# CYBER SECURITY newsletter

## TELECOMMUTING SECURELY

### Problem

Technology has become extremely powerful, it allows you to connect to the Internet and communicate anytime you want, anywhere you want. From tablets and smartphones to light weight laptops you can potentially work from 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 to you these issues and how you can securely work while telecommuting. Please remember to work from home you must first have permission from your management. In addition, depending on the type of information you are working on you may need permission to work when traveling or when away from the office. If you are not sure then please check with your supervisor first.

### Solutions

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

First, while working from home make sure you use only 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 IT help desk or security team for more information.

Also, ensure that only authorized people have access to any system used for work. For example children, guests or other household members should not have access to your work computer. Unauthorized users can accidently infect your computer, such as by downloading infected videos or children's games.

***Working Away From The Office***

*Technology is enabling more and more of us to work away from the office, either from home or while on the road. This gives you tremendous flexibility, but also has certain risks.*

University of Colorado
Boulder | Colorado Springs | Denver | Anschutz Medical Campus

This newsletter is published by the University of Colorado Office of Information Security. For more information please send email to security@cu.edu or visit https://www.cu.edu/information-privacy-and-security

# Losing Your Laptop

*There are many threats you have to consider when working away from the office. Not only do you have to be concerned about cyber criminals who may try to hack into your computer, but you have criminals who may try to physically steal your laptop.*

*However there is another threat that you have to consider, yourself. Believe it or not lost laptops and smartphones are a very common way confidential data is compromised. The challenge with traveling is you are in a 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 tricks 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, leaving an office, or exiting an airplane.*

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

**2. Protecting Against Theft.** A major risk while traveling is physical theft, someone stealing your laptop or smartphone. While traveling 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, be sure to lock it in your trunk first.

**3. Connecting Into Work:** When you are working away from the office you will often need to connect to the Internet, perhaps to send an email or read a document. In some cases you may even need to remotely connect to our internal networks. Please remember that when you do so, your activities and information can be monitored by others. For example, when you connect from a café, airport terminal or hotel lobby, these are on public networks that anyone can access, as such you should not trust them.

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 IT 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 three services have been enabled on your computer, these are critical to protecting your system.

- Ensure your computer has automatic updating enabled, this ensure it always has the latest patches and 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 you.

**5. Using Other Computers.** Be sure when traveling that you use only your own, authorized computers for accessing work related information. Never use publicly available computers, such as those in a hotel lobby, nor even a friend's computer. There is a good chance these computers are already infected. If you were to use them, potentially your login and password could be compromised, or even work related information stolen by others.

**6. Password Screen Lock.** If you leave your computer on and walk away from it, make sure you password lock the screen. This means that if anyone walks up to your computer, they cannot access your information.