How to Stay Safe and Secure on the Internet

1. Awareness and proper handling of cyber-criminal communications
   A malicious attack carried out with intent to damage computers, servers, peripherals, etc., for the purpose of stealing data or carrying out illegitimate activities. There are several ways Cyber Fraud can take place.

2. Tips to Prevent Cyber Attacks in the Future
   Weak passwords were the reason for almost 80% of cyber-attacks.
   600000 Facebook accounts are compromised every single day. Avoid responding to requests that ask for personal information.

3. Protect your communication devices

   a. **First Line of Defense** is your DNS (Domain Name System).
   b. **Second Line of Defense** is the browser and its configuration you use. A safe browser is of a prime importance, since it is the software that communicates to the websites on the internet.
   c. **Third Line of Defense** is a good antivirus and is kept updated (the best antivirus, when not kept updated quickly becomes next to useless).

Personal awareness and proper handling of cyber-criminal emails, phone calls and other communications aimed at stealing your personal ID.

Here are some common scams and tips on how to prevent them from happening to you:

"Too-Good-to-Be-True" Scams

As a general rule: If something sounds too good to be true, it probably is. The same rule applies when it comes to flagging a potential scam. If someone you do not know or an organization you do not recognize is contacting you either to give you money, save you unrealistic amounts of money or to court you as a middleman to move money, they may be attempting to scam you. These types of scams, commonly referred to today as '419 scams' or 'advance fee scams,' typically apply some sort of urgency, such as a time limit on your response, whether by phone or via email.

Although these scams can originate from international locations, Canadian homegrown scams of this nature are common as well. Always be vigilant when it comes to people offering you special tax breaks if you provide your bank account information for direct deposit or malicious fake employment websites demanding fees in return for finding you your dream job.

Phishing Scams from ***fishing*** in the sense of catching the unwary by offering bait; computer-hacker slang often replaces *f* with *ph*

Done primarily through email, but also done via phone, this type of scam involves fraudsters sending emails with the intention of getting you to reveal information or to pay non-existent fees. Common tactics involve instilling fear in order to coerce victims to comply. For example, you may receive an email allegedly from your bank informing you that your account has been compromised and that you need to move your savings into another account while they "investigate." You are then directed to an imposter site which mimics the look and feel of your bank, asking for personal information regarding your account, from your Social Insurance Number (SIN) to usernames and passwords, to your bank and line of credit numbers.

In Canada, a prominent scam of this type is the 'CRA Scam,' where a fraudster claiming to be an agent of the Canadian Revenue Agency (CRA) uses threatening or forceful language to coerce you into settling supposed debts with the CRA. While efforts have been made to end this scam, newer versions involve a fraudster contacting a previous victim offering payback of losses in installments with fees attached. We will never ask you to provide personal information, such as your SIN, over email. Be wary of emails asking you for this type of information.

Spearphishing Scams

Like phishing scams, this type of scam is designed to gain access to personal information, install malware on your computer or just defraud you out of some cash. But, unlike a traditional phishing scheme, spearphishing emails, texts, phone calls or even social media posts appear to originate from trusted sources or people you know. If a company or someone you know is asking for personal details or money, it never hurts to double-check with them personally to see if their own personal lines of communication have been compromised or hacked.

How to prevent common scams from happening to you:

Always vet suspicious addresses, people or companies attempting to contact you

Question emails which include spelling or grammatical errors, threats

Never disclose your Credit Card® online unless shopping from a verified secure site, distinguishable by a lock or key symbol or 'https' URL

Never send money to someone or a company you do not know or trust

Check your Credit Card® statements regularly for suspicious activity

Additional Cyber Security Tips:

Block malware attacks – Ensure that anti-malware products are installed and kept up-to-date, and operating system security patches are applied and kept current.

Be vigilant with your emails – Never open emails or attachments from people you don't know, and never follow any links to Web sites included in such emails.

Surf securely - Avoid connecting to untrusted networks, such as free and insecure public WiFi.

Tips to keep your password secure

Don't give out your password to anyone.

Don't use the same password across all your accounts

Don't only use common words that would be found in the dictionary.

Don't post it on a sticky note! Keep your passwords out of plain sight

If you or someone you know falls victim to a common scam or other fraudulent activity, immediately report it to the Canadian Anti-Fraud Centre via their online tool or call toll-free at 1-888-495-8501. Also be sure to contact your local police service for more information on how to proceed.

