# Easy Internet Safety Tips for Beginners | BestVPN.co

**Written By Hamza Shahid**

"We are all now connected by the internet, like neurons in a giant brain"

Gotta owe it to Stephen Hawking for summarizing things so accurately, yet leaving so much to our own imagination. What he said about the internet is for the most part, TRUE. Some may find it commendable: the 'digital world'. What a time to be alive, eh? At the same time, others may be skeptical about internet usage. We at BestVPN.co understand both sides, but have some of our own thoughts on the subject.

Like everything else in life, there are certain pros/cons to the internet. It is an incredible learning resource, provides access to instant entertainment, makes jobs easier with SaaS tools, and helps in gaining exposure as an individual via social media (presenting many opportunities to become your own boss). Concurrently, there are threats to your personal security and privacy, putting your family/business/money at risk!

## Cybersecurity Awareness!

Unfortunately, there exist individuals who'll exploit the internet by indulging in criminal activities, fooling users through malicious software, obtaining data via phishing, or creating schemes that cheat individuals of their money. Cybercriminals are becoming smarter and more sophisticated in their operations using creative measures to steal identities, commit fraud, or even launch cyber-attacks against others.

If that weren't enough, the internet is filled with violence, dark temptations, and immorality with companies/individuals actively seeking users out, EVERYWHERE! Governments don't want trust their own citizens and impose internet laws that allow for monitoring/eavesdropping on the common man. All this makes you realize that staying SAFE online is no longer a given, but a necessary extracurricular activity.


Now, we know what you're thinking, all this seems gibberish and superficial, right? However, we can assure it ain't! This is why for this National Cyber Security Awareness Month (NCSAM), we've taken the decision to go all-out with helping customers stay safe online. With a little common sense and knowledge about the do's/don'ts, you can surf the 'net unscathed.

## What Internet Safety Issues Are We Facing Today?

The internet serves as a marvelous tool for self-expression, boosting knowledge, and the ability to stay connected to people from around the world. The widespread availability of internet-enabled devices provides everyone around-the-clock access to shopping, credit/financial services, instant entertainment, managing relationships, engaging in sexual instincts, and even receiving help/advice!

As such, there is no doubt that the internet has indeed changed/improved our lives in so many ways, that now it is impossible to imagine a world without it. However, it is only when you realize how dangerous things can get on the internet, do you worry about privacy/security. Below we discuss some serious personal safety risks, which you could end up getting stuck in:

Ransomware – A malicious software that uses cyptovirology, takes over your PC and threatens to publish the victim's data until a ransom is paid. Notable examples include Fusob, WannaCry, Petya, Bad Rabbit, and SamSam, all of which were found using similar patterns for encrypting user files.

Identity Theft – Didn't think it was possible right? It does happen though! Imposters may use techniques like phishing or malware planting to fool you into revealing your financial information, which they then use to commit fraud by impersonating you. Shit hits the ceiling very quick!

Cyberstalking – A very serious crime, due to which a lot of women have to suffer through harassment and mental torture! In this scenario, an attacker repeatedly uses electronic communications to frighten or scare a victim. It may also include libel, slander, defamation, and false accusations.

Sextortion – Thought the real world is a b**ch? The digital world is worse! Some cybercriminals try fooling users into sending nude/sexual images of themselves. Later on, these images are used to extort money or sexual favors from the victim, which can lead to serious depression/anxiety!

Cyberbullying – Easy exposure to violence, graphic images/videos, and petty politics is something that social media getting quite famous for! However, things just take a serious turn, when people use the digital world for bullying people online. This may involve defamation, viral memes, and more!

Online Predation – The internet is a dangerous place particularly for children, as they have the ability to connect with people twice/thrice their age. Some innocent adolescents may become victim to manipulation/coercion by online predators, who have ulterior abusive/sexual motives.

Spamming – Oftentimes, when you join a new social media site or website, you may click somewhere you weren't supposed to, and this results in you having to deal with hundreds and thousands of spammy advertisements, unwanted bulk messages, which opens the door to malware and phishing!

Obscene Content – While the internet can be a happy place for many, it can also be incredibly dark and dangerous. There is tons of obscene content available in the form of information/images/videos that contain gore/killing/bomb blasts and other unpleasant content.

