Internet Safety

This information is presented as general purpose suggestions and the effects may differ on each device or based upon specific updates done to each device. The County of York assumes no liability to unintended results this may have on your specific device and will not assist in any issues that may arise from implementing these tips. This is not an all-inclusive list of all software options available, simply a partial list of some options for the reader to further research for what might work best for them.

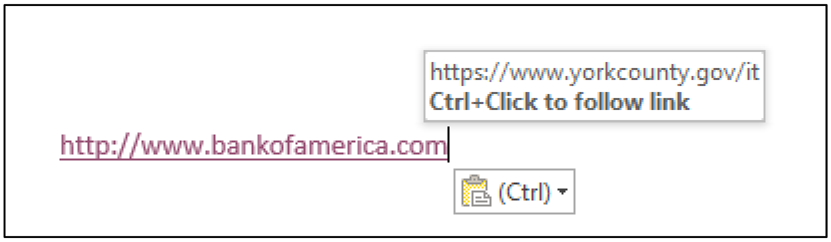
Overview

The two most common ways to be hacked are through spam (unwanted) emails and surfing the Internet (including downloading software). Below are various tips to keep in mind that will help you identify many of the common mistakes that allow a person's device to be compromised. If you know there is a paid program but are trying to find an illegal (free) version of the software, you are breaking the law and will be a target for hackers since you will not want to admit how your system was compromised. Avoid this practice to keep your system, money, and information safe.

Identifying Spam (Unwanted Emails)

If you are reading this, you have an email address and have received spam (unwanted email) many, many times. Most are obvious, but some are very sophisticated and we all have had a bad day where we were in too much of a rush and clicked before thinking. Overall, the most important tip is simply to slow down and think before you click, this will save you from 99% of spam. However considering that many of us get 1000+ spam emails a year, that's still 10 that are a little harder to spot. Below are some tips to help identify those harder emails. Do not reply to them: this alerts the hacker that your email account is valid and if you took the time to respond (even nastily) then they will take the time to target your account even more.

1. **Easy Items** – Usually the first red flag is it being time sensitive and you have to act now or else. Seldom do legitimate companies send these via email. Be on the lookout for bad spelling or grammar, since many of the perpetrators primary language is not English. Never open an attachment that you are not expecting.
2. **Hover over links** – if you are on a computer where you have a cursor, hover over the link with the cursor (do not click). A tool tip or alt text will appear and tell you where that link actually goes. For example [http://www.bankofamerica.com](https://www.yorkcounty.gov/IT), if you hover over will see that this will actually take you to https://www.yorkcounty.gov/IT. Criminals will probably send you to a site you don't want to visit. Below is a screenshot in case you are on a device now that doesn't have a cursor.



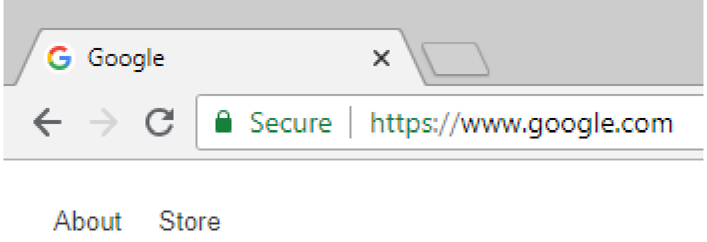
https://www.yorkcounty.gov/it
Ctrl+Click to follow link

http://www.bankofamerica.com

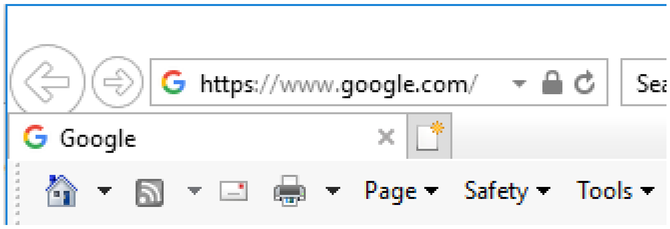
3. **Manually go to website** – For the example above go to your favorite search engine (like google) and type in "Bank of America" and click on the bank from there. Some hackers could get the domain www.bankoamerica.com and unless you can looking VERY closely you may not see the difference.
4. **Check from address –** Never trust the friendly From address. A sender can have this display anything they want such as "John Doe". Look to the actually from email address goingtobehacked@goingtobeavictim.com. Be aware that a hacker may even be able to fake the from email address (although most don't), so it's a way to identify a spam email but won't guarantee a legitimate email.
5. **Trust nothing –** Unfortunately almost half of all emails are spam. Be cautious, and realize the criminals will and do lie. They want to make it look convincing. If they give you a customer care phone number on the email don't use it. Using a search engine, look-up the company's customer care number and call that if you believe it might be legitimate.

Surfing

1. **HTTP vs HTTPS –** At the beginning of most websites is usually "http://" or "https://". The one with the S signifies that it's secure and encrypted. In most browsers as shown below there will additionally be a "lock" icon to additionally signal that it is secure as shown below. When dealing with sensitive information you want to always check for the lock, no lock then do not use it!