2017 witnessed several cyber-attacks; where WannaCry and Petya created the most amount of havoc! Digitalization, not only made life easy but has also made us prone to online threats. The consequence of taking security issues lightly had an aftermath on major companies, government sites, health and banking organizations as well as individuals. To avoid cyber-crimes, cyber security awareness is crucial.

What Is It?

A malicious attack carried out with an intent to damage computers, servers, peripherals, etc., for the purpose of stealing data or carrying out illegitimate activities. There are several ways Cyber Fraud can take place, these include –

Hacking

A process wherein your online accounts are accessed illegally or a company's system is manipulated to steal information.

Identity Theft/Data Breach

Illegally making use of individuals or organizations personally identifiable information for fraudulent purposes.

Social Engineering

When the hacker makes use of social interaction by posing as someone you could trust to gain information about a system or organization to infiltrate it.

Malware

Malicious software (virus, Trojans, spyware) designed by hackers designed to damage your device or system to gain access to information.

Key Logger

Designed to keep a track of every key you type on the keyboard. These may run in the background without your knowledge.

More Cyber Security Tips to Prevent Cyber Attacks in the Future

1) The Case of Passwords

Weak passwords were the reason for almost 80% of cyber-attacks.

a) 12 characters min; preferably gibberish and shouldn't involve real words, date, name, or things associated with you that can be easily guessed.

b) Should include a combination of uppercase, lowercase, symbols and numbers. You can check how strong your password is here.

c) Make sure no two accounts have the same password – Use a password manager, such as LastPass or Dashlane, to keep a track of all your passwords.

d) Choose creative answers for security questions – "What's your hometown" – "Venus". Just make sure you don't forget the answer later.

600000 Facebook accounts are compromised every single day. Avoid responding to requests that ask for personal information. What accounts as PII? Name, Birth Date, Address, Credit Card Information, Email Address, Race, Gender, etc.

Never enable 'remember' login & password.

2) Track your financial activities

Sign up for real time alerts. So that when a transaction is made on your card, you are notified in an instant. However sometimes, due to technical glitches, you may not get notifications. Furthermore, it's not possible to constantly keep a check on your financial activities.

3) Online Shopping

If you are shopping online, ensure that the website has a secure https highlighted in green in the top left corner. When you click on the lock symbol on the right, it will indicate that your site is secure.

Sometimes, hackers can embed malware in advertisements, which can reach your through trusted websites as well – **Use Ad Blockers**.

Block attachments of such file types –
exe|pif|tmp|url|vb|vbe|scr|reg|cer|pst|cmd|com|bat|dll|dat|hlp|hta|js|wsf

4) Protect your IP

Unprotected IP = $1 billion extracted in 2 years from 30 countries. Hackers can easily gain access to your IP by means of social engineering and once they have it, there no end of the things they can do.

i) A virtual private network (VPN) helps safeguard your online data through proxy tunneling and encryption by redirecting traffic through a different server and hiding our IP.

ii) Change the administrative password on your router and update firewall rules to not accept any ping requests from the Internet.

Protect your communication devices (computers, tablets, phones).

First Line of Defense,

Is your DNS (Domain Name System). A good analogy of how this works would be an example of a phone book in which you look up the name of the party you want to call. Once you find the name, it displays the phone number to call. So when a DNS server receives your request to connect to ***cnn.com***, it "looks up" the IP number (An **Internet Protocol address** (**IP address**) is a numerical label assigned to each device connected to a computer network that uses the Internet Protocol for communication.[1] An IP address serves two principal functions: host or network interface identification and location addressing.) and connects you to ***cnn.com*** website.

** using the command line window, "look up" the IP numbers for *cnn.com, townofnewmarket.ca, pcplus.ca*.

** ping cnn.com

This is the job of the DNS server to which you connect.

Wouldn't it be nice, if this DNS server, while looking up the IP number for the URL address (Universal Resource Locator, such as *cnn.com*) would take a special care and not connect you to a dangerous website?

Fortunately, this can be done and is not at all difficult.

