Information Security

1. Traveling with Personal Mobile Devices

Many establishments (e.g., coffee shops, hotels, airports, etc.) offer wireless hotspots or kiosks for customers to access the Internet. Since the underlying infrastructure is unknown and security is often lax, these hotspots and kiosks are susceptible to adversarial activity. The following options are recommended for those with a need to access the Internet while traveling:

a) Mobile devices (e.g., laptops, smart phones) should utilize the cellular network (e.g., mobile Wi-Fi, 3G or 4G services) to connect to the Internet instead of wireless hotspots. This option often requires a service plan with a cellular provider.

b) Regardless of the underlying network, users can setup tunnels to a trusted VPN service provider. This option can protect all traffic between the mobile device and the VPN gateway from most malicious activities such as monitoring.

c) If using a hotspot is the only option for accessing the Internet, then limit activities to web browsing. Avoid accessing services that require user credentials or enteringpersonal information.

Whenever possible, maintain physical control over mobile devices while traveling. All portable devices are subject to physical attack given access and sufficient time. If a laptop must be left behind in a hotel room, the laptop should be powered down and have Full Disk Encryption enabled as discussed above.

2. Storage of Personal Information on the Internet

Personal information which has traditionally been stored on a local computing device is steadily moving to the Internet cloud. Examples of information typically stored in the cloud include webmail, financial information, and personal information posted to social networking sites. Information in the cloud is difficult to remove and governed by the privacy policies and security of the hosting site. Individuals who post information to these web-based services should ask themselves "Who will have access to the information I am posting?" and "What controls do I have over how this information is stored and displayed?" before proceeding. Internet users should also be aware of personal information already published online by periodically searching for their personal information using popular Internet search engines.

3. Use of Social Networking Sites

Social networking sites are an incredibly convenient and efficient means for sharing personal information with family and friends. This convenience also brings some level of risk; therefore, social network users should be cognizant of what personal data is shared and who has access to this data. Users should think twice about posting information such as address, phone number, place of employment, and other personal information that can be used to target or harass you. If available, consider limiting access to posted personal data to "friends only" and attempt to verify any new sharing requests either by phone or in person. When receiving content (such as third-party applications) from friends or new acquaintances, be wary that many recent attacks have leveraged the ease with which content is generally accepted within the social network community. This content appears to provide a new capability, when in fact there is some malicious component that is rarely apparent to the typical user. Also, several social networking sites now provide a feature to opt-out of exposing your personal information to Internet search engines.

4. Enable the Use of SSL Encryption

Application encryption (also called SSL or TLS) over the Internet protects the confidentiality of sensitive information while in transit. SSL also prevents people who can see your traffic (for example at a public WiFi hotspot) from being able to impersonate you when logging into web based applications (webmail, social networking sites, etc.). Whenever possible, web-based applications such as browsers should be set to force the use of SSL. Financial institutions rely heavily on the use of SSL to protect financial transactions while in transit. Many popular applications such as Facebook and Gmail have options to force all communication to use SSL by default. Most web browsers provide some indication that SSL is enabled, typically a lock symbol either next to the URL for the web page or within the status bar along the bottom of the browser.

5. Email Best Practices

Personal email accounts, either web-based or local to your host, are common attack targets. The following recommendations will help reduce your exposure to email-based threats:

a) In order to limit exposure both at work and home, consider using different usernames for home and work email addresses. Unique usernames make it more difficult for someone targeting your work account to also target you via your personal accounts.
b) Setting out-of-office messages on personal email accounts is not recommended, as this can confirm to spammers that your email address is legitimate and also provide awareness to unknown parties as to your activities.
c) Always use secure email protocols if possible when accessing email, particularly if using a wireless network.
d) Unsolicited emails containing attachments or links should be considered suspicious. If the identity of the sender can’t be verified, consider deleting the email without opening. For those emails with embedded links, open your browser and navigate to the web site either by its well-known web address or search for the site using a common search engine. Be wary of an email requesting personal information such as a password or social security number. Any web service that you currently conduct business with should already have this information.

6. Password Management

Ensure that passwords and challenge responses are properly protected since they provide access to large amounts of personal and financial information. Passwords should be strong, unique for each account, and difficult to guess. A strong password should be at least 10 characters long and contain multiple character types (lowercase, uppercase, numbers, and special characters). A unique password should be used for each account to prevent an attacker from gaining access to multiple accounts if any one password is compromised. Disable the feature that allows programs to remember passwords and automatically enter them when required. Additionally, many online sites make use of password recovery or challenge questions. The answers to these questions should be something that no one else would know or find from Internet searches or public records. To prevent an attacker from leveraging personal information about yourself to answer challenge questions, consider providing a false answer to a fact-based question, assuming the response is unique and memorable.

7. Photo/GPS Integration

Many phones and some new point-and-shoot cameras embed the GPS coordinates for a particular location within a photo when taken. Care should be taken to limit exposure of these photos on the Internet, ensure these photos can only be seen by a trusted audience, or use a third-party tool to remove the coordinates before uploading to the Internet. These coordinates can be used to profile the habits and places frequented for a particular individual, as well as provide near-real time notifications of an individual’s location when uploaded directly from a smart phone. Some services such as Facebook automatically strip out the GPS coordinates in order to protect the privacy of their users.

Source: http://www.nsa.gov/ia/_files/factsheets/Best_Practices_Datasheets.pdf