## How Can Users Leverage Maximum Protection Online?

We're sure reading about the dangers above might've got you a little flabbergasted! After all, who could've ever though, things like these happen too, right? Why can't people just learn to be civilized and not be a pain in the a$$ for others? We guess that is something nobody can answer, but if there is one thing BestVPN.co can, is leveraging maximum protection online to protect yourself from such online threats !

Before we get started though, let me please just put this out there. This isn't one of those cliché, re-phrased online guides where the only TIPS you get for protecting your privacy revolve around outdated methods. While researching, we were literally amazed by the type of redundant content available on the internet. So, we hope you find our research impressive, as we try going a little broader!

## Internet Safety Tips: Basic Rules

Similar to how you avoid walking from shady neighborhoods, dodge visiting dangerous websites online, as they may contain ransomware, viruses, or malware.

Always limit the amount of info you reveal online. Potential employers and customers don't need to know your home address or personal relationship status (duh!).

Avoid downloading third-party software/applications, as they might contain malware or may try to steal information. Go for apps/software that certified/verified by relevant authorities.

The internet doesn't have a delete key. Once posted, it forever lives on in the deepest, darkest allies of caches or copies that other people might have made, without you knowing of it.

If you haven't got one already, use a security code on your phone. It can be a password, PIN, or an unlock pattern. Regardless of what you choose, using one is necessary for online privacy!

Make sure your social media accounts are private. Only your close family and friends should be able to see anything about you. The last thing you need is a cyber stalker!

Update your operating system and software regularly to prevent cybercriminals from exploiting old bugs and loopholes in your security, which could result in loss of all personal data.

NEVER connect to public Wi-Fi networks in cafes or restaurants without using a VPN service, as these places are where you can most likely be scammed/hacked/tricked by clever cybercriminals.
Memorizing all your passwords can be a huge pain in the buttocks unless you've got exceptional memory recalling skills. For the average joe, we advise using a password management program.

Avoid writing hate messages or indulge in any kind of bashing/racism/violence as it can get you in serious trouble. Simply writing a threatening message can get you into legal hassles!

## Internet Safety Tips: Protect Yourself from Ransomware

Sometimes life just keeps on giving you lemons and there's nothing you can do about it. Ransomware's are tricky, so you need to make it a habit to back up your data on a regular basis.

Use an anti-virus or anti-malware software that grants you the ability to configure the search to scan archived and compressed files, as that's how most ransomware take control of your system.

It doesn't matter if you are visiting a website, accessing a software, or simply browsing through different games/programs, make sure to keep your firewall turned on at all times.

Make sure to regularly install updates for your operating system and anti-virus/malware software, so that you have an updated firmware that can counter any suspicious file!

It is imperative that users be extra vigilant when clicking links or attachments, particular those that seem suspicious. Analyze the link to get a better idea before clicking it.

## Internet Safety Tips: Stay Protected from Identity Theft

Always remember not to use P2P/File-Sharing apps, if they don't offer data security and privacy. Make sure to use a VPN service if you do, as this will keep your identity anonymous at all times.

As mentioned earlier, never shop from online stores that have a poor reputation, particularly those that have a history of suffering from data breaches in the 'recent' past.
It is imperative to be proactive about your financial information at all times. Do your due diligence in checking your bank and credit card statements every month to quickly identify irregularities.

One of the best ways to keep your identity and information secure at all times is changing the passwords of your financial accounts on a regular basis. Breaches often go unnoticed for weeks!
Make sure that you always send all emails and messages with end-to-end encryption or use a dedicated IP from a VPN service to leverage an unbreakable layer of security at all times.

## Internet Safety Tips: Learn how to Tackle Cyberstalking

If you are being cyberstalked, it is vital that you save all communications with the perpetrator for evidence. It may sound harsh, but you need to report it to the law enforcement agencies.
If you break up with an intimate partner, make sure that you reset all your email accounts, social media, and banking information, so that they are unable to manipulate you in any way.
When it comes to using social media, emails, or chat rooms, it is imperative that you be careful about the information you share, otherwise, you can make it easier for stalkers to gather your pictures/posts!
If it is not mandatory, avoid filling out fields that ask for your personal information like your birthdate when signing up/registering for something online. Who knows how that info might be used!
When posting a picture online (especially if you have doubts about being cyberstalked), make sure that it does not reveal your location. Go for one with a plain background.