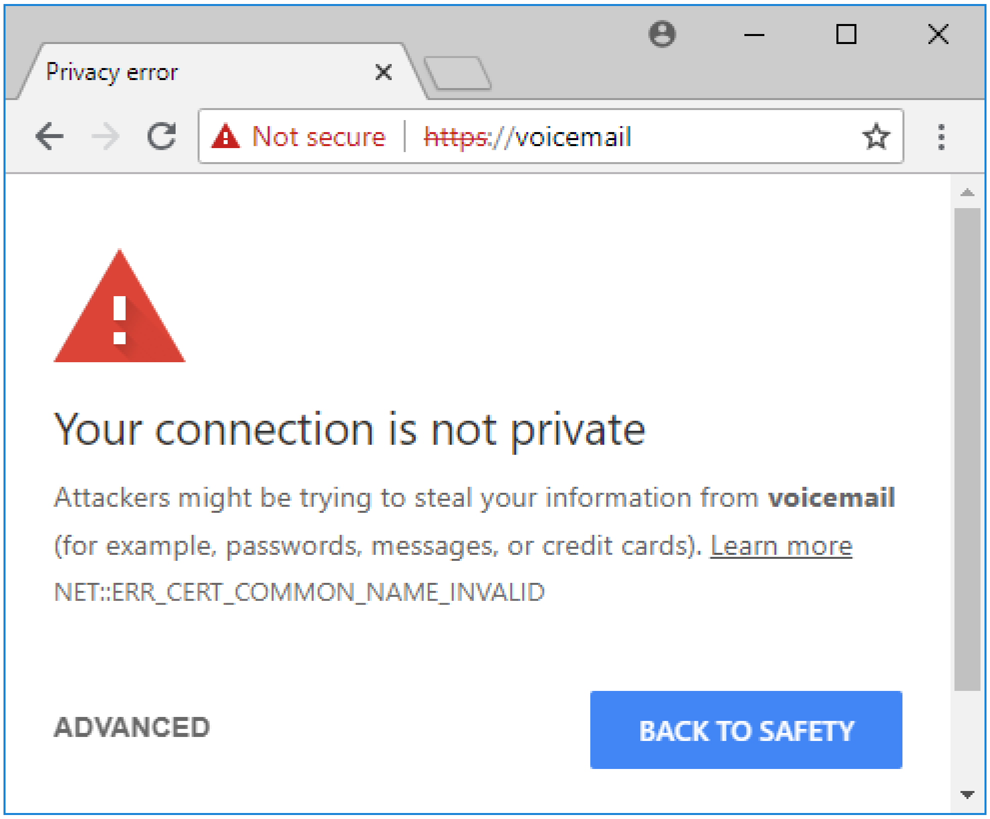


Secure | https://www.google.com



https://www.google.com/

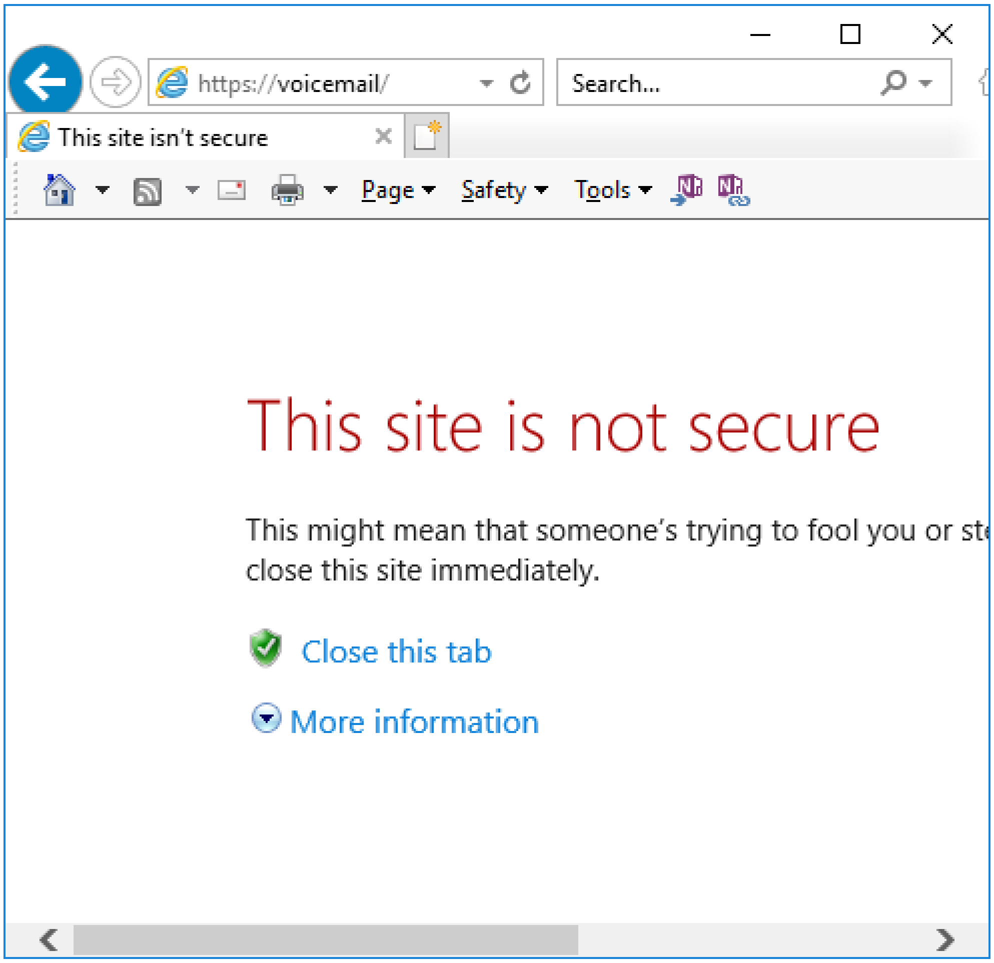
If you ever attempt to go to a site that has https and no lock (meaning it's secure but the destination website is not who it appears to be) stop and do not access the site. Most browsers will warn you to this as shown below.



