Stay Safe Online

Nine Things to Remember When You're Online

1. Don't post your personal information online. This includes:
    a. Social insurance number
    b. Drivers license
    c. Address, phone number, etc.
2. Think carefully before posting pictures or videos of yourself. Once you put something online, *it's there forever.*
3. Companies will ***NEVER*** ask you for your password. If someone asks you for your password to something, ***NEVER, EVER*** give it out.
4. On the Internet, anyone can claim to be anything and say anything they want.
5. Think carefully about what you say before you post something online. Just like videos and pictures, once you put something online, *it's there forever*.
6. If you're meeting someone in person that you met online, always meet in a public place first. ***NEVER*** meet at their house or your house the first time.
7. ***NEVER*** click on advertisements. Some sites might say, "you've won a free X, click here to claim." They're almost always scams or at best, wastes of time.
8. If you're ever in doubt about where you are on the internet, close the window and start again.
9. If you're ever in doubt about posting something on the internet, ***don't do it!***

Finally***, NEVER*** give your bank account number over the internet. Ever.

© 2017 Elias Puurunen | www.puurunen.ca | www.northernhci.ca | Twitter: @agfinn
Feel free to redistribute.

Where *is* Safe on the Internet?

When starting out, stick to well-known, reputable sites from companies you've heard of before. Some examples:

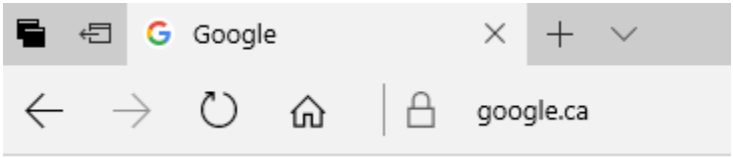
- www.cbc.ca, CBC online
- www.amazon.ca, Amazon
- en.wikipedia.org, Wikipedia, the Free Encyclopedia
- www.google.ca, Google, the Search Engine
- london.kijiji.ca, London Kijiji

© 2017 Elias Puurunen | www.puurunen.ca | www.northernhci.ca | Twitter: @agfinn
Feel free to redistribute.

How Do I Know this Site is Safe?

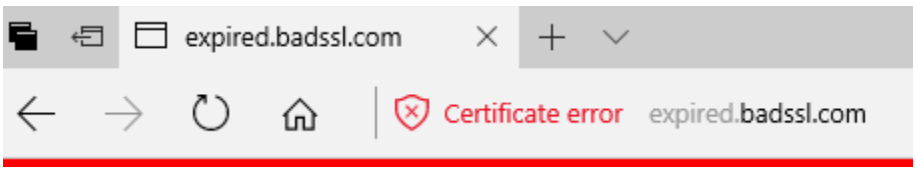
Like walking down an unfamiliar street or purchasing something at the store, you have to build up a sense of what is safe and what isn't when exploring the internet. There are some general rules of thumb to look out for.

At the top-left of your browser window (the program you use to go to websites), there's something called an Address Bar.



In the example above, google.ca is in the address bar. Notice the Padlock icon next to it? That's an indication the site was sent over a *secure* connection. That means that whoever runs this site has some proof they are who they say they are. This is a **good sign**. If you click the padlock, something like this will come up:

Now, if you ever see this, **back out of the site right away. NEVER give any personal information or post anything to a site that displays a Certificate Error.** In fact, you'll even be given a big warning there's something wrong with the *site certificate.* Just back out.



That padlock isn't the be-all end-all of security though. It's possible for someone to get a certificate very easily and get that padlock to show up. How else can you be certain that the site you're at is legitimate?

- Look at the address bar. Do you recognize the website? For example, if you expected to be at Google's site, you should see www.google.ca. If the site *says* it's Google but you don't see Google in the address bar, that may be a sign.
- Does the website end in an odd suffix, like .com.ru? That can be a red flag.
- Does the website address look random or illegible, for example www.asxiinngm.com? Long, illegible addresses are signs of deception.

© 2017 Elias Puurunen | www.puurunen.ca | www.northernhci.ca | Twitter: @agfinn
Feel free to redistribute.

- Does the site say they're a major company, but there's obvious grammar and spelling mistakes? For example, if you go to a site that claims to be a bank, but they have spelling errors all over the place, that's a huge red flag.
- Does the site ask for personal information like social insurance numbers? Unless you're on a Government of Canada website (and you can confirm you are), it's a huge red flag.

Basically, always ask yourself, am I where I think I am? Always err on the side of caution. If something feels out of place, back out.

© 2017 Elias Puurunen | www.puurunen.ca | www.northernhci.ca | Twitter: @agfinn
Feel free to redistribute.

What if I'm Surfing and my Computer Says I have a Virus and to call a 1-800 Number?

First, don't panic. These do come up from time to time and can be scary. Try to close the window. If it won't close, just switch the computer off. ***NEVER CALL THE NUMBER.*** These are always scams where the technician claims that your computer has a virus and then tries to get your credit card to "fix" the issue.

Usually these kinds of scams claim to be a well-known company like Microsoft or Symantec or Apple. ***NEVER, EVER CALL THE NUMBER***.

What if Someone Calls Me and Says I Have a Virus?

Hang up the phone. Don't engage the person in conversation, don't berate them, just hang up the phone. Again, it's a scam. ***Microsoft and any other company will never call you to say you have a virus.*** Just hang up the phone.

What if I Want to Buy Something Online?

Buying online can be very convenient, but it does have its risks. To buy stuff, you'll usually need to sign up on the site first, then enter your credit card information.

