use personal devices such as personal computers unless you have prior management approval. If you have been approved to use personal systems, you may be required to install additional security software. Please check with your help desk or security team for more information.

Also, ensure only authorized people have access to any system used for work. Children, guests or other household members should not have access to your work computer. Unauthorized users can accidently infect your computer downloading infected videos or children’s games.
2. Protecting against Theft
One major risk while traveling is physical theft of your laptop or smartphone. While traveling you should make sure these devices are with you at all times. If you must leave a device behind, be sure it is in a secure location. For example, if you must leave your laptop in your car, securely lock it in your trunk.

3. Connecting into work
While working remotely you will often need to connect to the Internet, perhaps to send an email or read documents. In some cases you may need to remotely connect to our internal networks. Please remember when you do so your activities and information can be monitored by others. When you connect from a café, airport terminal or hotel lobby, these public networks can be accessed by anyone and should not be trusted.

Any remote connection that will have confidential work information should be encrypted. For example, you may be required to use VPN (Virtual Private Network) software whenever connecting to internal networks or conducting work related activity. If you are not sure about encryption requirements, please contact the help desk or your security team.

4. Securing your laptop
While traveling you will be connecting your computer to untrusted public networks. You need to ensure your laptop has been properly secured. Please be sure the following critical protections have been enabled on your computer.

- Ensure your computer has automatic updating enabled, the latest patches and a current operating system.
- Ensure you have anti-virus installed and automatic updates enabled.
- Ensure your firewall is on, this ensures other computers cannot connect to yours.

5. Using other computers
Be sure when traveling you only use your authorized computers for accessing work related information. Never use publicly available computers such as those in a hotel lobby, airports, or even a friend’s computer. There is a good chance these computers are already infected. Utilizing them could potentially compromise your login and password.

6. Password screen lock
If you leave your computer on and walk away make sure you password lock the screen to eliminate users from accessing your information.

There are many threats you have to consider when working remotely. You need to be concerned with cyber criminals who may try to hack into your computer as well as criminals who want to physically steal your laptop.

There is another threat you have to consider, yourself. Lost laptops and smartphones are a very common way confidential data is compromised. The challenge while traveling is the constantly changing environment, such as when traveling through an airport. It is very simple to misplace or forget your smartphone or laptop. Here are some tips to remember when traveling.

- Always store your laptop and smartphone in the same bag or location, this way it is easy to spot if missing.
- Make a habit of checking critical items whenever you have passed security checkpoints, left an office or exited an airplane.

If you have lost a work related item, be sure to report it immediately.