**8 Ways to Keep Your Internet Identity Safe from Hackers**

The internet has brought a revolutionary change in the modern world and opened doors of convenience and accessibility. But it has also exposed us to online dangers. To get the most out of your online experience, it is important to follow safe digital practices. Whether you are shopping online, entering personal information in a form, or using social media, it’s important to protect your private information from cyber criminals.

Below are 8 ways that can help you keep your identity safe from hackers over the internet.

# Avoid Phishing Scams

Phishing emails are very common scams where cybercriminals trick a user into clicking malicious links. They do this by convincing the receivers that the email is legitimate and is either from their bank, taxation service, or any legitimate organization. Often, the fraudsters lay a bait by offering rewards that are too good to be true. For example, “You have won a lottery”, or “We are excited to announce that you have won two free tickets to Disneyland”. These kinds of messages entice users into clicking the malicious link right away where they are redirected to fake login pages.

Always think before you click. Look out for unofficial email addresses, spelling errors and unexpected messages from friends. It is always better to manually enter a URL of the organization in question and log into their official page, or call on their official number mentioned on their website and verify the information.

# Use Strong Passwords

This cannot be said enough. Keeping strong passwords is the key to your digital kingdom. Always use complex, unique passwords that have a combination of uppercase and lowercase letters, special characters and numbers. Never use the same passwords for multiple accounts. If you feel too anxious to remember so many passwords, use a password manager. It is also important to never share your password with anyone. Another recommended practice is to keep changing your passwords once every year.

# Use Multi-Factor Authentication

Even with the strongest of passwords, there are still good chances of someone cracking them. This is where two-factor or multi-factor authentication is important. Where possible, particularly for financial transactions, use multi-factor authentication such as Google Authenticator. In addition to a password, users are required to input another authentication factor such as a code received on cell phone or a card credential.

# Always Keep a Backup

It is always a safe practice to keep a backup of all your data. If your computer gets infected with malware, ransomware or if it crashes, one must be able to retrieve their lost data. You should also be able to recover your data if you accidentally delete some important information.

# Keep a Robust and Up-to-Date Internet Security Software

As online threats are becoming increasingly sophisticated with more chances of malware success, it’s important to keep a security software that stops malicious software from installing in your system. Some popular security software suites include AVG, Norton, McAfee, and Ad-Aware.

# Install Latest Updates and Patches on Your System

Always keep your operating systems updated and install latest patches for potential vulnerabilities to keep hackers and cyber criminals at bay. Software that is not patched can have vulnerabilities that hackers can exploit to infect your system with malware. To ensure that software is patched at all times, it is recommended to use an automated patch management system.

# Verify a Website Before Entering Sensitive Information

Before entering sensitive information such as payment details on a website, always ensure that the URL should start with an https. Here the “s” stands for “secure”. Websites with only http are not secured and can be hacked easily by criminals. Also look for a lock symbol on the right side of the address bar or at the bottom left of the window. Along with “https”, the lock sign also indicates that the website is encrypted. This means that when you enter your sensitive information such as credit card details, nobody will be able to intercept this information while it is being sent to the website. Your name, credit card details, phone number, and all other related information will be safe.

If a website with transactions does not have “https” and “lock” sign, try to avoid entering your information.

# Avoid Putting too Many Details on Social Media

Once you put your information online, it will be there to stay. Anyone can see it and misuse that information against you. Never put your address, school, office, or other identifiable information on the internet. Also, never share your credit card details such as card CVC, name, manufacturer (e.g. [Cardzgroup](http://www.cardzgroup.com)), or date of issuance and expiry, etc.

# Key Takeaways

Always keep these tips in mind and stay vigilant when using the Internet to prevent fraud and identity theft. Educate your family and friends about how they can stay safe and invest in trusted security software. If more of us are aware and protected, attackers will have little room for exploiting vulnerable victims.