Your connection is not private

Attackers might be trying to steal your information from **voicemail** (for example, passwords, messages, or credit cards). Learn more

NET::ERR_CERT_COMMON_NAME_INVALID



This site is not secure

This might mean that someone's trying to fool you or st
close this site immediately.

2. **Log out when done** – After you complete any banking or transaction where you are logged in make sure to log out of the website. It is not simply good enough to close your browser or even restart your computer. This is because a hacker can perform a man-in-the-middle attach and hijack your session with your bank or other website. Essentially after you closed your browser they've simply taken over and website login without ever needing to break your username and password.
3. **Clear private data from browsers** – After you log out of the website it is ideal to empty the browser cache in case something was stored locally on your PC. Below are the processes to empty the cache on some popular browsers. Warning this will delete various information such as but not limited to history, form data, passwords, cookies, temporary internet files. Please know data you may have to reenter before performing any of these steps. Often you can choose
    a. **Internet Explorer –** "Tools" | "Internet Options" | "Browsing History" | "Delete…" | choose desired options | "Delete".
    b. **Chrome** – click on the menu or 3 vertical dots | "More Tools" | "Clear browsing data" | choose desired options | "Clear data"

   c. **Safari** – “Preferences” | “Privacy” icon | “Manage Website Data” | choose site | “Remove” or “Remove All”

4. **Do not save passwords or credit card information** – Often after entering credentials to a website your system will prompt asking if you want it to save your credentials. It is ideal to always click no to this. While the system should be storing it in an encrypted format it creates an unnecessary copy of your password that can potentially then we leveraged by other systems or websites impersonating that website later.
5. **Only enter sensitive information into well-known reputable websites** – Before typing your credentials into a website always pause and look over the site. Does this look like the website you are used to going to? Verify in the URL (website address) that it is where you meant to go. Is it paypa1.com instead of paypal.com? Be sure you feel comfortable you are truly at the correct website before entering your credentials.

Downloading

Below are tips for safely downloading documents or programs.

1. **Never from a link sent unsolicited** – Generally, you should only download something that you are actively searching for. Avoid advertisements, pop-up links, and unsolicited emails. If you are interested in a product from one of these sources simply do a separate search on the internet for that product or company and maybe reviews to verify they are a valid company/product.
2. **Freeware, Trial, versus Commercial** – freeware is free, commercial will cost money, and trails will only work for a period of time or will only allow certain functionality.
3. **Free Downloads versus Free Software** – A free download doesn’t mean the software being downloaded is necessarily free.
4. **Download Advertisements** – Many download websites have many advertisements that often display as generic green download pictures. Take your time and make sure that you click on the correct download link.
5. **Custom Installation** – During the first few screens of the install program you may get an option for additional software that will be checked by default. You may also need to choose “custom Installation” to even see these programs. These may have nothing to do with the actual program and have been packaged with it to make money, be sure to read carefully and uncheck unwanted programs.
6. **Use a reputable download site** – Below are a list of well-known download sites that avoid custom installations. Being on this list doesn’t mean any software from them is safe, only a higher chance of being safe

   a. LO4D.com www.lo4d.com
   b. MajorGeeks www.majorgeeks.com
   c. TechSpot www.techspot.com/downloads
   d. Softpedia www.softpedia.com
   e. SnapFiles www.snapfiles.com

f. Betanews http://fileforum.betanews.com
g. Uptodown www.uptodown.com
h. FileHorse www.filehorse.com

References: https://www.macworld.co.uk/how-to/mac-software/safari-cache-mac-3496193/

https://www.lifewire.com/how-to-safely-download-install-software-2625183