Remember that anyone can claim to be anything on the internet, so stick to trustworthy sites like Amazon if you're ordering anything online. If you're ever in doubt, don't hand over your information. Get someone who is familiar with purchasing online to help you out the first few times.

© 2017 Elias Puurunen | www.puurunen.ca | www.northernhci.ca | Twitter: @agfinn
Feel free to redistribute.

How Do I Know an Email is Legitimate?

The majority of the time online, when you get an email it's safe. However, there are times where you'll get an email from someone claiming to be a company or a friend. Worse, if you have a friend whose computer is infected with a virus, that virus can sometimes send emails and make it look like your friend sent it.

Whether an email is legitimate can be answered by asking, "what does this email want me to do?" If it doesn't have any particular links (e.g. click here, download, etc.), then it's probably safe. Ask yourself:

If the email is from a friend:

- Does the content they're sending generally match their behaviour in real life? For instance, if you have a friend who's an engine mechanic and you suddenly get emails from them asking to check out their new flower website, something's probably fishy.
- Is the writing in this email the same style as previous ones? For instance, if they usually have perfect spelling, punctuation and grammar, then suddenly you get an email that has a lot of errors, poor English, or missing punctuation, that could be a red flag.
- Are they asking you to go to a link? Do you recognize where they want you to go? (See below for more tips on that)
- Do you recognize their email address? If your friend emails you from joe@rogers.com then suddenly you get an email from mrjoe@rogers.com or joe@rogers.com.ru, that could be a fake.

If the email is from a company:

- Are there issues with spelling, grammar and punctuation? Most companies can afford to hire good copywriters. This should raise red flags immediately.
- Are they asking for personal information? Probably not legitimate.
- Have you had business dealings with them recently? If not, not legitimate.

Finally, ask yourself, **did I give this company or this person my email address?** If you didn't, be cautious. If it's a friend, call them and ask if they sent you an email. If you get a "huh?" back, they probably didn't. If it's a company, call them and ask the same. Ask them to confirm your email address. If you don't want them contacting you by email, ask to be taken off their lists.

© 2017 Elias Puurunen | www.puurunen.ca | www.northernhci.ca | Twitter: @agfinn
Feel free to redistribute.

Finally, one special note about passwords and bank information. **Your bank will NEVER, EVER ask you to confirm your bank account number, personal or any other information online, EVER.** If you get an email like that, delete it. **If you are ever in doubt about the legitimacy of an email that claims to be the company, look up their number and call them.** If the number is listed in the email and you already suspect the email is bogus, don't trust that number – always look it up elsewhere! Also, **no company will ever ask you to confirm your password or credit card info by email.** ***NEVER*** give out your credit card or banking information ***in an email, EVER***.

© 2017 Elias Puurunen | www.puurunen.ca | www.northernhci.ca | Twitter: @agfinn
Feel free to redistribute.

What if I get an Email that Asks for me to go to a Website to…

As you sign up for services online, you may get emails that ask you to go to a website to do something. Here's some general rules to follow.

The email asks me to…

- **…confirm my email address by clicking a link.** Generally safe, so long as you just signed up for that service. If the email comes out of the blue, delete it. It's probably a scam. If it takes you to a site you don't recognize, back out right away.
- **…click a link to view your bill/etc. online.** Probably legitimate as long as you recognize who it's from. Again, if you end up at a site you don't recognize, back out.
- **…click a link otherwise my account/access/etc. will be suspended.** Scam. Delete it.
- **...confirm my banking details.** Scam. Delete it.
- **…confirm your password.** Very likely a scam. Delete it.
  ...go to a site because you have a virus. Scam. Delete it.
  …click to get your free gift. Probably a scam. Delete it.
  …click because beautiful women/men are waiting for you. Scam. Delete it.
  …click to get discount prescription drugs. Scam. Delete it.

For the most part, as long as you recognize **the company** the email is coming from, it's usually safe to click on the link.

What About if the Email is from a Friend and it has a Link?

Be careful. If someone's computer has a virus, the virus can send emails on their behalf. If the link takes you somewhere weird (see above), then back out right away. If you get an email from someone who claims to be your friend and to ***Click Here***, that's almost always a scam of some sort.

© 2017 Elias Puurunen | www.puurunen.ca | www.northernhci.ca | Twitter: @agfinn
Feel free to redistribute.

Conclusion

All of this probably sounds like a lot of information to absorb. As you become more comfortable with using the internet, it will become second nature. The internet holds tons of information and can provide endless entertainment, but using it improperly can be dangerous too. Always err on the side of caution, stick to well-known sites, and if something sounds too good to be true, it probably is.

© 2017 Elias Puurunen | www.puurunen.ca | www.northernhci.ca | Twitter: @agfinn
Feel free to redistribute.

Notes

© 2017 Elias Puurunen | www.puurunen.ca | www.northernhci.ca | Twitter: @agfinn
Feel free to redistribute.

Notes

© 2017 Elias Puurunen | www.puurunen.ca | www.northernhci.ca | Twitter: @agfinn
Feel free to redistribute.

Notes

© 2017 Elias Puurunen | www.puurunen.ca | www.northernhci.ca | Twitter: @agfinn
Feel free to redistribute.

Notes

© 2017 Elias Puurunen | www.puurunen.ca | www.northernhci.ca | Twitter: @agfinn
Feel free to redistribute.

Notes

© 2017 Elias Puurunen | www.puurunen.ca | www.northernhci.ca | Twitter: @agfinn
Feel free to redistribute.