Techno-Tips

How much of your Personal Information is Available on the Internet?

By Antonio Hernández

In the January 2017 AFSM Newsletter, I published an article on "Cybercrime and your Computer Health" where I provided recommendations on how to protect computers and networks to avoid hacker intrusions.

Also, I provided a set of thoughts that I summarize below:

- *Be cautious of free programs on the Internet, such as free email accounts. In exchange for these services, you are freely giving away your personal information! It might be used or sold for advertising purposes.*

- *It is easier for hackers to penetrate the system or computer via free programs. They have fewer safety protections.*

- *Always be mindful that, in the world of cyberspace, you are not the USER, you are the PRODUCT. Your information is merchandise.*

- *If you want to keep something secret or private, **never** upload it or send it via the internet. The information will be there forever, even if you delete it. Be particularly careful of what you post on social media portals.*

In the same article, I wrote about a new type of cybercrime linked to the malware called "ransomware." This virus, once activated, encrypts the data on the computer and blocks access to the information until a ransom payment is made.

The first reasons for bringing back this issue of computer vulnerability and cybercrime is because the intrusions and attacks on computers have increased lately. It is likely you've heard of the recent global attack of computers with the ransomware "WannaCry" that simultaneously attacked corporate computer systems in more than 150 countries, affecting more than 200,000 people. Hospitals, major companies, and government offices were among those that were badly affected. The ransomware was spread by taking advantage of a Windows operating system vulnerability. Microsoft released a security patch in March to fix this vulnerability. The patch was released also for previous and discontinued versions of Windows operating systems. **If you have not updated your computers and networks with this patch, you are at risk.** The average ransom sum requested is US $300, paid in BITCoins.

The second reason was triggered by a recent article in the Wall Street Journal related to how people approach privacy concerns on the web and the mechanisms and tricks used to collect and add personal information, making them "a wide-open book on the web."

At some point, all of your information is vulnerable, from the most insignificant to the most critical. This may be used to harass, blackmail, or disrupt your normal operations. In summary, your information could be weaponized and used against you.

In cyberspace, there are groups of data aggregators specialized in collecting data using "bots" (web robots that are software applications that run automated and repetitive tasks that are both simple and structurally repetitive, at a much higher rate than would be possible for a human alone). The bots collect anything and everything they can about you, from browsing habits to email contacts and contents. This information is aggregated in dossiers to be used for different purposes such as sending target advertisements of the products and services you frequently search for, or to attack you and your financial information. This situation gets critical when the segmented information of multiple sources is analyzed and synthetized using data analytic tools.

Social media platforms have privacy controls. The problem is that people tend not to be very good at using these controls. There are public programs available on the internet with search functions that facilitate or allow to search posts on platforms like Facebook.

Please remember, even if you remove or delete your information on the social media platforms or cancel your accounts, you cannot remove information posted by others.

On top of the recommendations and thoughts I have provided, I want to add a last one related to "cookies" (they are small text files created by a website that are stored in the user's computer, either temporarily or permanently, that provides a way for the website to recognize you and keep track of your preferences). Be aware of internet sites that request you to accept a cookie. Use your good judgment in the decision to accept the request. Not all cookies are bad, but they are considered a vulnerability to privacy.

In summary, cyberspace contains more information about you than you think, and it is readily available for anyone that searches for your name and other keywords, like place of work. If you have not done so, you can try it and you might be surprised at the amount of information about you that comes up. ℵ