AVOID BECOMING A VICTIM OF CYBERCRIME

The news is full of reports detailing the stories of victims who have lost thousands, even millions, of dollars at the hands of cyber criminals. Many of us know someone who has already been the victim of one of these crimes.

As widespread as cybercrime appears to be, it would be easy to conclude there is little anyone can do to avoid becoming a victim.

However, the prevalence of cybercrime does not mean that victimization is inevitable or that people should avoid using the Internet. Users can make themselves aware of the vulnerabilities its use creates and can take steps to reduce their risks.

Computer users can take measures to decrease their risk of becoming the victim of cybercrime by adhering to a few simple Internet usage rules. First, users should remember to log off and shut down their computers when they are not being used. Cyber criminals often scan networks searching for “always on” computers, which they consider readily accessible and unattended targets. By minimizing the amount of time computers are powered on and connected to the Internet, people can reduce their vulnerability to hacking attacks.

Next, users should install and maintain both antivirus and firewall programs. These applications serve as a first line of defence against viruses and other malicious computer programs designed to circumvent security features within computers’ operating systems. Additionally, operating system developers regularly release updates or “patches.” To increase their computer’s security, users should install these updates as soon as they become available. Cyber criminals frequently disguise malicious software as images or documents attached to email messages, so users should never open or download email attachments from unknown senders.

Many people now use wireless networks in their homes. Strong encryption within a wireless router’s settings can prevent cyber criminals from accessing and exploiting data stored on computers. Unprotected, or “open” wireless networks that do not utilize encryption to protect network traffic are very popular targets for cyber criminals. By intercepting this wireless network traffic, crooks can quickly glean personal information, passwords, and other data they can then use to perpetrate various cyber crimes.

Even worse, they sometimes abuse their access to other people’s networks to make it seem like the victims are committing cyber crime. If you have an unencrypted wireless network in your home, don’t be surprised if the police shows up at your door to find out whether you have been hacking into computers, committing online fraud, or distributing contraband.

Many people maintain accounts on literally dozens of different websites, so they create easy to remember passwords. While this means you're less likely to forget an infrequently used password, these simple passwords are quickly compromised by savvy cyber criminals. Moreover, many people use the same password on their social networking websites and their banking and brokerage accounts. When cyber crooks steal passwords for social networking websites, they often try to use them to access financial accounts. In order to avoid such problems, people should use unique and complex passwords for each of their accounts.

These simple rules provide baseline security for most Internet users. However, there are additional precautions people can take to further reduce their risk of becoming the victim of a cyber crime. Understanding and recognizing some of the more common criminal schemes can help people avoid falling prey to them.

In one prevalent scheme, cyber criminals send phishing emails. These emails falsely claim to be from legitimate senders and contain documents meant to dupe the unsuspecting recipient into divulging personal, sensitive information such as passwords, credit card numbers, and bank account information. Some phishing emails have links to fake websites that look just like sites the victims use regularly. After tricking victims into providing banking credentials or other sensitive information, the criminals utilize a number of different methods to access and steal the victim's money.

Internet auction fraud is very common. Cyber criminals saturate the Internet auction sites and offer almost every product people are looking for. The postings often make it appear the seller is located in the same country as the buyer, and the criminal then advises the victim to send money to a business partner, associate, sick relative, a family member, etc.

Money is typically transferred via wire transfers, leaving little recourse for the victim. The most recent trend is an increase in bank-to-bank wire transfers. Most significantly, these wire transfers go through large banks but are then routed to banks in other countries. Similarly, sellers also occasionally direct the victims to pay using phony escrow services. Sometimes they even hijack legitimate escrow websites to make themselves appear even more bonafide. Once the funds are wire transferred to the escrow website, the seller usually discontinues contact.

Another popular scheme is the passing of counterfeit cashier's checks. This scheme targets people who use Internet classified advertisements to sell merchandise. Typically, an interested party contacts a seller. The seller is told the buyer has an associate in the victim's country who owes him money. As such, he will have the associate send the victim a cashier's check for the amount owed to the buyer. The amount of the cashier's check is frequently thousands of dollars more than the price of the merchandise and the victim is told the excess amount will be used to pay the shipping costs associated with getting the merchandise to his location. The victim is instructed to deposit the check, and as soon as the funds are credited to their account, to wire the excess funds back to the criminal or to another associate identified as a shipping agent. Because a cashier's check is used, banks typically release the funds immediately, or after a one or two day hold. Falsely believing the check to be genuine, the seller wires the money as instructed. Ultimately, the bank discovers the cashier's check is fraudulent and removes these funds from the victim's account.

Some people become unwitting accomplices of cyber criminals. Criminals post work-at-home job offers on popular Internet employment sites. These jobs are advertised as "financial manager" or "payment processor" positions. People who accept these positions are told to open bank accounts and provide the account numbers to their employers. They receive transfers to these accounts and are instructed to withdraw this money and transfer it (minus their commission, of course) to designated recipients in foreign countries. When approached by law enforcement, these people are often surprised to learn they have been playing the role of "money mule" for cyber criminals. By acting as a third party receiver of funds, these people have facilitated the transfer illegal proceeds directly to cyber criminals in foreign countries.

Although the threat posed by cyber criminals is real, through the use of a few basic Internet security practices and an awareness of the more common cyber criminal schemes, individuals can reduce their risk of becoming a victim. Users should remain aware of the latest online fraud scams, many of which are described at www.lookstoogoodtobetrue.com. However, if an individual believes he has already been the victim of a cyber crime, he should notify the appropriate law enforcement agency as soon as possible, and may file a complaint online from anywhere in the world at www.ic3.gov, a partnership between the Federal Bureau of Investigation and the White Collar Crime Center. Providing timely and thorough information detailing the particulars of the scheme and identifying characteristics of the criminals helps law enforcement develop an effective investigative strategy.

* Scot Huntsberry is a Supervisory Special Agent who most recently has been working for the FBI in the Cyber Division in Washington, D.C. The FBI's Cyber Division is dedicated to applying the highest level of technological capability and investigative expertise toward combating cyber-based terrorism, hostile foreign intelligence operations conducted over the Internet, and cyber crime. The work of the Cyber Division allows the FBI to stay one step ahead of the adversaries technologically threatening the United States. The Cyber Division addresses all violations with a cyber nexus, which often have international facets and national economic implications, and simultaneously supports FBI priorities across program lines, assisting counterterrorism, counterintelligence and other criminal investigations when aggressive technological investigative assistance is required.