hotel, library, etc., anything that you enter into the workstation, including IDs, passwords, and data, may be captured by an attacker.

If you think your UMNetID and password, information or electronic device has been compromised, contact the IST Service Desk as soon as possible at (204) 474-8600.

STEP 3 - WHEN YOU RETURN

Change your passwords!

When you return from your trip, change any passwords that you may have used during your travels.

Have your devices inspected, cleaned and restore trusted versions of software

If you connected your device to an unknown or public network while travelling, there is the chance that an attacker installed malicious software on your device and is patiently waiting for you to connect it to the University or your personal network. Upon your return, before reconnecting to your University or personal networks, best practice is to wipe the device clean and reimage it with trusted software versions.

Contact the IST Service Desk at (204) 474-8600 for assistance.

Information Security Starts with You!

Additional resources

Canadian Government Cyber Safe Travel Recommendations
https://travel.gc.ca/travelling/health-safety/cyber-safe/recommendations

United States Government Travel Alerts and Warnings
https://travel.state.gov/content/passports/en/alertswarnings.html/

US Department of Justice Travel Tips Brochure

Higher Education Information Security Council – Collection of Security Tips for Travelling
https://spaces.internet2.edu/display/2014infosecurityguide/Security+Tips+for+Traveling+Abroad

PROTECTING YOUR INFORMATION WHILE TRAVELLING

DID YOU KNOW THAT THE INFORMATION STORED ON YOUR ELECTRONIC DEVICE, INCLUDING LAPTOP, TABLET AND SMARTPHONE IS MORE VULNERABLE TO ATTACKERS WHEN YOU ARE TRAVELLING?
PROTECTING YOUR INFORMATION WHILE TRAVELLING

Did you know that the information stored on your electronic device, including laptop, tablet and smartphone is more vulnerable to attackers when you are travelling? For example, if you connect your device to a public wifi network in an airport, an attacker can more easily infect your smartphone with a virus, wiping all your data and contacts from the device. If you get distracted for a minute, this is enough time for an attacker to walk away with your device and all the information stored on it. Not only could this have implications for your personal information, but it could also have serious consequences for University systems and information, research data, student information, etc.

Travelling introduces significant risks to the information you have stored on the electronic devices that you take with you. Protect your personal and University-related information by taking simple, but necessary, precautions.

STEP 1 - PREPARING FOR YOUR TRIP

Be as informed a possible about your destination. Information about your destination can be found on the Canadian government’s travel advice and advisories page.

Be aware of the information stored on your electronic devices.

If you are taking an electronic device, such as your laptop, review the information that is currently stored on it and remove any sensitive information.

For more information on what types of information are classified as sensitive and restricted, see the University of Manitoba’s data security classification document.

Backup your device and patch your device.

Imagine losing years of research data because of device theft! Create a backup of the information stored on your electronic device. In the event that your device is compromised and you lose all the information contained on it, you can restore it when you return from your travels. Also ensure operating system and applications have the latest security updates.

Did you know that it takes up to 10 days to get fully operational after a laptop loss?

Better yet, take a loaner device!

Consider taking a loaner device instead. Loaner devices prepared by the University contain minimal information and applications. They contain just the basics required for travel.

Contact the IST Service Desk at (204)-474-8600 to request a loaner device.

STEP 2 - WHILE YOU’RE TRAVELLING

Avoid logging into the University network with your UMNetID and password

If possible avoid logging into the University network with your UMNetID and password. An attacker may be trying to capture your credentials. If an attacker is successful, they would have access to your information as well as the University’s information and systems. If you must access email or other systems, ensure that you are using the UofM VPN service which will create an encrypted secure connection.

Did you know that it takes up to 10 days to get fully operational after a laptop loss?

Be aware of your surroundings when logging in or entering data into your devices

Keep a watchful eye when you are entering your UMNetID and password. It’s not uncommon for an attacker to simply watch from a close distance, or “shoulder surf”, as you type in your credentials.

Avoid using public workstations

Public workstations should not be considered secure. When you use a public workstation in a café,