As the internet is increasing with every passing day, so are its associated security risks. Cybercrimes are now a real and widespread threat and governments are doing research and development to formulate plans and develop policies for minimizing the potential risks we face in the cyberspace each day.

However, as people share more personal information on social media and networking websites, it has become more difficult to safeguard valuable data. It is important to recognize and avoid the online threats we face every day.

Let’s look at 10 ways you can keep your personal information and internet identity safe.

1. **Use Encryption**

Before you make any online transaction, always ensure that the website is encrypted. For this, you need to look for two important things. Firstly, you should check that the website URL has an extra “s” at the end of http. The “s” stands for “secured”. Secondly, also look for the trusted security lock symbol in the web address bar. When a website is encrypted, the ‘http’ should change into ‘https’ when it asks you to enter your card information. A lock symbol also appears either at the bottom left of your browser window or the right side of your address bar. Both of these are indication that the website is encrypted and no outsider can see the information you send to the site owner. Your name, credit card number, phone number, address, and other personal information will be safe from hackers.

1. **Use Password Best Practices**

This is the basic step towards protecting your identity online. It is important to keep strong passwords and follow password best practices such as using alphanumeric characters, upper and lowercase letters, and special characters. Never choose a word that can be easily associated with you such as your name, address, or phone number. It is also important to keep different passwords for different accounts and never to repeat your passwords. In case of multiple accounts, it is advisable to use a password manager. Finally, never share your password with anyone and change it once a year.

1. **Turn on Web Browser Blacklisting**

Web browsers usually have the additional option to enable secure web surfing, such as blacklisting. It allows you to visit only trusted and secure websites, and disallows you from accessing websites that are not trusted or encrypted.

1. **Hide Your Personal Information**

When using a web browser, you can sometimes unknowingly share your personal information with others. To avoid this, always configure your browser when you first install it. This can be done by accessing the ‘setup’ option in the browser and configuring it for not revealing your email address, name or other sensitive information.

1. **Install an Anti-Malware Program**

Malware includes harmful software used by hackers and cyber criminals to harm your data and steal your information. It includes programs such as all forms of viruses, spyware, and ransomware. Always install an anti-malware program to help detect and delete such programs from your system. Some of the trusted anti-malware software programs include AVG, Norton, McAfee, and Ad-Aware.

1. **Be Wary of Phishing Scams**

Phishing scams aim to steal your identity and obtain your personal information. To avoid them, it is important to first educate yourself on recognizing them. Most of these scams are in the form of emails that lure you into clicking a link or opening an attachment. In case of an unknown sender or if the email offering seems too good to be true, never open the attachment or click on any link. Also avoid replying to anyone who offers you money, a job offer you didn’t apply for, or any requests for donating to charity. All of these can be a way to steal your identity or your personal information.

1. **Get Private Data Protection**

To protect your sensitive information when sharing it online, you can also get a private data protection suite. It helps in protecting any data that you enter in emails, social media websites, private messengers or blogs.

1. **Enable Cookies Only When Required**

It is also advisable to protect your information, specifically financial information such as credit card data, by enabling cookies only when a website requires it. Cookies are your details that a website stores on your computer and include everything you do on the website. Always enable your cookies only for websites that absolutely require them.

1. **Avoid Public WIFI and Protect Home WIFI with a Password**

Unprotected public WIFI are the key spots for hackers to access your system and spy on your sensitive information. Never use a public WIFI when doing any [transaction](http://www.cardzgroup.com/ContactLessSmartCard.html) or entering your sensitive details on a website. When using home router, always protect it with a password so no unauthorized individual can access it. If you don’t do this, a hacker can access your router and steal your information from your computer. It is also a safe practice to enable encryption on your wireless router to scramble all the data you send online.

1. **Avoid Sharing Your Personal Life on Social Media**

Often, we tend to share too much on social media sites, forgetting that hackers are always on the lookout for information they can misuse to their benefit. It is a safe practice to never share your everyday routine, office, school, bank name, or family details on social media to avoid potential identity theft.

By adopting these 10 basic safety rules in mind, you can avoid many of the threats that lurk online to steal your internet identity. Hence, it is always best to educate yourself and stay vigilant when using the internet.