## Internet Safety Tips: Stay Vigilant about Sextortion

Sextortion is not only restricted to older men, but even teenagers have been found guilty of such acts. Jealous exes may make life a living hell. Don't hesitate on reporting them immediately!
The internet is filled with gadgets and apps that have the weirdest uses. Did you know there are spyware apps too? Improve your safety online by installing an anti-spyware program. Update it daily!
It is imperative that you realize this valuable lesson of life: people can pretend to be some they're not. Be choosy about the people you choose to add to your social media.
As mentioned earlier, parents need to be involved in the lives of their children. Decide which apps and SM platforms are suitable for them, and regularly review their activity on all.
Make it a habit to turn off electronic devices and webcams, particularly when you are not using them. Hackers/cybercriminals may hack into the camera, record videos, and then blackmail you!

## Internet Safety Tips: How to Handle Cyberbullying

It's important that people themselves have a moral compass. If you see someone you know who is a victim of cyberbullying, don't sit quietly! Report it to an adult as soon as you can.
When using a public computer or someone else's phone to access your social media accounts/email, make sure to log out, as they could use your account for their own ulterior motives.
Avoid sharing your passwords and account information with anybody, as they could take advantage of your kindness and indulge in activities that may come biting your buttocks later on!
It is vital for people to be aware of the consequences of what they write or post online. Refrain from sharing anything that could hurt/ embarrass you in the future. The internet is a messed up place!
As much as we'd like to vent out our frustration and anger on people who send threatening and offensive messages, it is vital to be tolerant and not give two-shits. Nothing can hurt more than blocking them instantly.

## Internet Safety Tips: Learn to Prevent Online Predation

Be extra vigilant and involved with your kids especially if they use social media. Ask them if there's anybody who makes them feel uncomfortable online, so that you can report that individual ASAP!

When we talk about parents being extra careful about watching their kids on social media, we don't mean you should invade their privacy. Just supervise their use of internet-connected devices.

Tell your children that to never talk with individuals who appear to be older in age, and avoid opening/downloading any images sent by people they don't know.

It is imperative that you teach children the do's and don'ts of social media, which include avoiding strangers. Make it clear that they should never meet face-to-face with someone from the internet!

Train your children to be smart about sharing their personal information. Teach them never to talk about their school, house, and other personal stuff. They should end the conversation right away.

## Internet Safety Tips: It's Time to Get Rid of Spamming

Use a secondary email address at times where you are unsure about visiting a particular public directory, social media network, or chat room to avoid getting spam on your original ID.

Many users aren't aware but there are ways to avoid receiving spam mail. One of the most important and proven hacks include installing a spam filtering tool.

Spammers are very tricky with their tactics of sending more spam. Never click the "unsubscribe" link in emails at all costs, as they could confirm that your email address is active.

Don't give your email address to just about anybody. These details should be private and only given to those individuals who you trust completely and blindly.

When signing up at different services, make sure to keep your Email Address hidden by configuring the settings and shifting exposure to "Only Me" or something similar.

## Internet Safety Tips: Block Offensive/Obscene Content

There is nothing more irritating than visiting a website only to find naked images and other obscene content in the form of ads. To get rid of them, use an ad-blocking tool.

If you want to block explicit search results because you have children at home or simply hate the unsolicited exposure of such content, it is wise to turn on "Safe Search" on Google.

If you find any content that may come across as offensive/racist/derogatory, it is your JOB to report it to the relevant administrator right away to avoid further spreading of hate speech.

Social media is loaded with obscene photos, pornographic images, and sometimes gore content. Report them instantly to get the posts taken down, while at the same time eliminating similar results.

It can get difficult for people to watch out for offensive/obscene content on websites since they pop-up so unexpectedly. It is a wise option to install a Web-Filtering tool.

