Computer hacking is not a new phenomenon, but unlike most computer hackers of today, the first computer hackers intended no harm. Computer hacking began in the 1960’s as a way for computer whizzes to impress one another. They would break into the computer systems of large companies and government agencies to gain bragging rights among their friends. Eventually, some hackers learned how to profit from their abilities and computer hacking evolved into a criminal activity. The most common types of criminal activities carried out by hackers include spam, extortion, and identity theft (Goldsborough, 2010). Hackers are constantly developing new means for gaining access to the computers of others. Therefore, it is important for Internet users to be aware of the strategies computer hackers are using in order to avoid becoming a victim of their crimes.

Some of the recent computer hacking strategies include the use of rogue antivirus programs, wireless Internet networks, zombie computers, and social networking sites. Rogue antivirus programs are fake antivirus programs that have names and interfaces similar to reputable antivirus programs. Hackers have developed these reputable-looking antivirus programs to trick computer users into installing them. Some of the programs even have their own key words on search engines that lead to fake reviews written by the creators (Vamosi, 2009). People often install these programs after receiving an alert that says their computer is infected with a virus (Bradley, 2010). In most cases, the computer is not infected with any viruses, but the user gives the hacker access to their computer once they install what they think is an antivirus program.
Many people unknowingly allow access to their personal information when their computers and ipods connect to wireless Internet networks. Hackers have begun setting up free wireless Internet networks with names such as “Free Public Wi-Fi” to entice unsuspecting users to join. Joining these networks could give the hackers easy access to a user’s email, the information they transmit, and even their hard drive (Sundaralingam, 2009).

Zombie computers are computers infected with viruses that allow hackers to gain control of them. Hackers use these computers to send out spam or launch “denial of service” attacks. “Denial of service” attacks are when hackers use thousands of computers to communicate with a target website simultaneously, in order to overwhelm the website so it cannot handle requests (Schectman, 2009). The victims of “denial of service” attacks are usually businesses that have a vital online presence and would lose money if their website went down. Hackers often launch these attacks and then request that the businesses pay them money in order to stop the attacks (Goldsborough, 2010). Millions of computers around the world are infected by viruses that allow hackers to carry out these types of attacks without the computer owner’s knowledge (Schectman, 2009).

Hackers use social networking sites for harvesting data about users and to hack into users’ accounts. Many users of facebook and other social networks share personal details, such as their date of birth, their hometown, and the high school they attended in their profile. These types of details are often used as security questions for banking and other websites. If hackers can gain access to enough information through people’s social networking profiles, they may also be able to gain access to their online banking and
other personal accounts. Hackers also hack into social networking accounts to gain access to the information from the hacked account and that person’s friends’ accounts. In addition to stealing information, hackers may send messages through hacked accounts to trick the user’s friends into sending them money or clicking on malicious links (Bradley, 2010). These strategies and many others are being used by hackers every day to take advantage of unsuspecting Internet users.

Not only is it important for Internet users to be aware of the strategies hackers are using, but it is also important for them to know how to safeguard their computers and their personal information. First, there are some basic precautions that every computer and Internet user should take. Users should buy legitimate software, not cheap or pirated programs and operating systems. Illegitimate programs are difficult to patch with the necessary security updates, allowing easier access to hackers. Third party security software such as Symantec or McAfee should be used to help protect against hackers, viruses, and spyware. Users should also keep all of their software updated when new versions come out (Goldsborough, 2010). Strong web browser, such as Firefox or Google Chrome, and malware-resistant platforms, such as Mac OS or Linux, are less targeted by hackers. Using these will not guarantee safety from attacks, but they will lower the odds.

There are also steps that computer users should take to protect themselves from the various strategies hackers are using. To avoid being tricked into downloading rogue antivirus software, computer users should become familiar with their security software so they can identify virus alerts from fake programs (Bradley, 2010). The safest option for using wireless Internet is to purchase a personal network rather than using public
networks. Wireless internet users can purchase pocket-sized internet hot spots and pay about 60 dollars a month to receive wireless internet service anywhere there is phone service. If users choose to use public networks, they should avoid sending passwords or credit card information over the internet (Sundaralingam, 2009). When connecting to the wireless Internet network of an establishment, such as a Starbucks or a McDonalds, users should verify the name of the network with the establishment. When in doubt, users should not trust open networks because most are unencrypted and unprotected which means information can be intercepted and viewed by others. Internet use on open networks should be limited to checking public websites such as news websites, not logging into accounts or transmitting personal information (Bradley, 2010). For security on social networks, users should adjust their privacy settings so that only their friends can view their personal information and they should only accept friend requests from people they know. To avoid clicking on malicious links sent by hackers over social networks, users should install a URL preview plug-in, which displays a preview of the destination site when the link is hovered over (Bradley, 2010).

The Internet has become such an integral part of our daily lives that many people forget that there are risks associated with sending personal information over the Internet. Internet users need to remain conscious of their online activity and take the proper precautions to protect themselves. Installing the proper security software and keeping browsers and programs up-to-date are the most basic steps that all Internet users should take. In addition, users should be aware of the techniques hackers are using and how to protect themselves from becoming victims of the attacks. Since hackers are constantly
developing new strategies and targeting the easiest victims, it is the responsibility of Internet users to stay informed about Internet hacking and to keep themselves protected.
References


