



Don't Let Identity Theft Be One of Your Spring Break Memories

Release Date: March 14, 2019

**Contact: Jerad Albracht, Communication Specialist
(608) 224-5007, jerad.albracht@wisconsin.gov**

MADISON – The steps you take to protect your personal information before you start your vacation are the key to mitigating potential identity theft if your devices or documents are stolen or misplaced during your trip. The Wisconsin Department of Agriculture, Trade and Consumer Protection (DATCP) offers some simple pre-, during, and post-trip tips to help travelers limit the threat of identity theft.

“When you are on the go and making memories, you don't want to constantly worry about whether someone is snooping through your online accounts or making new credit accounts with your identity,” said Lara Sutherlin, Administrator for the Division of Trade and Consumer Protection. “Some small preventative measures like updating the operating system and antivirus software on your mobile devices can go a long way toward fending off identity thieves.”

Devote a couple of pre-trip minutes to shoring up your online accounts, strengthening the protection around your mobile devices, and limiting your risk of information exposure. While traveling, avoid sharing sensitive information over public WiFi networks and keep the trip details you share on social media accounts to a minimum. When you return home, run an antivirus scan on your devices and update passwords for your social media, email, and financial accounts.

Here are additional pre-, during, and post-trip tips:

Before you start your trip:

- Make sure that your mobile devices are password protected and update the operating systems and antivirus packages.
- Alert your financial institutions about your travel plans and ensure that fraud alerts are in place on your accounts – this will allow you to be immediately notified of suspicious activity while you are traveling. Use the number on the back of your credit and debit cards to contact the banks.
- Put your mail on hold. Identity thieves could steal mail from unattended mailboxes, giving them the information they need to misuse your identity and open credit lines in your name. The post office can hold your letters and packages until you return.
- Limit what is in your wallet. Keep your bank cards to a minimum and do NOT pack your Social Security card or carry it in your wallet or purse if it is not necessary.
- Photocopy your documents and cards. Leave the relevant information from the front and back of your passport, driver's license, credit cards, tickets, and hotel reservation confirmations with a friend or family member at home in case your original documents are lost or stolen during your trip.
- Share your plans with friends and family to avoid "grandparent scams."
- Turn off auto-connect to WiFi and Bluetooth connections.

(MORE)

- Tighten the security around your social media accounts. Your public posts could give a thief the tools to steal your identity or rob your home while you travel. Adjust the security settings on your accounts to only allow friends and family to view your posts, and consider turning off the location services on your phone so the photos you post online are not tagged with GPS data.

While on vacation:

- Use caution with public WiFi. Avoid banking or sharing sensitive data over public WiFi networks. Only send sensitive information over password-protected networks and in secure websites (those that start with "https" – the information is encrypted).
- Use caution with public computers – even those in your hotel.
- Keep personal documents close. Make use of a room safe when available for mobile devices, valuables, and sensitive documents like passports, ID cards, credit cards, and airline tickets.
- Always keep your mobile devices in a secure location. Your smartphone, tablet, and laptop contain a wealth of personal information. Know where these devices are at all times and keep them secure in public. Log out of all websites so your accounts are not accessed if your device is lost or stolen.

When you get home:

- Change passwords. Any website you accessed on your trip was fair game for scammers, so change all of your passwords – especially for your email account.
- Check accounts. Take a look through your bank and credit card accounts and identify any irregularities. Bring them to the immediate attention of your financial institution.
- Check credit reports. Review your credit reports to ensure that no unexpected accounts have been created in your name.

For additional information, visit the Bureau of Consumer Protection at <http://datcp.wi.gov>, send an e-mail to datcp@wi.gov or call the Consumer Protection Hotline toll-free at 1-800-422-7128.

Connect with us on Facebook at www.facebook.com/wiconsumer or on Twitter: @wiconsumer.

###

Find more DATCP news in our [newsroom](#), and on [Facebook](#) and [Twitter](#).