Free & Public DNS Servers (Valid October 2017)

Provider	Primary DNS Server	Secondary DNS Server
Level3[1]	209.244.0.3	209.244.0.4
Verisign[2]	64.6.64.6	64.6.65.6
Google[3]	8.8.8.8	8.8.4.4
DNS.WATCH[4]	84.200.69.80	84.200.70.40
Comodo Secure DNS	8.26.56.26	8.20.247.20
OpenDNS Home[5]	208.67.222.222	208.67.220.220
Norton ConnectSafe[6]	199.85.126.10	199.85.127.10
GreenTeamDNS[7]	81.218.119.11	209.88.198.133
SafeDNS[8]	195.46.39.39	195.46.39.40
OpenNIC[9]	23.94.60.240	128.52.130.209
SmartViper	208.76.50.50	208.76.51.51
Dyn	216.146.35.35	216.146.36.36
FreeDNS[10]	37.235.1.174	37.235.1.177
Alternate DNS[11]	198.101.242.72	23.253.163.53
Yandex.DNS[12]	77.88.8.8	77.88.8.1
UncensoredDNS[13]	91.239.100.100	89.233.43.71
Hurricane Electric[14]	74.82.42.42	
puntCAT[15]	109.69.8.51	

Tip: Primary DNS servers are sometimes called *preferred* DNS servers and secondary DNS servers are sometimes called *alternate* DNS servers. Primary and secondary DNS servers can be "mixed and matched" to provide another layer of redundancy.

In general, DNS servers are referred to as all sorts of names, like *DNS server addresses*, *internet DNS servers*, *internet servers*, *DNS IP addresses*, etc.

Why Use Different DNS Servers?

One reason you might want to change the DNS servers assigned by your ISP is if you suspect there's a problem with the ones you're using now. An easy way to test for a DNS server issue is by typing a website's IP address into the browser. If you can reach the website with the IP address, but not the name, then the DNS server is likely having issues.

Another reason to change DNS servers is if you're looking for a better performing service. Many people complain that their ISP-maintained DNS servers are sluggish and contribute to a slower overall browsing experience.

Yet another, increasingly common reason to use DNS servers from a third party is to prevent logging of your web activity and to circumvent the blocking of certain websites.

Know, however, that not all DNS servers avoid traffic logging. If that's what you're after, make sure you read all the details about the server to know if that's the one you want to use.

Finally, in case there was any confusion, free DNS servers do *not* give you free internet access! You still need an ISP to connect to for access - DNS servers just translate IP addresses and domain names.

Verizon DNS Servers & Other ISP Specific DNS Servers

If, on the other hand, you want to use the DNS servers that your specific ISP, like Verizon, AT&T, Comcast/XFINITY, etc., has determined is best, then don't manually set DNS server addresses at all - just let them *auto assign*.

Verizon DNS servers are often listed elsewhere as 4.2.2.1, 4.2.2.2, 4.2.2.3, 4.2.2.4, and/or 4.2.2.5, but those are actually alternatives to the Level 3 DNS server addresses shown in the table above. Verizon, like most ISPs, prefers to balance their DNS server traffic via local, automatic assignments. For example, the primary Verizon DNS server in Atlanta, GA, is 68.238.120.12 and in Chicago, is 68.238.0.12.

The Small Print

Don't worry, this is *good* small print!

Many of the DNS providers listed above have varying levels of services (OpenDNS, Norton ConnectSafe, etc.), IPv6 DNS servers (Google, DNS.WATCH, etc.), and location specific servers you might prefer (OpenNIC).

While you don't *need* to know anything beyond what I included in the table above, this bonus information might be helpful for some of you, depending on your needs:

[1] The free DNS servers listed above as *Level3* will automatically route to the nearest DNS server operated by Level3 Communications, the company that provides most of the ISPs in the US their access to the internet backbone. Alternatives include 4.2.2.1, 4.2.2.2, 4.2.2.3, 4.2.2.4, 4.2.2.5, and 4.2.2.6. These servers are often given as Verizon DNS servers but that is not technically the case. See discussion above.

[2] Verisign says this about their free DNS servers: "We will not sell your public DNS data to third parties nor redirect your queries to serve you any ads." Verisign offers IPv6 public DNS servers as well: 2620:74:1b::1:1 and 2620:74:1c::2:2.

[3] Google also offers IPv6 public DNS servers: 2001:4860:4860::8888 and 2001:4860:4860::8844.

