Download files without giving away your personal information

Many sites ask for personal information before you can download information from their site. Your information ends up as a method to spread marketing information via e-mail. This can become very annoying. If you are using Firefox, you may be able download the information without giving up your information. By typing a "control u" when asked for your information, you can view the source code of the WEB page requesting your information. A new window will appear with the source code in it. Search for keys words like download and you may find the link to the information you want. Paste the link into a browser and you should get your information without giving up your personal information.

Beware of the curious neighbor

Beware of shoulder surfing when entering credentials for accounts in crowded places. Places like the supermarket, ATM machine, and mobile devices in crowds are susceptible to shoulder surfing. Once an attacker has your credentials, they could try and access your information.

Keep mobile devices up to date

Smart devices such as iPhones and iPads are increasingly becoming business tools storing sensitive or confidential information. As the market and adoption of these devices continues to grow, so will the attention from attackers. It is important to apply security updates to iPhones and iPads to help protect your data from unauthorized access.

Add a passphrase to your iPad or iPhone

By default, passwords on an iPad or iPhone are four digits in length. Cracking a four-digit password is trivial; there are only 10,000 different combinations. Using an automated program, an attacker can crack a four-digit password quickly. Using the "iPhone Configuration Utility" users can implement a complex password scheme on their iPhone/iPad. By implementing an easy to remember passphrase, the security of the iPhone/iPad significantly increases.

Disable GPS and Geographic tagging data in iPhones

Today's iPhones have the ability to use GPS information and tag photos with Geographic information. This may sound like a good idea so you do not forget where you took a photo. However, if you load a photo onto the Internet you may expose information about yourself you do not want to reveal. For example, a female may open herself to stalking if the location of their residence is on photos. To disable GPS and Geographic tagging of photos in an iPhone:

- Tap on Settings
- Tap on General
- Tap on "Location Services"
- Select the On/Off switch next to "Camera" so that the switch is set to OFF
- Exit settings

Protect your wireless location

Attackers can use the tool Kismet gather a list of networks that a device previously connected. Using the site http://www.wigle.net an attacker may be able to find the geographic coordinates of an SSID. Once the attacker has the coordinates, they can use Google to find the exact location of the network. Users can help protect themselves and their families by using a random SSID and changing the SSID frequently.

Keep your applications current and patched

It is difficult to keep all application current and patched on a computer. Using a tool such as Secunia can help automate the task and make it easier. Secunia collects information concerning software on your system, and then compares these software signatures against a database on Secunia servers. The program then makes recommendations based on this comparison. Secunia personal is available free at http://secunia.com/vulnerability_scanning/personal/.

Carefully read terms of use for mobile applications

Many applications, especially games have terms of use that allow them to access contact information and other private information on the device. Although the terms of use clearly state this, many users do not read the terms and agree to the terms without understanding them. The applications can gather private information they can sell or use for their own nefarious intentions.

Be care what mobile applications you install

Malicious applications are a problem for mobile devices. Apple does have a vetting process covered under an NDA, developers are forbidden to speak about the process. Android applications do not have a formal vetting process for applications , so users have no little assurance an application does not contain malicious code.

Beware of SMSishing Attacks

SMSishing attacks are a form of social engineering where an attacker sends an SMS message to a mobile device or cell phone that appears legitimate but is malicious. When the user responds to the message by clicking on a link, responding to the text message, or calling a number (depending on the message sent), the user starts accumulating charges to their cellular bill. Most users do not have clauses in their cellular contracts protecting them from scams so they are responsible for paying the charges.