RCM&D

Assurex GLOBAL | Private Client Practice Group

Cybersecurity While Traveling:

Important tips and considerations while on the go

HOW OFTEN DO YOU TRAVEL FOR WORK OR PLEASURE? The majority of us do so quite frequently, and yet we give little thought to how we keep our identity and data safe while doing so. To keep us informed and vigilant during our travels, Assurex Global asked its "go to" resource for digital forensics and cybersecurity, LIFARS, to answer some questions all of us should be asking—but often don't think to consider—regarding our digital security while on the road.

Social Media

I want to share photos of my trip with family and friends. Am I risking the security of myself or my possessions? Unfortunately, yes. While sharing updates of your travels is a great way to keep in touch with family and friends, checking in to places that you are visiting, posting updates mentioning your location, or posting photos from your journey are all voluntary compromises of privacy. Although this may not be an issue 99 percent of time, there is a risk that your social media updates will end up in the wrong hands and abused for criminal purposes, such as burglarizing your vacant house.

Am I safe if I don't post anything about my trips? Only if none of your family or friends are posting, either. It is important to remember that **you** don't have to be the person sharing the information—your spouse, children, or friends who tag or mention you in their own posts are also threats. Because of this, make sure to set high privacy settings and to educate your family and friends about the potential dangers of oversharing.

Public Wi-Fi

Just how safe are hotel networks? The short answer is, they're not. Most hotel networks are relatively easy to breach. This is of particular concern at exclusive hotels, as the high net worth individuals who frequent them represent a larger paycheck for hackers. To ensure that you are not a victim, never use the free Wi-Fi networks offered by most hotels, and avoid the paid connections when possible. Although the paid connections at hotels are typically safer, it is more secure to use an alternate method of connecting to the internet.

SEPTEMBER 30, 2015. ISSUE 1

ASSUREX GLOBAL QUARTERLY SECURITY UPDATE: PROVIDED IN COLLABORATION WITH LIFARS

What should I use instead? It is recommended that you use a Virtual Private Network (VPN). A VPN functions as a secure tunnel that adds an extra layer of security to your connection, making it much harder to successfully gain unauthorized access to your computer. For a list of top VPN providers, take a look at this comparison article published in PC Mag, a reputable computer magazine.

As an alternative to VPN use, most smartphones are able to share their Internet connection with a computer. With the high speed of mobile Internet, your smartphone is an easy and secure way to check emails, log into your online banking, and perform other high-privacy tasks.

Mobile Devices

How do I secure devices from unauthorized access? If you haven't already, set up a lock code or a password on every single one of your devices. Although this is fairly easy for a tech-savvy person to circumvent, it will ensure that people with little tech knowledge will not be able to gain access.

How do I remain secure if somebody circumvents my lock code? To ensure you stay safe even if someone gets through the login screen, do not save passwords in your browser. Most browsers will automatically store passwords used, thus lowering your overall security. Instead, use a password manager such as LastPass or Sticky Password. These will securely store all of your passwords and are compatible with 2-factor authentication to ensure maximum safety. You could also encrypt your devices and the folders on your laptop that contain sensitive data.

General Security

What are other methods for remaining secure while traveling? Security doesn't begin and end with digital. Sometimes, old-fashioned paper can make your travels more secure. For example, it is always a good idea to make copies of all important documents, especially when traveling abroad. Copies can be a lifesaver in case your originals are lost or stolen. This holds true for credit cards as well—having your credit card numbers on hand (even if stolen) makes a huge difference in case an emergency happens.

The number one rule for security while traveling: Stay vigilant and use common sense. Most cybercrime (and crime in general) can be avoided by remaining vigilant, informed, and careful.

2-factor authentication (**2FA**): This security measure adds an extra step to the authentication process by requiring something you know (ex: password) and something you have with you (ex: cell phone). By requiring both entities, 2FA provides an additional layer of security, making your devices less likely to be breached.

LIFARS
your digital world, secured

LIFARS is a digital forensics and cybersecurity intelligence firm based in New York City. Our incident response and penetration testing teams consist of the top experts in the field. As a testament to our excellence, LIFARS was ranked the #2 cybersecurity company in New York Metro area on the Cybersecurity 500 list of the hottest and most innovative cyber security companies.

Assurex GLOBAL | Private Client Practice Group

Founded in 2014, the Private Client Practice Group assists Partner firms to collectively leverage their resources and industry influence to better meet the personal protection needs of high net worth clients. Through this Group, our Partners are able to provide their private clients with access to proprietary insurance solutions, specialty programs, and the collective thought leadership that can only be achieved in a culture of collaboration among best in class personal risk advisors.

SEPTEMBER 30, 2015. ISSUE 1

ASSUREX GLOBAL QUARTERLY SECURITY UPDATE: PROVIDED IN COLLABORATION WITH LIFARS