[4] DNS.WATCH also has IPv6 DNS servers at 2001:1608:10:25::1c04:b12f and 2001:1608:10:25::9249:d69b. In an uncommon but much-appreciated move, DNS.WATCH publishes live statistics for both of their free DNS servers. Both servers are located in Germany which could impact performance if used from the US or other remote locations.

[5] OpenDNS also offers DNS servers that block adult content, called OpenDNS FamilyShield. Those DNS servers are 208.67.222.123 and 208.67.220.123. A premium DNS offering is also available, called OpenDNS Home VIP.

[6] The Norton ConnectSafe free DNS servers listed above block sites hosting malware, phishing schemes, and scams, and are called *Policy 1*. Use *Policy 2* (199.85.126.20 and 199.85.127.20) to block those sites plus those with pornographic content. Use *Policy 3* (199.85.126.30 and 199.85.127.30) to block all previously mentioned site categories plus those Norton deems "non-family friendly." Be sure to check out the list of things blocked in Policy 3 - there are several controversial topics in there that you may find perfectly acceptable.

[7] GreenTeam DNS "blocks tens of thousands of dangerous websites which include malware, botnets, adult related content, aggressive/ violent sites as well as advertisements and drug-related websites " according to their FAQ page. Premium accounts have more control.

[8] Register here with SafeDNS for content filtering options in several areas.

[9] The DNS servers listed here for OpenNIC are just two of many in the US and across the globe. Instead of using the OpenNIC DNS servers listed above, see their complete list of public DNS servers here and use two that are close to you or, better yet, let them tell you that automatically here. OpenNIC also offers some IPv6 public DNS servers.

[10] FreeDNS says that they "never log DNS queries." Their free DNS servers are located in Austria.

[11] Alternate DNS says that their DNS servers "block unwanted ads" and that they engage in "no query logging." You can sign up for free from their signup page.

[12] Yandex's *Basic* free DNS servers, listed above, are also available in IPv6 at 2a02:6b8::feed:0ff and 2a02:6b8:0:1::feed:0ff. Two more free tiers of DNS are available as well. The first is *Safe*, at 77.88.8.88 and 77.88.8.2, or 2a02:6b8::feed:bad and 2a02:6b8:0:1::feed:bad, which blocks "infected sites, fraudulent sites, and bots." The second is *Family*, at 77.88.8.7 and 77.88.8.3, or 2a02:6b8::feed:a11 and 2a02:6b8:0:1::feed:a11, which blocks everything that *Safe* does, plus "adult sites and adult advertising."

[13] UncensoredDNS (formerly censurfridns.dk) DNS servers are uncensored and operated by a privately funded individual. The 91.239.100.100 address is anycast from multiple locations while the 89.233.43.71 one is physically located in Copenhagen, Denmark. You can read more about them here. IPv6 versions of their two DNS servers are also available at 2001:67c:28a4:: and 2a01:3a0:53:53::, respectively.

[14] Hurricane Electric also has an IPv6 public DNS server available: 2001:470:20::2.

[15] puntCAT is physically located near Barcelona, Spain. The IPv6 version of their free DNS server is 2a00:1508:0:4::9.

Ditching the default DNS service can boost performance, reliability and security. Here are the options
(John E DunnJuly 11, 2017)

https://www.computerworlduk.com/security/best-6-free-dns-services-boost-internet-performance-security-3632790/

