Internet Security

Internet security is a branch of computer security specifically related to not only Internet, often involving browser security and the World Wide Web, but also network security as it applies to other applications or operating systems as a whole. Its objective is to establish rules and measures to use against attacks over the Internet. The Internet represents an insecure channel for exchanging information, which leads to a high risk of intrusion or fraud, such as phishing, online viruses, Trojans, worms and more.

Many methods are used to protect the transfer of data, including encryption and from-the-ground-up engineering. The current focus is on prevention as much as on real time protection against well-known and new threats.

The following tables shows the influence of some of the threats on internet security in several years

		2013	2014	2015	2016	2017
Breaches	Total Breaches	253	312	318	300	
Email threats, malware and bots	Overall Email Spam Rate	66%	60%	53%	53%	55%
	Email Malware Rate (Overall)	1 in 196	1 in 244	1 in 220	1 in 131	1 in 412
	Number of Bots	2.3M	1.9M	1.1M	7.5M	12.2M
Mobile	New Mobile Vulnerabilities	127	200	552	606	933
Web	Web Attacks Blocked per Day	569K	493K	1.1M		
	Websites Found with Malware	1 in 566	1 in 1126	1 in 3172		
Vulnerabilities	New Vulnerabilities	6787	6549	5585	7692	
	Zero-day Vulnerabilities	23	24	54	45	48
Spear-phishing (email targeted attacks)	Spear-Phishing Emails per Day	83	73	46		

Recommendations

I suppose several measures to take to protect from security threats. These may limit your exposure to online snoopers.

1. Web Browsing
   Since browsing is probably what internet users do most, it's worth taking browser security and privacy seriously. If you're unhappy that your clickstream (the log of the sites you visit) is in effect public property as far as the security services are concerned, you might consider using freely available tools such as Tor Browser to obscure your clickstream. And to protect yourself against the amazingly brazen efforts by commercial companies to track your online behavior you should, at the very minimum, configure your browser so that it repels many of these would-be boarders.

2. File Storage and archiving
   An option that an increasing numbers of people are exploring is running their own personal cloud service using products such as PogoPlug and Transporter that provide Dropbox-type facilities, but on internet connected drives that you own and control. And if you carry around confidential data on a USB stick, make sure it's encrypted using True Crypt.

3. Cloud Services
   It is better to avoid all cloud services (Dropbox, iCloud, Evernote, etc) that are based in the US, the UK, France and other jurisdictions known to be tolerant of NSA-style snooping. Your working assumption should be that anything stored on such systems is potentially accessible by others. And if you must entrust data to them, make sure it's encrypted.

4. Wireless services
   Have Bluetooth off by default in all your mobile devices. Only switch it on when you explicitly need to use it. Otherwise you'll find that even a dustbin can snoop on it. Similarly, beware of using open wifi in public places. At the very minimum, make sure that any site you interact with uses HTTPS rather than unencrypted HTTP connections. If you don't then anyone nearby can use Firesheep to see everything you're doing.

5. Location data
   Avoid using services such as FourSquare that require location information.

   Apart from those you can follow the below simple methods
   - Create strong passwords.
   - Rethink answers to security questions
   - Opt for double-verification when available
   - Set up a dedicated password-recovery email
   - Protect your Wi-Fi with a password
   - Don’t click on unfamiliar links
   - Always back up your data

Findings

- Internet security is a never-ending battle. A permanently decisive solution to the problem will not be found in the foreseeable future.
- Improvements to the Internet security posture of individuals, firms, government agencies, and the nation have considerable value in reducing the loss and damage that may be associated with Internet security breaches
- Improvements to Internet security call for two distinct kinds of activity: (a) efforts to more effectively and more widely use what is known about improving Internet security, and (b) efforts to develop new knowledge about Internet security
- Publicly available information and policy actions to date have been insufficient to motivate an adequate sense of urgency and ownership of Internet security problems afflicting the United States as a nation
- Internet security is important to the United States, but the nation has other interests as well, some of which conflict with the imperatives of Internet security. Tradeoffs are inevitable and will have to be accepted through the nation's political and policy-making processes

Conclusion

The internet Security is very important. People get addicted to Internet very easily. Internet is tempting, We don't know when we started browsing and when we finished. We have to be aware before doing things. Some people use Internet for illegal activities leading to Cybercrime, they will be jailed or fined according to the regional laws and for the kind of crime they did.

Internet security is a complex subject whose understanding requires knowledge and expertise from multiple disciplines, including but not limited to computer science and information technology, psychology, economics, organizational behavior, political science, engineering, sociology, decision sciences, international relations, and law. In practice, although technical measures are an important element, Internet security is not primarily a technical matter, although it is easy for policy analysts and others to get lost in the technical details. Furthermore, what is known about Internet security is often compartmented along disciplinary lines, reducing the insights available from cross-fertilization.

Attackers target organizations and individuals as well as machines and networks, so internet security is inherently concerned with human adversaries and behaviors of those in the organizations they target. Protecting cyberspace thus involves human, behavioral, psychological, and economic factors and management expertise as well as technical skills and knowledge.

Reference

- Symantec Internet Security Threat Report - February 2019 (ISTR24)
- Symantec Internet Security Threat Report - April 2018 (ISTR23)
- Symantec Internet Security Threat Report - April 2017 (ISTR22)
- Symantec Internet Security Threat Report - April 2016 (ISTR21)
- https://www.slideshare.net/WaqasAmir/symantec-ternetsecuritythreatreportvolume202015social-v2
- https://www.nap.edu/read/18446/chapter/5#24
- https://www.ncbi.nlm.nih.gov/books/NBK223216/