CYBERCRIME IN CHINA

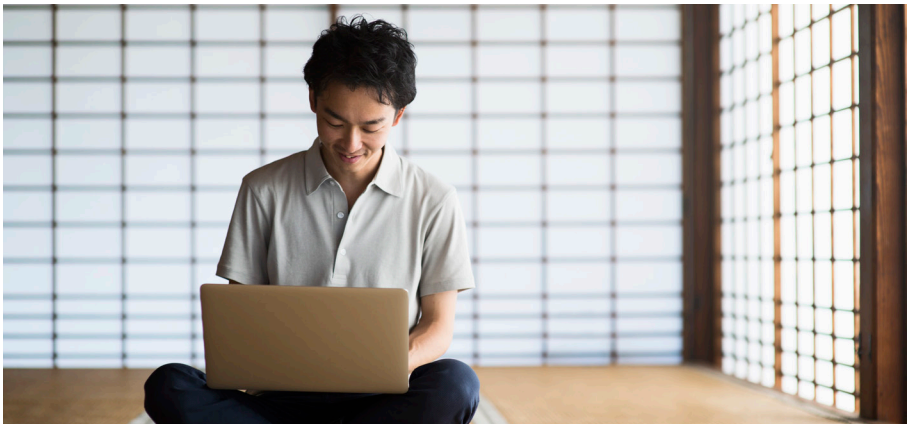
COUNTRY CYBER RISK RATING: **HIGH**

AIG Travel's security team rates China as a **HIGH** cyber risk location. Widespread online censorship and monitoring, as well as the frequent incidence of cybercrime, pose a HIGH risk in the cyber domain. Beyond internet restrictions, government security forces have been known to confiscate electronic devices without prior notice from travelers at both rural and urban airports in order to investigate the electronics systems. High-profile travelers, such as business executives, are at an increased risk of experiencing these confiscations. In an effort to limit the circumvention of controls on internet access, the government has increasingly begun to limit the use of Virtual Private Networks (VPNs), which were the primary means employed by internet users to view restricted sites.

Notable Concerns

China has experienced sharp increases in cybercrime in recent years due to various hacker groups and information thieves becoming active; these groups have been responsible for both domestic and international cybercrimes. In general, individuals and small, loosely affiliated groups are responsible for identity thefts and theft of other internet user information, while larger groups are responsible for money laundering, hacking of financial institutions and theft of corporate information. In some cases, criminal syndicates within the country have established online drug trafficking and sale networks. China and the U.S. have cooperated with one another to combat these groups with limited success. In particular, cooperation has increased since the signing of the U.S.-China Cybersecurity Agreement in 2015, which was designed to deter economically driven cyber espionage.

There is widespread censorship and monitoring of online activity throughout China. The country's police, military as well as government owned Chinese social media corporations all have large monitoring teams tracking internet activities in real time; these groups filter through information related to sensitive political issues and topics deemed potentially harmful for the Communist Party of China's rule. Numerous cases involving police tracking and/or arresting internet users who posted content deemed by the government as "hostile information" online have surfaced in recent years, although what constitutes "hostile information" is not well-defined. In addition to government surveillance, popular social media networks and other sites, including Facebook, YouTube and Twitter, are restricted from the public. Google and Yahoo can also be difficult to access. Internet, phones and other forms of electronic communication at high-end hotels are usually monitored by the government.



Beginning 31 March 2018, the Chinese government (by way of the Cyberspace Administration of China and the Ministry of Industry and Information Technology) instituted a ban on non-state sanctioned VPNs. The ban applies to both consumers and companies; however, the government has been opaque regarding implementation of the rules since the ban took effect, which has led to uncertainty about sanctions for its violation. There have been reports of Chinese nationals being imprisoned for utilizing a VPN. Anecdotal reports indicate that foreigners utilizing non-approved VPNs have experienced involuntary shutdowns of their mobile devices, which then have to be unlocked by local security services who inspect the contents of the phone. There are no reported instances of foreign nationals being imprisoned for violating the ban at this time.

It should be noted that application of laws in China can be uneven and due process cannot be expected. There is potential for arbitrary detention for a range of purported offenses, including alleged violations of state regulations.

Wi-Fi service in country cannot be considered secure and all data accessed via Wi-Fi is subject to surveillance. Proprietary personal, business or financial information should not be accessed or stored on devices in country as this information could be subject to confiscation or monitoring by government authorities.

Mobile phones and tablets that require a local SIM card for telephone and/or internet usage can generally utilize cards from the major carriers in country. The primary mobile internet carriers are China Mobile, China Unicom and China Telecom. Reportedly, China Mobile and China Unicom can be used nationwide on domestic and foreign devices. While China Telecom can also be used in most locations nationwide, the carrier may not be compatible with devices purchased outside China. SIM cards can be purchased at telecom storefronts and mobile device vendors throughout most cities. SIM cards can be topped up at convenience stores, telecom storefronts or via electronic payment services such as Alipay or WeChat. Extreme caution should be exercised with secure data or devices, including personal or identity information.

Learn more at www.aig.com/travel

Travel Guard®

GSOC-10750-18 R03/18