Travel Tips to Stay Safe this Holiday Season as Cybercrime Increases

TransUnion cited a 12% suspected increase over last year in digital fraud from Nov. 23-27, 2023. Proactive steps can reduce risk, especially when traveling.[1]

SPOKANE, WA, UNITED STATES, December 13, 2023 / EINPresswire.com/ -- 115 Million Americans to travel over the holidays in 2023, says AAA.[2] Travelers can avoid being a statistic of cybercrime, by being prepared.

“Awareness is key to address any challenge. These few travel tips for cybersecurity can enhance one's peace of mind and successful travel,” stated Heather Stratford, Founder/CEO of Drip7.

> Awareness is key to address any challenge. These few travel tips for cybersecurity can enhance your peace of mind and successful travel,”
>
> *Heather Stratford, Drip7*
> *Founder and CEO*

Nothing will ruin a holiday trip more than learning of identity theft or accounts have been compromised, money stolen or credit cards frozen. Preparation before holiday travel can make the difference between holiday cheer or despair. Here are tips to stay cyber safe.

Training - Leverage any employer cybersecurity training, to learn more about cybersecurity. Employers who want to learn tips to prepare for the holidays can go to a Drip7 holiday post.

Updates or Patching - Be sure all electronic devices are updated - including hardware, phones, and computers plus the applications used - Microsoft, Google, Wordle, Facebook, Instagram, SnapChat, Abobe. Do not install patches while traveling.

Passwords - Passwords are more vulnerable when traveling. Long and complex passwords are safer than short simple passwords. Do not change passwords while on the road unless

something has been compromised. 38% of Americans report having at least one of their passwords cracked or guessed. In 2022, over 24 billion passwords were exposed by hackers.[3]

Mobile apps - Most people use their phone more when traveling. A large percentage of online fraud (70%) is now accomplished through mobile applications.[4]

Juice Jacking - Juice jacking is more common than one would think. It can be found in malls, airports, and public places with free charging stations. Bad actors can tamper with charging stations loading a virus onto the device being charged.[5] Use one's own cord and charging device.

Wi-Fi - Wi-Fi networks found in public places from airports to coffee shops, not to mention the homes of relatives, are often unprotected, therefore targets for hackers. This is a primary cybersecurity risk when traveling. A VPN, virtual private network, is the easiest way to keep safe. If one doesn't have a VPN, then limit the kinds of data and information being transferring over an unknown Wi-Fi network, don’t log into a bank, transfer money, or send critical data.

Phishing - Phishing is increasing. Be wary of messages that are urgent, asking for personal information and are from unknown sources. Carefully, review the full email address as it may be similar to known contacts but not an exact match. Verify the authenticity of emails requesting information before sending a response.

Social Media - While traveling, increased use of social media can raise potential risks. These risks might include: ads with links to websites with malware, questionnaires asking for personal information that could be used to access passwords and accounts, impersonation of contacts, ads that replicate real businesses to lure the unsuspecting. It is best to initiate going to a desired website and not clicking on ads.

Social Engineering - An example is shoulder surfing, when someone is looking over a shoulder to access information entered, such as when using a credit card and entering a pin. Bad actors love to steal credentials. Losses from identity theft cost Americans $5.8 billion.[6] From 2001-2021, the reported frauds, identity thefts, and similar crimes went from 325,519 to nearly 6 million annually.[7]

Loved Ones - When talking to loved ones who may be using devices, be sure they know how to stay safe. Older adults can often feel intimidated when it comes to technology. Be a part of the security team and help them use better passwords, secure devices and set up multi-factor authentication. Younger people also need to know the basics of cybersecurity.

Posting Locations - Don’t advertise being away from home. Wait to post those travel photos until safely home. When criminals know folks are traveling, they can more easily enter a physical home and attack social profiles to gain access.

Backups - Backing up devices can be done with an external drive, in the cloud, or both.

Charitable Donations - Fake charity campaigns abound during the holiday season. Giving is good, but knowing donations are going to the correct place is essential. Initiate contributions to known charities on verified websites if donating online. Ideally, wait and donate at home or use a VPN.

IoT - If buying or receiving a gift of a new device that connects to Wi-Fi, think about access. Many IoT devices have a password and should be set up when first received. The Internet of Things, IoT, has exploded and over 10.54 million IoT attacks were reported in December 2022.[8]

Privacy Screen - If conducting confidential work on a flight, consider adding a privacy screen to the laptop screen to prevent visual hacking. Review and update privacy settings on social media platforms to control what is public.

Physical Safety - Be aware of one's surroundings and belongings. Make smart choices on where and how traveling. Be vigilant in crowds. Personal safety is paramount but also protection from theft of property and devices. Most cybersecurity experts agree that about 20 percent of travelers are subject to cybercrime when abroad.[9]

In 2023 alone, over 5 billion records have been compromised, and the risk escalates during holidays.[10]

“In a world where we are constantly connected, cybersecurity cannot be limited to the home or office. When traveling, whether domestic or international, it is always important to practice safe online behavior and take proactive steps to secure Internet-enabled devices. The more we travel, the more we are at risk for cyberattacks,” CISA warns in a travel alert.[11]

With consideration of these simple steps, the holiday season can remain safe and joyous. Ben Franklin stated, “an ounce of prevention is worth a pound of cure,” in warning of the dangers of fire. Today, cyberthreats are the “fire” we need to prevent.

[1] https://newsroom.transunion.com/digital-holiday-fraud-in-2023/
[2] https://www.forbes.com/sites/suzannerowankelleher/2023/12/11/115-million-americans-travel-holidays-in-2023-aaa/?sh=322faa8a1e93
[3] https://us.norton.com/blog/privacy/password-statistics
[4] https://www.getastra.com/blog/security-audit/phishing-attack-statistics/#:~:text=Phishing%20email%20statistics%20suggest%20that,attack%20occurring%20every%2011%20seconds.
[5] https://www.globaldatavault.com/blog/protecting-your-network-during-the-holidays-reminders-to-stay-vigilant/
[6] https://www.cyberdefensemagazine.com/halting-hackers-on-the-holidays-2023/
[7] https://www.daytondailynews.com/local/rise-in-cyber-crimes-during-holiday-shopping-season-a-concern-for-december/REDPU5ZG7REAPHSJTSUKN2E4PU/

[8] https://www.statista.com/statistics/1322216/worldwide-internet-of-things-attacks/
[9] https://www.fcmtravel.com/en-us/resources/insights/why-cyber-security-fastest-growing-source-travel-risk#:~:text=Most%20cybersecurity%20experts%20agree%20that,at%20additional%20information%20security%20risk.
[10] https://fintech.global/2023/12/11/unwrapping-cyber-risks-how-to-protect-your-investments-during-the-holiday-se
ason/#:~:text=In%202023%20alone%2C%20over%205,companies%20operate%20at%20reduced%20capacity.
[11] https://www.cisa.gov/sites/default/files/publications/Cybersecurity%2520Awareness%2520Month%25202021%2520-%2520Travel%2520Tip%2520Sheet.pdf

Deb McFadden
Drip7
+1 509-703-5400
PR@drip7.com
Visit us on social media:
Facebook
Twitter
LinkedIn
Instagram