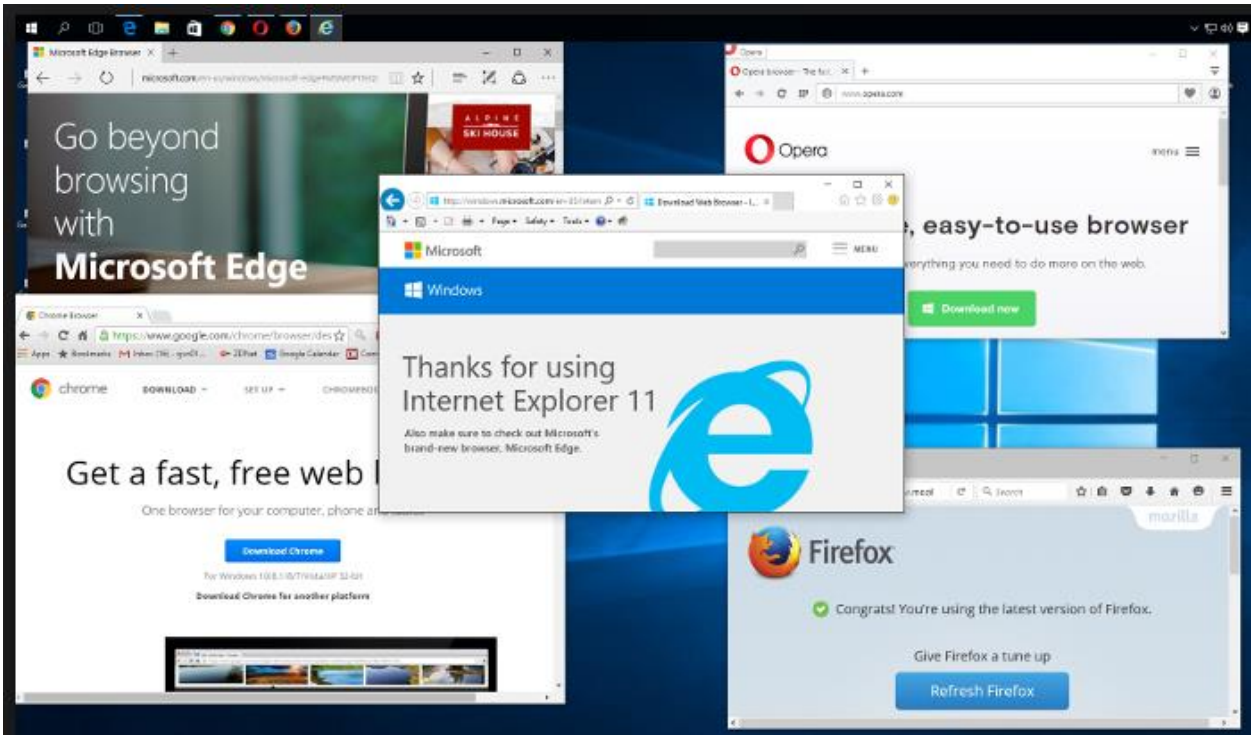
** demo of changing the DNS in the router and in a computer

Second Line of Defense,

Is the browser and its configuration you use. A safe browser is of a prime importance, since it is the software that communicates to the websites on the internet.

Safest Browsers

Chrome took home the gold by a nose over **Opera**, 521 to 520. **Firefox** came in third with a score of 468 and Edge was fourth with 453. Coming in dead last, once more, was IE, 343. First things first: The browser you don't want to run on Windows 10 is **IE 11**.Jan 15, 2016



Here's a look at what you need to know to choose the most secure web browser.

- Opera. If you're analyzing a browser's security level by looking only at its vulnerabilities, you might think Opera is the safest internet browser. ...
- Firefox. ...
- Chrome. ...
- Safari. ...
- Internet Explorer.

The best secure browsers of 2017

All browsers claim to be secure these days, so is there any point in using one that majors on its security?

By John E Dunn & Christina Mercer | Aug 01, 2017

Browsing the internet is becoming more of a minefield as new, more complex and even more aggressive malicious code keeps surfacing.

While some of the nastiest campaigns will be aimed at large businesses, the average user should also take extra care.

https://www.techworld.com/security/best-8-secure-browsers-3246550/

Best Browser Video

https://www.digitaltrends.com/computing/best-browser-internet-explorer-vs-chrome-vs-firefox-vs-safari-vs-edge/

If you don't want to be tracked while browsing the internet, you will have to hide your IP address. There are several ways to do this, from downloading and installing VPN software to using web-based proxies. This wikiHow will guide you through the various processes of blocking your IP address. It will also help you gain a better understanding of how IP addresses and proxies work.

https://www.wikihow.com/Block-Your-IP-Address

Third Line of Defense,

Is a good antivirus and is kept updated (the best antivirus, when not kept updated quickly becomes next to useless).

You can even have two antiviruses running, but have to make sure they do not interfere with each other. This can be especially good when their focus is not the same, i.e. they look out for different types of malware.

For example you can have running at the same time:

Windows defender	+	virtually any mainline antiviruses
Malwarebytes	+	AVG or Eset or Avira

** see page 2 & 3 in the PC CARE – Maintaining your Windows PC section