Courthouse Libraries
Dynamic Centers of Civic Engagement Learning

Quarterly Ethics Update
Judicial Integrity and Independence

State Sponsored Hackers
What You Should Know

Save the Date!
57th Annual Convention
Redondo Beach, CA
July 15-17, 2019

President’s Message
GROWING TOGETHER
International Travel with Electronic Devices: A High Level Non-Technical Overview

By Amy Bennett, Information Technology Security Officer
Office of the Circuit Executive for the 9th Circuit

 iPhones, iPads, Androids, Surfaces, laptops, home computers, and a growing number of “smart” devices use the internet as a highway to send and receive information. Personal devices communicate with other personal devices as well as with home and business networks. Home and business networks can include websites, applications, and shared storage. On the main highway, information is aggregated and transmitted at the speed of light. On the main highway, it is both difficult and expensive to intercept and decipher specific information exchanges.

It is the edges of the internet - the people, devices, and initial connections from devices to networks - that are the easiest to intercept, change, block, and track. Simple pickpocketing can net hundreds of dollars in equipment and potentially thousands of dollars in information. A wireless signal from a personal device, like any radio transmission, can be intercepted, jammed, and imitated. An attacker can simply record the information exchange or pretend to be one of the ends of the exchange and transmit malware in either direction. Service provider computers communicate directly with personal devices as the latter request and negotiate access to the internet. Service provider networks can install malware as well as embed malware in routine device and application updates.

Malware is the weapon of choice in cyberspace. Malware, literally bad software, can be a code like ransomware which will encrypt devices and information, holding them for hostage until a victim pays the ransom and receives the decryption key. Malware can be a Trojan horse, which is a malicious program hiding in a benign program, generally designed to call home and allow an attacker remote access to the device or network.

Computers can continuously send malware at the speed of light. Networks of infected computers, robot networks or “botnets”, can work in concert to overwhelm victim computers and networks or simply to attack vast numbers of victims. Botnets swamp the edges of the internet with coordinated attacks from throughout the internet. Defenses against the
ongoing barrage of malware include ensuring operating systems are current, applications are patched, and being careful about to which websites and networks users connect.

Foreign locales increase the difficulty of protecting the edges. Different laws, capabilities, and motivations complicate information security. In some countries, espionage is an accepted form of national influence and cyber is a powerful tool. State sponsored hackers, known as Advanced Persistent Threats (APT), operate with impunity from their home countries as they attack internationally. When a traveler is in a country that supports APTs, communications will traverse infrastructure to which the state sponsored hackers have sustained and sanctioned access.

Travelers are more vulnerable because they may not have the rights of citizens of the country, may not be familiar with the language or the culture, and may not have staying power to see an investigation through or even file an initial police report. Personal devices and local wireless networks may appear to be the same internationally but the connection to the internet can be fundamentally different. Physical and logical access from foreign locales is higher risk, sometimes much higher risk, than from domestic venues.

Criminals – to include APTs - want devices and digits to obtain money and influence. They patrol the edges, physically and electronically, looking for a pocket to pick, a keyboard or screen to record, and wireless connections and transmissions to intercept and perhaps infect with malware or alter. Not having an electronic device at all is the ideal solution to being safe on the international digital edges. Understanding the threats, vulnerabilities, and managing the resultant risk is the next best option.

Whether traveling or not, keeping the number of applications to the absolute minimum helps reduce the likelihood of compromises of the application, of other applications that work with the compromised application, and possibly the rest of the device. Reducing the information applications and devices are authorized to access and transmit to their manufacturers helps protect privacy, personal information, and especially geographic location. There is no reason the helpful free local sightseeing application should be sending the iPhone’s “contacts” list back to its manufacturer. Often, obtaining user information is the goal of application developers. Setting a loaner device to not accept updates or download new applications is a solid approach to preventing infection by malware hidden in updates or applications during a trip.

Using a loaner device with the absolute minimum capabilities to support communications requirements for the trip is the same principle as taking a travel wallet with one credit card and one form of identification. If the travel wallet is stolen, the traveler doesn’t have to replace everything. If the travel device is physically stolen or logically compromised, the traveler doesn’t have to replace everything. IT staff also have the advantage of knowing exactly what was on the travel device.

Using a personal hot spot from either the phone or a mobile wireless hot spot device helps reduce the risk of interception from a wireless provider or someone simply intercepting transmissions on a public wifi network. Using a virtual private network, such as DUO, encrypts the information from the device to the friendly network, in this case the judiciary. Every time a device connects to the judiciary’s network, it

continued on page 16
Announcements by the National Conference of Federal Trial Judges

The National Conference of Federal Trial Judges (NCFTJ), a subdivision within the larger ABA, is the "voice" of the federal trial judges within the ABA. The NCFTJ works with the larger ABA to encourage diversity (gender, race, ethnicity) in the federal trial courts, among other timely issues. The NCFTJ sponsors and partners with others in programs, webinars, and conferences targeted to judges and lawyer members. It's a great networking opportunity with state and appellate judges, and there are all kinds of service opportunities. Click here to view a list of upcoming events, special projects and information.

International Travel
continued from page 15

becomes part of the network. If the device or the connection is compromised, it presents a threat to the entire judiciary. Minimum connections to work networks maximize their security. Physical connections to power outlets only will help protect mobile devices. “Free” charging stations for mobile devices also carry risk. The power cables double as data cables. Mobile charging stations can both remove information from the traveler’s device and install malware. The same is true of USB devices.

Finally, basic reconnaissance before traveling can help enormously to protect person and property. A simple internet search of the country or city and combinations of the words “crime”, “theft”, “iphone”, “laptop”, “mobile device” will provide any major reports from the open press and some from travel blogs. The initial results can be used to make more specific follow on searches. Checking the State Department’s website for the country the traveler is going to and looking at any notifications about the country – especially from the embassy staff will provide current information on what other travelers and Americans living in the country might encounter.

Traveling and staying connected are good things. Unfortunately, criminals are adept at exploiting travelers for influence and profit. Travelers are at the edges of the internet, away from home, using mobile devices, and connecting through third party networks. Making it hard for criminals to steal devices and information and minimizing the impact on the traveler and the organization if they are targeted takes a few extra steps for the traveler and the supporting IT staff. The extra steps can be the difference between a day admiring Notre Dame and a day filling out police reports in the Paris central police station. They can also be the difference between a day settling back into the office and a day working with the IT department to recover files, reset passwords, and configure a brand new mobile device. Safe travels – around the world and along the edges of the internet.