From the Desk of Ron Jimerson, Chief Information Security Officer

Summer is finally here and for many of us that means it’s time to get away! It’s not surprising that many cyber criminals target travelers. Luckily, with a little care it’s possible to protect yourself and avoid potential problems.

**Sharing isn’t always caring**

- Avoid publicly posting details of where and when you’ll be traveling. When you reveal these specifics, you are providing information that could be used by criminals to target your home or your family while you’re gone.

  Sending private posts and photos during your vacation to family and friends is ok, but if you post them publicly, you increase the risk of someone using that information for malicious activities.

  Just as important as using discretion when posting, is making sure your children and friends understand the risks associated with posting your vacation plans.

- Do not use public computers and open wireless networks for sensitive online transactions. Wi-Fi spots in airports, hotels, coffee shops, and other public places can be convenient but they’re often not secure and can leave you at risk. If you’re accessing the Internet through an unsecured network, you should be aware that malicious individuals might be able to eavesdrop on your connection. This could allow them to steal your login credentials, financial information, or other sensitive information. Any public Wi-Fi should be considered “unsecure.”

  Consider turning off features on your computer or mobile devices that allow you to automatically connect to Wi-Fi and other services such as social media websites. Also consider...
using a cellular 3G/4G connection as a hotspot, which is generally safer than an open Wi-Fi
connection. If you do connect through your hotel’s Wi-Fi, verify the name of the Wi-Fi hotspot
with hotel staff.

**Recommendations**

- Use discretion when posting information online. Consider keeping your social media pages
  private, so only authorized individuals can visit.
- Password protect your devices so if they are lost or stolen the information is protected; and
  enable device tracking.
- Make sure your laptop and other mobile devices have the latest patches installed. Your
  software vendor should notify you whenever an update is available. Set your device to auto
  update.
- Use of security software is a must. Some programs can also locate a missing or stolen phone,
  tablet or other similar device, while others will back up your data and can even remotely wipe
  all data from the phone if it is reported stolen. Definitely make sure you have anti-virus
  software installed, updated and running.
- Do not access sensitive accounts (e.g. banks, credit cards, etc.) or conduct sensitive
  transactions over public networks, including hotel and airport Wi-Fi and business centers, or
  Internet cafes. Use wired connections instead of Bluetooth or Wi-Fi connections, whenever
  possible.
- Do not plug USB cables into public charging stations; only connect USB powered devices using
  the intended AC power adapter as USB cables can be used to

**Further Information**

More information is available in the User Recommendations section of the CIS Primer on Overseas

For more information about how to stay safe in cyberspace, visit the Center for Internet Security
at [www.cisecurity.org](http://www.cisecurity.org)

*Provided By: Multi-State Information Sharing & Analysis Center™*