## Internet Safety Tips: Recognize Fake from Real (Phishing)

Phishing is incredibly tricky, as it uses copies of official websites to fool customers in giving their information. Install an anti-phishing software or browser extension to alert you instantly of such sites!
A RULE OF THUMB: NEVER EVER IN YOUR LIFE email your financial details to any person via email, regardless of how much you trust them. Simply because it is not a secure way to transmit such info.
Most people aren't aware of this, until they actually get fooled into clicking a pop-up link. Some of these tricky pop-ups are usually phishing attempts. Always hit close to prevent any incident.
When it comes to leveraging top security from phishing attacks, you need to use a strong firewall software. This will prevent them from gaining access to your network/computer.
If you don't know the sender who is emailing you, avoid clicking on any links and most importantly DON'T download any files, if visible. Untrusted senders are not to be messed with!

## Internet Safety Tips: Destroy Malware and Protect your Data!

If you want to keep your smartphone/laptop/computer secure at all times, install a powerful antivirus/anti-malware software for instant threat detection and deletion.
Never connect to websites that don't utilize HTTPS. The "S" at the end stands for secure. Use HTTPS Everywhere for websites that don't implement it. This will keep your online communications secure!
What most people do after installing an antivirus/anti-malware software is forget that they ever existed. Don't be that careless person and make sure to run scans at regular intervals.
Some links may took you to a website page that looks identical to the original. Be wary of social engineering tactics like phishing. Make sure to always read the link address to get a better idea.
Change the default SSID (name of your Wi-Fi Network) and use WPA2 encryption to prevent unauthorized users from accessing your connection and planting anything suspicious.

## Internet Safety Tips: Don't Get Fooled by Online Scams

This may sound a little harsh, considering social media is for networking, but avoid making unnecessary friends (especially with people you haven't met with or have no knowledge about).
It doesn't matter if you have a tech-geek friend or a person who knows another person, the only person who should be allowed access to your computer remotely is your local ISP.
There are plenty of new e-commerce websites opening up nowadays, but not all of them are secure. Only indulge in online shopping from legitimate resources like eBay, Ali Express, or Amazon!
Scammers can easily fake caller IDs and fool you into giving your financial information. If someone calls and asks for your credit data, hang up and call back to check if the caller is genuine.
Never trust online services that they can provide debt relief and mortgage assistance at the click of a button. They are most likely scam services, so avoid making the mistake of paying upfront!

## Internet Safety Tips: How to Prevent Wi-Fi Eavesdropping

For travelers who often use Wi-Fi networks in public spaces like pubs, coffee shops, and restaurants, always make sure to use a VPN to keep your identity anonymous and connection encrypted.

As mentioned earlier, avoid any unsecure websites that only have “HTTP” before the address. Make sure the websites you visit utilize the “HTTPS” tag. This indicates a secure connection.

When using public Wi-Fi’s never disable your antivirus, anti-malware, or firewall programs, as there are many viruses/malware that can enter through the network.

Some hackers go the extra mile in fooling customers by setting up fake Wi-Fi Hotspots near legitimate public networks. They then steal user data and further go on indulging in identity theft.

Always use Wireless Hotspots that you can trust. Talk to the manager/representative at the coffee shop or restaurant to learn more about their safety measures when connected on Wi-Fi.

## Internet Safety Tips: Keep Your Children Safe Online!

Keep your children’s computer and other internet-enabled devices in a common area, not individual bedrooms. This may sound a bit harsh, but is actually a good way to monitor their use.

Share a social media or email account with your kids, so that you can monitor messages and check to see if he/she is not viewing obscene content on YouTube Kids or talking to strangers!

Tell your kids it’s never okay to buy anything from online without asking you first! Some ads may trick you by offering free things in order to lure you into revealing your personal information.

Follow the safety guidelines by Facebook, Twitter, Instagram and other social media platforms and make sure your kids only join them, after meeting the minimum age requirements.

Train your children to be clever online. Teach them never to post or trade personal photographs, reveal personal information, agree to meet a stranger, or respond to threatening messages!

## Wrapping Things Up

With this, we come to an end of this Internet Safety Tips Guide for the Cyber Security Awareness Month. We hope you appreciate our contribution to spreading the message about being safe on the internet. Let us clarify that we don't deny the usefulness and effectiveness of the Internet.

It has paved the way for vital advancements in the economic, technological, and social landscapes. However, you need protection from the dark sides too of such a platform, and this is exactly what our mission is! Don't hesitate on sharing the guide further on. Have a nice day and enjoy a safer internet!